

# Répertoire UXP 2.5

**Guide d'installation et de configuration**

UXP-IG-DIR

# Table des matières

---

<b>Notes de mise à jour de Répertoire UXP</b>	<b>1</b>
<b>1. Introduction</b>	<b>2</b>
1.1. Aperçu	2
1.2. Public cible	3
1.3. Concepts UXP	3
1.4. Aperçu du processus	5
1.5. Références	5
<b>2. Installation</b>	<b>7</b>
2.1. Configuration requise	7
2.2. Informations requises	8
2.3. Conditions préalables à l'installation de Répertoire UXP	8
2.4. Installer les paquets Répertoire UXP	9
2.5. Installer la licence	10
2.6. Connecter le serveur de sécurité	10
2.7. Vérifications après l'installation	12
2.8. Haute disponibilité	12
<b>3. Configuration</b>	<b>14</b>
3.1. Définir le schéma d'entrée	14
3.2. Configuration de l'interface utilisateur	16
3.2.1. Langues disponibles	16
3.2.2. Définir la langue par défaut	16
3.2.3. Définir les logos	16
3.2.4. Définir le titre	17
3.2.5. Définir les traductions d'entrée	18
3.2.6. Configurer les colonnes affichées	18
3.2.7. Désactiver certaines pages	22
3.2.8. Désactiver les statistiques du tableau de bord	22
3.2.9. Désactiver les statistiques de surveillance de la vue détaillée	23
3.3. Modifier les paramètres de configuration	23
3.3.1. Modifier l'intervalle de mise à jour de Répertoire	27
3.3.2. Se connecter à Elasticsearch	28

Configuration de l'authentification de base dans Répertoire UXP .....	28
Configuration de la connexion TLS dans Répertoire UXP.....	28
3.3.3. Haute disponibilité entre plusieurs nœuds Elasticsearch .....	29
3.3.4. Configurer la visualisation des données d'instance .....	30
3.3.5. Configurer les données ouvertes de l'instance .....	31
3.4. Liste noire .....	31
<b>4. Ajouter un service de Répertoire au serveur de sécurité .....</b>	<b>33</b>
<b>5. Dépannage .....</b>	<b>34</b>
5.1. Fichiers journaux .....	34
<b>Annexe A: Configuration de base de l'interface utilisateur pour Répertoire UXP... ..</b>	<b>35</b>
<b>Annexe B: Schéma JSON de base pour Répertoire UXP .....</b>	<b>36</b>
<b>Annexe C: Exemple de fichier de configuration de Répertoire .....</b>	<b>38</b>
<b>Annexe D: Formes valides des identifiants UXP .....</b>	<b>40</b>
<b>Annexe E: Notes de mise à jour de Répertoire UXP.....</b>	<b>41</b>

# Notes de mise à jour de Répertoire UXP

---

## 2.5.5 (11.2025)

- La version 9.x d'Elasticsearch est désormais prise en charge.

## 2.5.4 (09.2025)

- Amélioration des performances des membres, des vues des systèmes d'information et de la fonction de recherche pour les instances comportant un nombre élevé de membres et de sous-systèmes.
- Correction : les métadonnées des sous-systèmes ne sont pas mises à jour correctement pour Security Server v1.24.
- Correction : nombre de membres incorrect dans directory-updater-jetty.log.
- Correction : ne pas afficher le métaservice getSecurityServerOperationalDataStats sur la page de visualisation de l'instance lorsque 'Metaservices: Exclude' est sélectionné.

## 2.5.3 (06.2025)

- Ajout de paramètres de délai d'attente Elasticsearch configurables, amélioration de la journalisation et de la gestion des erreurs.

## 2.5.2 (08.2024)

- Correctifs de localisation.

## 2.5.1 (04.2024)

- Correction des fuites de connexion réseau dans le composant de mise à jour.

## 2.5.0 (06.2023)

- 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.
- Amélioration de la prise en charge d'Elasticsearch.
  - La version 8.x d'Elasticsearch est désormais prise en charge.
  - Remplacement du client Java High Level REST d'Elasticsearch obsolète par le client Java API.



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

- L'historique des journaux système est désormais conservé pendant 60 jours au lieu de 30.
- Java Runtime Environment est mis à jour vers la version 17. Mise à niveau d'autres bibliothèques et composants tiers afin de garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

# 1. Introduction

---

## 1.1. Aperçu

Répertoire UXP est un composant d'UXP qui donne accès aux informations relatives à l'instance UXP et permet de les présenter à d'autres parties.

Ainsi, Répertoire UXP :

- rassemble les informations déjà existantes au sein de l'instance UXP ;
- fournit une fonctionnalité permettant d'ajouter/supprimer des informations personnalisées dans/depuis Répertoire UXP via un utilitaire d'interface en ligne de commande (le guide d'utilisation de l'utilitaire CLI est fourni dans [\[UXP-UG-DIRCLI\]](#)) ;
- fournit une interface RestAPI afin que d'autres systèmes puissent lire les informations contenues dans Répertoire UXP (la spécification de l'API est fournie dans [\[UXP-SPEC-DIR-API\]](#)) ;
- fournit une interface utilisateur conviviale pour naviguer et rechercher le contenu de Répertoire UXP (y compris les visualisations des échanges de données entre organisations, sous-ensemble des statistiques d'échange de données en tant que données ouvertes).

Ce guide décrit les tâches liées à l'installation de Répertoire UXP. En outre, il décrit la configuration qui doit être effectuée sur le serveur de sécurité qui fournit le service de répertoire aux autres membres de l'instance.

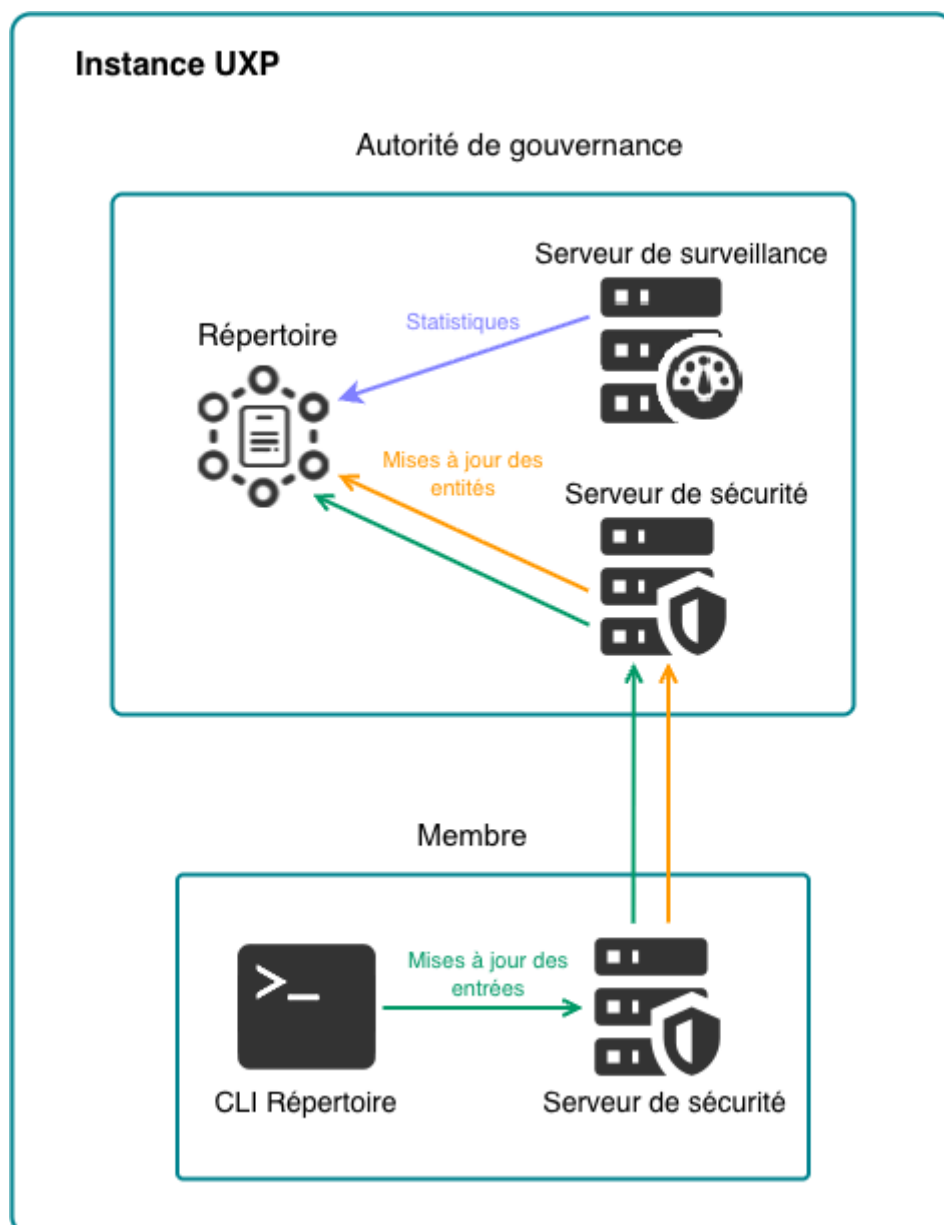


Figure 1. Présentation générale de Répertoire UXP

## 1.2. Public cible

Ce guide s'adresse aux administrateurs système chargés de l'installation et de la maintenance du logiciel Répertoire UXP.

Ce document est destiné aux lecteurs ayant une connaissance moyenne de la gestion des serveurs Linux, des réseaux informatiques et des principes de fonctionnement de la technologie UXP. De plus, on suppose que le lecteur connaît bien le [format JSON](#) et possède des connaissances de base sur le [schéma JSON](#).

## 1.3. Concepts UXP

**Instance UXP** – une installation unique du système UXP à laquelle le Répertoire UXP est lié.

**Entité du Répertoire** – un objet pour lequel Répertoire UXP est conçu pour stocker des entrées de répertoire. Les entités de Répertoire UXP stockeront les informations suivantes :

- **Membre** – une personne physique ou morale qui a rejoint UXP pour fournir ou consommer des services, ou les deux.
- **Sous-système** – représente une partie du système d'information d'un membre UXP. Les membres doivent déclarer certaines parties de leurs systèmes d'information comme sous-systèmes afin d'utiliser ou de fournir des services UXP.
- **Service** – un service fourni via l'infrastructure UXP.
  - **Type de service** – UXP prend en charge deux types de services : SOAP et REST.
    - **Fichier WSDL** – description du service SOAP en langage de description des services Web. Cette description comprend des informations lisibles par l'utilisateur sur le service, ainsi que des descriptions des entrées et sorties qui ont été analysées dans des entrées du Répertoire.



Le Répertoire ne prend pas en charge les fichiers WSDL comportant plusieurs schémas. Pour que l'analyse syntaxique fonctionne, tous les schémas XML doivent être combinés en un seul schéma dans le fichier WSDL. Ce problème sera résolu dans les prochaines versions.

- **Identifiant UXP** – un identifiant unique de l'instance, du membre, du sous-système et du service UXP. Les identifiants UXP ont été formés comme suit :
  - Un code unique est attribué à l'instance UXP, par exemple le code de l'instance de production estonienne est EE.
  - L'identifiant UXP du membre se compose de trois parties : un identifiant d'instance, une classe de membre et un code de membre. L'identifiant UXP d'un membre est par exemple EE/GOV/12345678.
  - L'identifiant UXP du sous-système est constitué de l'identifiant UXP du membre auquel le code du sous-système a été ajouté. Un exemple d'identifiant UXP d'un sous-système est EE/GOV/12345678/testSystem.
  - L'identifiant UXP d'un service est constitué de l'identifiant UXP du sous-système auquel ont été ajoutés le code et la version du service (remarque : il n'est pas obligatoire d'indiquer les versions pour les services). Un exemple d'identifiant UXP de service est EE/GOV/12345678/testSystem/testService/1.
- **Entrée de Répertoire** – comprend une combinaison d'une clé et d'une valeur qui sont stockées dans Répertoire UXP et affichées aux utilisateurs publics. Contient des informations relatives aux entités du Répertoire, par exemple le nom du service qui a été automatiquement analysé par le Répertoire à partir du fichier WSDL ou le guide d'utilisation du service ajouté manuellement par l'administrateur du serveur de sécurité.
- **Configuration de l'entrée du Répertoire** – détails configurables qui déterminent les clés autorisées et le type correspondant de valeurs (par exemple, texte ou pièce jointe) stockées dans Répertoire UXP. Elle décrit à quelle entité du Répertoire l'entrée est liée (par exemple, à un membre, à un sous-système ou à un service) et quel titre est affiché pour

l'utilisateur public (par exemple, Manuel de l'utilisateur).

- **Directory WebUI** – une interface utilisateur Web qui permet aux utilisateurs publics de parcourir le contenu de Répertoire UXP.
- **Autorité de gouvernance (AG)** – organisation chargée de la maintenance de l'instance UXP, y compris Répertoire UXP.
- **Fournisseur de services** – membre ou sous-système UXP qui fournit des services via l'infrastructure UXP. Les fournisseurs de services conçoivent et mettent en œuvre des services, puis les mettent à la disposition des clients.
- **Service Client** – membre ou sous-système UXP qui utilise les services fournis par les fournisseurs de services UXP via l'infrastructure UXP.
- **Elasticsearch** – un outil externe d'analyse et de visualisation de l'instance UXP qui collecte les données de surveillance de l'instance UXP et les transmet au Répertoire UXP.
- **Serveur de sécurité** – composant UXP qui connecte les sous-systèmes des membres UXP à l'infrastructure UXP.
- **Serveur de registre** – composant UXP exploité par l'AG qui sert de registre des informations nécessaires à l'exécution de l'instance UXP. Le serveur de registre UXP distribue ces informations aux serveurs de sécurité sous la forme d'une configuration globale.
- **Configuration globale** – contient les informations dont les serveurs de sécurité ont besoin pour fonctionner. Les serveurs de sécurité téléchargent régulièrement la configuration globale à partir du serveur de registre.

## 1.4. Aperçu du processus

Le diagramme donne un aperçu des étapes à suivre pour mettre en place un Répertoire UXP pleinement fonctionnel.

Toutes les étapes, à l'exception de l'installation et de la configuration des serveurs de sécurité, sont décrites en détail dans les sections suivantes.

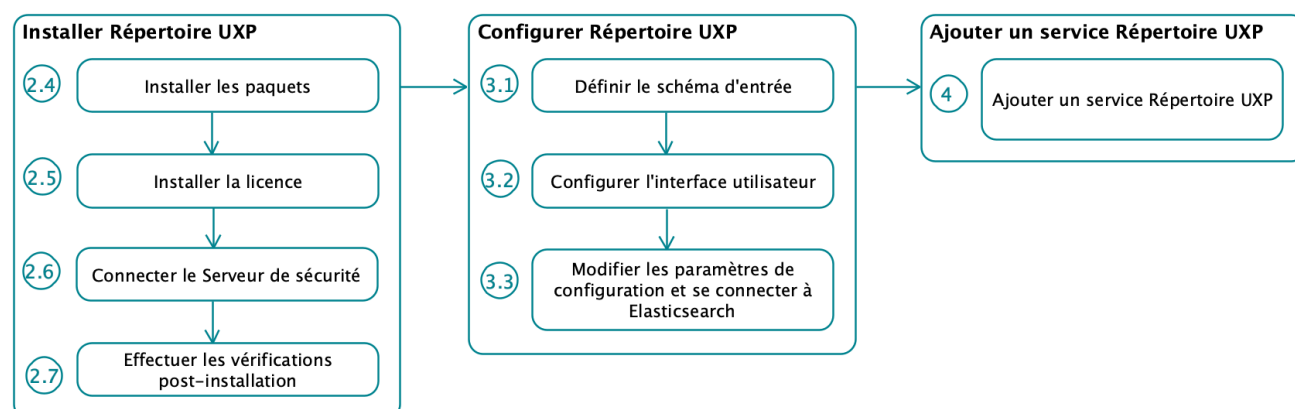


Figure 2. Étapes nécessaires pour installer et configurer un Répertoire UXP

## 1.5. Références



- [CRON] Expression CRON de Quartz Scheduler,  
<http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html>
- [Elastic-Authorization] Autorisation de l'utilisateur | Elasticsearch Guide,  
<https://www.elastic.co/guide/en/elasticsearch/reference/7.x/authorization.html>  
<https://www.elastic.co/guide/en/elasticsearch/reference/8.7/authorization.html>
- [Elastic-Security] Configurer la sécurité pour Elastic Stack | Elasticsearch Guide,  
<https://www.elastic.co/guide/en/elasticsearch/reference/7.x/configuring-stack-security.html>  
<https://www.elastic.co/guide/en/elasticsearch/reference/8.7/configuring-stack-security.html>
- [INI] Fichier INI,  
[http://en.wikipedia.org/wiki/INI\\_file](http://en.wikipedia.org/wiki/INI_file)
- [JSON-Schema] Schéma JSON,  
<https://json-schema.org/>
- [JSON] Présentation de JSON,  
<http://json.org/>
- [UXP-IG-DIRHA] Cybernetica AS. Répertoire UXP : Installation et configuration de la haute disponibilité. Identifiant du document : UXP-IG-DIRHA
- [UXP-SPEC-DIR-API] Cybernetica AS. Répertoire UXP : Spécification API. Identifiant du document : UXP-SPEC-DIR-API
- [UXP-UG-DIRCLI] Cybernetica AS. Répertoire UXP : Installation et utilisation du CLI de Répertoire. Identifiant du document : UXP-UG-DIRCLI
- [UXP-UG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-SS

## 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**. Ubuntu Server 20.04 LTS est également pris en charge.

Le logiciel Répertoire UXP peut être installé sur du matériel physique ou virtualisé.

Le logiciel Répertoire UXP a été testé et confirmé pour fonctionner avec les versions 7.17 - 7.x et 8.x d'Elasticsearch.

#### Paramètres matériels minimaux recommandés

- En général, le matériel du serveur (carte mère, processeur, cartes d'interface réseau, système de stockage) doit être compatible avec Ubuntu 22.04 (ou Ubuntu 20.04) LTS ;
- 2 Go de RAM ;
- carte d'interface réseau 100 Mbps.

#### Paramètres logiciels requis

- Un système d'exploitation Ubuntu 22.04 (ou Ubuntu 20.04) LTS x86-64 installé et configuré ;
- si le Répertoire est séparé d'autres réseaux par un pare-feu et/ou un NAT, les connexions nécessaires vers et depuis le Répertoire doivent être autorisées (voir les ports utilisés dans les tableaux suivants) ;
- si le serveur de sécurité a une adresse IP privée, un enregistrement NAT correspondant doit être créé dans le pare-feu.



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

#### Ports requis pour les connexions entrantes au Répertoire

Port (TCP)	Objectif	Portée du réseau
80	Redirection vers HTTPS	PUBLIC
443	Accès à l'interface utilisateur basée sur le Web	PUBLIC
7200	API du Répertoire UXP utilisée par l'interface Web	PRIVÉ
7400	Service du Répertoire UXP connecté à un serveur de sécurité	PRIVÉ

#### Ports requis pour les connexions du Répertoire

Port (TCP)	Objectif	Portée du réseau
80	Demande d'entités UXP auprès du serveur de sécurité	PRIVÉ
443	Demande d'entités UXP à un serveur de sécurité à l'aide du protocole HTTPS	PRIVÉ
9200	Demande de statistiques auprès du serveur de surveillance UXP	PRIVÉ



L'installation standard de Répertoire UXP configure les ports HTTP et HTTPS par défaut (80 et 443) pour afficher le contenu de Répertoire UXP. Pour changer ce comportement, modifiez la configuration de NGINX dans `/etc/uxp/directory/nginx/uxp-directory` après l'installation.



La liste des connexions sortantes requises ne comprend que les ports spécifiques connus d'UXP. Les ports requis pour des services supplémentaires tels que DNS, NTP, SSH ne sont pas couverts.

La portée du réseau spécifie si le port doit être visible uniquement au sein du réseau PRIVÉ (par exemple, au sein de votre organisation) ou si les ports doivent être visibles 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.

### Informations fournies par l'autorité gouvernante

- L'URL du dépôt des paquets UXP ;
- l'URL de la clé du dépôt des paquets UXP ;
- une licence Connecteur UXP

### Informations spécifiques au serveur que l'AG doit attribuer ou fournir

- Identifiant de l'instance UXP ;
- l'adresse IP privée ou DNS du serveur de sécurité où le service du Répertoire sera ajouté ;
- l'identifiant du fournisseur de services du Répertoire (voir la section [Conditions préalables à l'installation de Répertoire UXP](#) suivante pour plus d'informations) ;
- l'adresse IP privée ou DNS Elasticsearch du serveur de surveillance UXP.

## 2.3. Conditions préalables à l'installation de Répertoire UXP

Répertoire UXP utilise des serveurs sécurisés pour récupérer les données relatives à l'instance dans son ensemble :

- les méta-services sont utilisés pour collecter des données sur les membres, les sous-systèmes et les services UXP ;
- Les services UXP sont utilisés pour permettre aux membres de modifier les entrées relatives aux entités qu'ils gèrent.

Il est donc nécessaire d'enregistrer un client dédié pour effectuer des méta-requêtes et fournir des services du Répertoire.

### Sur le serveur de sécurité :

1. Ajoutez un nouveau client serveur de sécurité.
2. Enregistrez le client du serveur de sécurité.

Voir le guide de l'utilisateur du serveur de sécurité [\[UXP-UG-SS\]](#) pour plus de détails et des instructions étape par étape.

L'identifiant du client du serveur de sécurité enregistré à cette étape sera référencé dans les étapes suivantes de cette section (Fournisseur de services de Répertoire).

## 2.4. Installer les paquets Répertoire UXP

Pour installer le logiciel Répertoire UXP, procédez comme suit :

1. Ajoutez la clé de signature au 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 Répertoire UXP :

```
sudo apt update
sudo apt install uxp-directory
```

La boîte de dialogue d'installation demande les informations nécessaires à la configuration du Répertoire.

5. Entrez l'adresse IP privée ou l'adresse DNS du serveur de sécurité à partir duquel le Répertoire récupérera les informations sur les entités.
6. Entrez l'identifiant de l'instance UXP.
7. Entrez l'identifiant UXP du fournisseur de services de Répertoire (plus d'informations dans la section [Conditions préalables à l'installation de Répertoire UXP](#)) :
  - Classe de membres du service du Répertoire ;
  - Code membre du service du Répertoire ;
  - Code du sous-système du service du Répertoire.
8. Entrez l'adresse IP privée ou DNS d'Elasticsearch utilisée par le serveur de surveillance UXP.



Si aucun schéma n'est saisi pour les adresses IP/DNS, le protocole HTTP sera utilisé par défaut.

Si le schéma HTTPS est saisi ou si l'authentification de base est demandée, une configuration supplémentaire est nécessaire (voir la section [Se connecter à Elasticsearch](#)).



Si une erreur a été commise lors de la saisie des détails, les paramètres peuvent être modifiés dans le fichier de configuration (voir section [Modifier les paramètres de configuration](#)).

## 2.5. Installer la licence

Répertoire UXP ne fonctionne pas sans licence valide. Sans licence valide, le système ne mettra pas à jour les entités et les administrateurs ne pourront pas modifier les entrées.

1. Enregistrez la licence de Répertoire UXP sous `/etc/uxp/directory/license.lic`.
2. Changez le propriétaire et le groupe du fichier `license.lic` :

```
sudo chown root:uxp /etc/uxp/directory/license.lic
```

3. Modifiez les autorisations du fichier `license.lic` :

```
sudo chmod 640 /etc/uxp/directory/license.lic
```

4. Redémarrez le service du Répertoire et les composants de mise à jour :

```
sudo systemctl restart uxp-directory-service
sudo systemctl restart uxp-directory-updater
```

## 2.6. Connecter le serveur de sécurité

Par défaut, Répertoire est partiellement préconfiguré pour utiliser une connexion HTTPS avec le serveur de sécurité. Pour terminer la configuration, vous devez transférer le certificat TLS de Répertoire vers le serveur de sécurité et le certificat TLS du serveur de sécurité vers Répertoire. Voir les étapes ci-dessous :

1. Sur l'hôte Répertoire, copiez le certificat TLS interne de Répertoire à partir du dossier `/etc/uxp/directory/ssl/directory.crt` et enregistrez-le à un emplacement où vous pouvez accéder au fichier via un navigateur Web.
2. **Sur le serveur de sécurité**, configurez le client du serveur de sécurité qui est le fournisseur de services de Répertoire :
  - Naviguez jusqu'à la page Systèmes d'information du fournisseur de services de Répertoire.
  - Définissez le type de connexion comme HTTPS.
  - Sous les certificats TLS internes des systèmes d'information, ajoutez le certificat TLS interne de Répertoire.

Voir le guide de l'utilisateur du serveur de sécurité [\[UXP-UG-SS\]](#) pour plus de détails et des instructions étape par étape.

1. **Sur le serveur de sécurité**, exportez le certificat TLS interne du serveur de sécurité.
2. Ajoutez le fichier de certificat du serveur de sécurité exporté au dossier `/etc/uxp/directory/ssl` de Répertoire. Modifiez le propriétaire, le groupe et les permissions du fichier :

```
sudo chown uxp-directory:uxp /etc/uxp/directory/ssl/<TLS_CERTIFICATE_FILE_NAME>
sudo chmod 640 /etc/uxp/directory/ssl/<TLS_CERTIFICATE_FILE_NAME>
```

où `<TLS_CERTIFICATE_FILE_NAME>` est le nom du fichier de certificat TLS du serveur de sécurité.

Il est possible de renommer `<TLS_CERTIFICATE_FILE_NAME>` en `security-server.crt`

```
sudo mv /etc/uxp/directory/ssl/<TLS_CERTIFICATE_FILE_NAME>
/etc/uxp/directory/ssl/security-server.crt
```

et de définir la valeur du paramètre `security-server-tls-cert-file` dans la section `[common]` du fichier de configuration `/etc/uxp/directory/directory.ini` sur le chemin absolu du fichier de certificat (`/etc/uxp/directory/ssl/<TLS_CERTIFICATE_FILE_NAME>`).

3. Redémarrez les services de Répertoire :

```
sudo systemctl restart uxp-directory-backend
sudo systemctl restart uxp-directory-updater
```



La connexion HTTPS est fortement recommandée pour la communication entre le Répertoire et le serveur de sécurité. Si une connexion HTTP non sécurisée reste

nécessaire :

1. Définissez la valeur du paramètre `security-server-use-tls` dans la section `[common]` du fichier de configuration `/etc/uxp/directory/directory.ini` sur `false` et la valeur du paramètre `security-server-port` sur `80`.
2. Redémarrez les services de Répertoire :

```
sudo systemctl restart uxp-directory-backend
sudo systemctl restart uxp-directory-updater
```

## 2.7. Vérifications après l'installation



Par défaut, la connexion entre Répertoire et le serveur de sécurité est configurée sur HTTPS. Terminez la configuration de la connexion (voir [Connecter le serveur de sécurité](#)) avant de commencer les 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 (le résultat attendu est le suivant) :

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

uxp-directory-backend.service      loaded active    running    UXP Directory Backend
uxp-directory-service.service      loaded active    running    UXP Directory Service
uxp-directory-updater.service      loaded active    running    UXP Directory Updater
```

2. Assurez-vous que vous pouvez accéder à l'interface utilisateur du Répertoire à l'adresse `https://<directory>` à partir d'un navigateur Web.

Remplacez `<répertoire>` par l'adresse IP publique ou DNS de l'interface utilisateur du Répertoire.



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

Répertoire UXP a été installé avec succès. La configuration du Répertoire est décrite dans les sections suivantes.

## 2.8. Haute disponibilité

Le Répertoire UXP prend en charge une configuration en grappe pour obtenir une haute disponibilité (HA). La solution HA repose sur une réplication de la base de données entre les nœuds du Répertoire. La mise en grappe fonctionne comme une base de données asynchrone active-passive sans partage. Le nœud actif configuré est pleinement fonctionnel et réplique les données vers le(s) nœud(s) passif(s) (réplique). Le(s) nœud(s) réplique(s) est (sont) réservé(s) aux opérations en lecture seule.

Pour plus d'informations, veuillez consulter le guide d'installation haute disponibilité de Répertoire UXP [\[UXP-IG-DIRHA\]](#).



## 3. Configuration

---

### 3.1. Définir le schéma d'entrée

Répertoire UXP offre des fonctionnalités permettant d'ajouter/supprimer des informations personnalisées dans/depuis Répertoire UXP via un utilitaire d'interface de ligne de commande (le guide d'utilisation de l'utilitaire CLI est fourni dans [\[UXP-UG-DIRCLI\]](#)). Ces données sont stockées dans le Répertoire sous forme d'entrées de Répertoire.

Pour configurer les entrées de Répertoire UXP, un **schéma JSON** doit être défini. Pour modifier le schéma, ouvrez le fichier `/etc/uxp/directory/entry.schema.json`. Le schéma par défaut pour Répertoire UXP se présente comme suit :

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "title": "Directory Entry Root Schema",
  "additionalProperties": false,
  "definitions": {
  },
  "properties": {
    "member": {
      "type": "object",
      "additionalProperties": true,
      "properties": {
      }
    },
    "subsystem": {
      "type": "object",
      "additionalProperties": true,
      "properties": {
      }
    },
    "service": {
      "type": "object",
      "additionalProperties": true,
      "properties": {
      }
    }
  }
}
```

Le schéma ci-dessus accepte toute entrée qu'un membre UXP souhaite ajouter. Pour mieux contrôler la gestion des entrées, les champs *additionalProperties* et *required* peuvent être utilisés :

- "additionalProperties" : false empêchera l'envoi de toute propriété superflue/non

définie. Ceci est utile dans un scénario où il existe un ensemble d'entrées attendues auxquelles chaque membre doit se conformer.

- "required": ["entry1", "entry2"] s'assurera que lorsqu'un membre soumet une entrée, tous les champs requis ont été remplis. Ceci est utile dans un scénario où il existe des paires de champs obligatoires, de sorte que toutes les informations doivent être soumises. Par exemple, lors de l'ajout d'informations sur les coordonnées, il peut être utile de demander à tous les contacts d'indiquer leur nom, leur adresse électronique et leur numéro de téléphone.

En utilisant *additionalProperties* et *required* collectivement, il est possible de s'assurer que tous les membres ont saisi les mêmes informations.

Il est possible de définir différentes entrées au niveau des membres/sous-systèmes/services. Par conséquent, à des fins de réutilisabilité, la logique des entrées doit être définie dans le champ « définitions » puis référencée à l'aide de la construction "\$ref".

Pour définir une entrée du Répertoire qui inclut un fichier joint, le champ *\_file* doit être défini. Pour plus d'informations sur les références de fichiers, voir la section 4.4. dans [\[UXP-UG-DIRCLI\]](#).

Un exemple de schéma plus avancé est présenté dans [Schéma JSON de base pour Répertoire UXP](#), qui inclut l'utilisation des champs et des constructions décrits précédemment. De plus, l'exemple définit le schéma qui suit la description ci-dessous :

- Les administrateurs du serveur de sécurité ne peuvent pas soumettre de propriétés étrangères/non définies pour les membres, les sous-systèmes et les services.
- Deux logiques d'entrée ont été définies comme construction "\$ref" :
  1. La section *contacts* comprend les champs *contact-name*, *contact-phone* et *contact-email*, qui doivent tous être remplis.
  2. la section de *documentation* comprend les champs *managedBy* et *service-guide* qui contient le champ *\_file*. Ces données doivent également être saisies.
- Les administrateurs du serveur de sécurité doivent saisir les champs de la section *contacts* pour tous les membres, sous-systèmes et services,
  - c'est-à-dire que la section *contacts* est référencée dans les propriétés du membre, du sous-système et du service.
- Les administrateurs de serveurs de sécurité doivent télécharger un fichier joint (par exemple, un guide de l'utilisateur) et saisir la note concernant la personne responsable de ce fichier pour tous les services,
  - c'est-à-dire que la section *service-guide* est mentionnée dans les propriétés du service.

Voir la section [Définir les traductions d'entrée](#) pour configurer les traductions des champs d'entrée du Répertoire.



Directory WebUI affiche les valeurs saisies par ordre alphabétique des <key>s. Par exemple, l'ordre affiché de *contacts* dans [Schéma JSON de base pour Répertoire](#)

UXP est : `contact-email`, `contact-name` et `contact-phone`.



Répertoire UXP prend uniquement en charge les types de schéma JSON *object* et *string*.

## 3.2. Configuration de l'interface utilisateur

Répertoire UXP permet de personnaliser certains aspects de l'interface utilisateur, tels que le titre, les logos, la liste des langues prises en charge, la langue par défaut, les traductions des entrées, les colonnes affichées dans les tableaux et les pages masquées.

Pour configurer l'interface utilisateur de Répertoire, modifiez le fichier `/etc/uxp/directory/ui-config/config.json`. L'interface utilisateur sera automatiquement mise à jour après les modifications, c'est-à-dire qu'aucune étape supplémentaire ne sera nécessaire pour appliquer les changements.

Un exemple de configuration de l'interface utilisateur est présenté dans [Configuration de base de l'interface utilisateur pour Répertoire UXP](#).

### 3.2.1. Langues disponibles

Il est possible de modifier les langues disponibles dans l'interface utilisateur du Répertoire.

- Modifiez la section **languages** du fichier de configuration.
  - Ces valeurs sont représentées par des codes de pays.

```
"languages": ["en", "ua"]
```

Tableau 1. Langues prises en charge

Valeur du paramètre	Langue
en	Anglais
ua	Ukrainien (fourni avec le paquet <code>uxp-addon-directory-ua-lang</code> )

### 3.2.2. Définir la langue par défaut

Il est possible de définir la langue par défaut de la page web qui s'affiche lorsque l'utilisateur visite le Répertoire pour la première fois.

- Modifiez la section **defaultLanguage** du fichier de configuration.

```
"defaultLanguage": "en",
```

### 3.2.3. Définir les logos

Dans l'en-tête de l'interface utilisateur web de Répertoire UXP, plusieurs logos peuvent être affichés. Le nombre de logos possibles dépend de la taille de chaque logo. En plein écran, 460 pixels sont alloués à l'espace réservé aux logos, chaque logo étant séparé par un petit espace (20 px).

Les logos sont affichés dans l'ordre où ils sont définis dans la configuration. Chaque logo peut être accompagné d'une image alternative à afficher sur un petit écran. En outre, il est possible de rendre le logo interactif, de sorte qu'un clic sur le logo redirige l'utilisateur vers l'endroit souhaité.

- *imageLarge* — l'image affichée sur les grands écrans (largeur d'écran de > 800px) ;
- *imageSmall* — l'image affichée sur les petits écrans (largeur d'écran de < 800px) ;
- *href* — l'URL de la page web vers laquelle l'utilisateur sera redirigé lorsqu'il cliquera sur le logo.



S'il n'y a qu'un seul logo pour toutes les tailles d'écran, réglez les deux sources d'image sur la même valeur.



Des logos externes peuvent être utilisés. Si vous utilisez un logo externe, ignorez les étapes 1 à 3.

1. Copiez le(s) logo(s) dans `/etc/uxp/directory/ui-config`
2. Modifiez le propriétaire et le groupe du ou des fichiers logo :

```
chown uxp-directory:www-data logo-lg.svg logo-sm.svg
```

3. Modifiez les autorisations du ou des fichiers logo :

```
chmod 640 logo-lg.svg logo-sm.svg
```

4. Modifiez la section **logos** du fichier de configuration. Ajoutez le nom de fichier ou l'URL du logo comme valeur de *imageLarge* et/ou *imageSmall*.

```
"logos": [
  {
    "imageLarge": "logo-lg.svg",
    "imageSmall": "logo-sm.svg",
    "href": "/"
  }
]
```

### 3.2.4. Définir le titre

Pour chaque langue installée dans Répertoire UXP, il est possible d'utiliser un titre différent. Il est recommandé de garder un titre court, sinon des problèmes de lisibilité peuvent survenir sur des écrans plus petits. En outre, sur les écrans plus petits (largeur d'écran < 1400px), le

titre est masqué et seuls les logos sont affichés.

- Modifiez la section **title** du fichier de configuration.

```
"title": {
  "en": "UXP Directory",
  "ua": "Каталог веб-сервісів"
}
```

Il est également possible de modifier le titre affiché dans la barre de navigation du navigateur. Il est également recommandé de garder ce titre court, car plus l'utilisateur a d'onglets ouverts, moins le titre est affiché.

- Modifiez la section **navTitle** du fichier de configuration.

```
"navTitle": {
  "en": "UXP Directory",
  "ua": "Каталог веб-сервісів"
}
```

### 3.2.5. Définir les traductions d'entrée

Pour chaque langue installée dans Répertoire UXP, il est possible de définir une traduction différente pour une entrée. Ces entrées remplacent les fichiers de traduction.

- Modifiez la section **entryTranslations** du fichier de configuration.

```
"entryTranslations": {
  "en": {
    "is-contact-name": "Contact Name",
    "is-phone-number": "Contact Phone Number",
    "is-email": "Contact Email Address"
  },
  "ua": {
    "contact-name": "Контактне ім'я",
    "contact-phone": "Контактний телефонний номер",
    "contact-email": "Електронна пошта"
  }
}
```

### 3.2.6. Configurer les colonnes affichées

Dans les tableaux suivants de l'interface utilisateur de Répertoire, les colonnes sont configurables via le fichier de configuration :

- tableaux sur la page Membres, systèmes d'information et services ;
- tableaux de la page Détails sur les membres et détails sur les systèmes d'information.

Tableau 2. Colonnes disponibles dans le tableau des membres (affichée sur la page Membres)

En-tête de colonne	Valeur du paramètre	Explication
Nom	<code>__name</code>	Nom d'un membre. Récupéré à partir de la configuration globale.
Code membre	<code>_identifierEnd</code>	Code d'un membre. Récupéré à partir de la configuration globale.
Systèmes d'information	<code>_subsystems</code>	Le nombre total de sous-systèmes (c'est-à-dire de systèmes d'information) des membres.
Services	<code>_services</code>	Nombre total de services du membre.
Première découverte	<code>_dateOfFirstDiscovery</code>	Date à laquelle les données du membre ont été enregistrées pour la première fois dans Répertoire.
Dernière découverte	<code>_dateOfLastUpdate</code>	Date à laquelle les données du service ont été mises à jour pour la dernière fois dans Répertoire.
État	<code>_status</code>	Affiche si le membre est <i>ACTIF</i> ou <i>INACTIF</i> . Un membre est considéré comme <i>INACTIF</i> lorsqu'il a déjà existé, mais que Répertoire ne l'a pas retrouvé lors de la dernière mise à jour (par exemple, le membre a été supprimé).

Tableau 3. Colonnes disponibles dans le tableau des systèmes d'information (affichées sur la page Systèmes d'information et détails des membres)

En-tête de colonne	Valeur du paramètre	Explication
Nom	<code>subsystemName</code>	Nom du sous-système (c'est-à-dire du système d'information). Ajouté manuellement à Répertoire par l'administrateur du sous-système spécifique. S'il n'est pas saisi pour le sous-système spécifique, le code du sous-système est affiché à la place.
Code	<code>_identifierEnd</code>	Code d'un sous-système. Récupéré à partir de la configuration globale.
Propriétaire	<code>_memberName</code>	Nom du membre propriétaire du sous-système. Récupéré à partir de la configuration globale.
Services	<code>_services</code>	Le nombre total de services du sous-système.
Première découverte	<code>_dateOfFirstDiscovery</code>	Date à laquelle les données du sous-système ont été stockées dans Répertoire pour la première fois.
Dernière découverte	<code>_dateOfLastUpdate</code>	Date de la dernière mise à jour des données du sous-système dans Répertoire.

En-tête de colonne	Valeur du paramètre	Explication
État	<code>_status</code>	Affiche si le sous-système est <i>ACTIF</i> ou <i>INACTIF</i> . Un sous-système est considéré comme <i>INACTIF</i> lorsqu'il a déjà existé, mais que Répertoire ne l'a pas retrouvé lors de la dernière mise à jour (par exemple, le sous-système a été supprimé).

Tableau 4. Colonnes disponibles dans le tableau des services (affichées sur les pages Services, Détails des membres et Détails du système d'information)

En-tête de colonne	Valeur du paramètre	Explication
Nom	<code>__name</code>	Nom d'un service. Recueilli à partir du serveur de sécurité de son propriétaire. Si aucune entrée n'est effectuée pour le service spécifique, le code de service et la version (si disponible) s'affichent à la place.
Identifiant du service	<code>identifier</code>	Identifiant UXP complet du service. Recueilli à partir du serveur de sécurité de son propriétaire.
Code de service	<code>_identifierEnd</code>	Code d'un service. Recueilli à partir du serveur de sécurité de son propriétaire.
Système d'information	<code>_subsystemName</code>	Nom du sous-système (c'est-à-dire le système d'information) où se trouve le service. Ajouté manuellement à Répertoire par l'administrateur du sous-système spécifique. S'il n'est pas saisi pour le sous-système spécifique, le code du sous-système est affiché à la place.
Propriétaire	<code>_memberName</code>	Nom du membre propriétaire du service. Récupéré à partir de la configuration globale.
Dernière découverte	<code>_dateOfLastUpdate</code>	Date à laquelle les données du service ont été mises à jour pour la dernière fois dans Répertoire.
Première découverte	<code>_dateOfFirstDiscovery</code>	Date à laquelle les données du service ont été stockées pour la première fois dans Répertoire.
État	<code>_status</code>	Indique si le service est <i>ACTIF</i> , <i>INACTIF</i> ou <i>NON DISPONIBLE</i> . Un service est considéré comme <i>INACTIF</i> lorsqu'il a déjà existé, mais que Répertoire ne l'a pas trouvé lors de la dernière mise à jour (par exemple, le service a été supprimé par son propriétaire). Le service est considéré comme <i>NON DISPONIBLE</i> lorsque le service a déjà existé, mais qu'il n'est pas possible d'établir une connexion avec le serveur de sécurité.
Type de service	<code>_serviceType</code>	Type de service. Soit <code>SOAP_SERVICE</code> ou <code>REST_API</code> .

1. Modifiez la section **displayedColumns** du fichier de configuration pour modifier les

colonnes des tableaux suivants :

- tableau des membres (paramètre : *members*) ;
  - affiché sur la page Membres ;
- tableau des systèmes d'information (*subsystems*) ;
  - affiché sur la page Systèmes d'information ;
- tableau des services (*services*) ;
  - affiché sur la page Services.

```
"displayedColumns": {
  "members": ["__name", "_identifierEnd", "_dateOfFirstDiscovery"],
  "subsystems": ["subsystemName", "_memberName", "_identifierEnd"],
  "services": ["__name", "_identifierEnd", "_dateOfLastUpdate", "_status"]
}
```

2. Modifiez la section **embeddedColumns** du fichier de configuration pour changer les colonnes des tableaux suivants :

- page des détails des membres (paramètre : *members*) ;
  - tableau des systèmes d'information intégrés (paramètre : *subsystems*) ;
    - colonnes affichées dans le tableau Systèmes d'information de la page Détails du membre.
  - tableau des services intégrés (paramètre *services*) ;
    - colonnes affichées dans le tableau Services de la page Détails du membre.
- Page de détails du système d'information (paramètre : *subsystems*) ;
  - tableau des services intégrés (paramètre : *services*) ;
    - colonnes affichées dans le tableau Services de la page Détails du sous-système.

```
"embeddedColumns": {
  "members": {
    "subsystems": ["subsystemName", "_services", "_identifierEnd"],
    "services": ["__name", "_subsystemName", "_status"]
  },
  "subsystems": {
    "services": ["__name", "_subsystemName", "_status"]
  }
}
```



Si la section **embeddedColumns** ou certains de ses paramètres sont manquants dans la configuration, les paramètres et leurs valeurs de la section **displayedColumns** sont utilisés à la place.



**displayedColumns** est une section obligatoire !





La modification de **displayedColumns** et **embeddedColumns** peut entraîner des tailles incorrectes pour les colonnes du tableau. Ce problème sera résolu dans une prochaine version.

### 3.2.7. Désactiver certaines pages

Répertoire UXP permet de désactiver des pages du menu latéral et de les rendre inaccessibles.

Tableau 5. Pages de Répertoire UXP pouvant être désactivées

Titre de la page	Suffixe de page
Membres	/members
Systèmes d'information	/subsystems
Services	/services
Visualisation d'instance	/visualization
Instance Données ouvertes	/data
Page détaillée d'un membre/système d'information/service spécifique	Le suffixe est formé à partir de l'identifiant UXP (voir <a href="#">Formes valides des identifiants UXP</a> ) du membre, du système d'information ou du service spécifique. Par exemple, /EE/GOV/12345678



Il n'est pas possible de masquer la page du tableau de bord.



Bien qu'il soit possible de masquer la page de détails d'un membre, d'un système d'information ou d'un service spécifique, les suffixes de ces pages peuvent toujours être lus à partir du fichier de configuration accessible au public.

1. Ajoutez une section **guards** au fichier de configuration.
2. Ajoutez le suffixe de la page que vous souhaitez rendre inaccessible en tant que contenu de la section.

```
"guards": ["/visualization", "/data"]
```



Si une chaîne vide est fournie à la propriété guards ("guards": [""]), toutes les pages, à l'exception du tableau de bord, sont inaccessibles.

### 3.2.8. Désactiver les statistiques du tableau de bord

Il est possible de désactiver les statistiques de surveillance affichées sur la page Tableau de bord de Répertoire UXP.



Cette action ne masque pas le nombre de membres, de sous-systèmes et de services affichés dans le système Répertoire UXP.

- Modifiez la section **dashboardMonitoringStatistics** du fichier de configuration.

```
"dashboardMonitoringStatistics": false,
```

### 3.2.9. Désactiver les statistiques de surveillance de la vue détaillée

Il est possible de masquer les onglets de statistiques affichés sur la page de détails d'un membre, d'un sous-système ou d'un service.

- Modifiez la section **detailsMonitoringStatistics** du fichier de configuration.

```
"detailsMonitoringStatistics": false,
```

## 3.3. Modifier les paramètres de configuration

Pour modifier une valeur dans la configuration de Répertoire UXP, modifiez le fichier de configuration `/etc/uxp/directory/directory.ini`. Tous les paramètres système disponibles, ainsi que les sections dans lesquelles ils se trouvent, sont décrits dans les tableaux ci-dessous.

#### [common]

Champ	Valeur par défaut	Explication
instance <sup>[1,2,3]</sup>		L'instance UXP, dont les entités sont exposées par le Répertoire.
master-node <sup>[1,3]</sup>	true	Indique si ce nœud de Répertoire est maître ou non.
metaservice-client-class <sup>[1,2]</sup>		Classe de membre du client du serveur de sécurité hébergeant le service du Répertoire.
metaservice-client-code <sup>[1,2]</sup>		Code membre du client du serveur de sécurité hébergeant le service du Répertoire.
metaservice-client-subsystem <sup>[1,2]</sup>		Code du sous-système du client du serveur de sécurité hébergeant le service du Répertoire.
security-server-host <sup>[1,2]</sup>		Hébergeur du serveur de sécurité que le Répertoire utilise pour récupérer les données.

Champ	Valeur par défaut	Explication
security-server-port <sup>[1,2]</sup>	80/443	Port du serveur de sécurité, par défaut 80 pour HTTP et 443 pour HTTPS.
security-server-tls-cert-file <sup>[1,2]</sup>		Nom du fichier (chemin absolu) du certificat TLS du serveur de sécurité. Obligatoire en cas d'utilisation d'une connexion TLS.
security-server-use-tls <sup>[1,2]</sup>	true	Si la communication avec le serveur de sécurité utilise TLS.
security-server-verify-hostname <sup>[1,2]</sup>	false	Indique si le client HTTP du serveur de sécurité doit vérifier le nom d'hôte du serveur en cas d'utilisation de la connexion TLS.

### [updater]

Champ	Valeur par défaut	Explication
entity-cron-expression <sup>[1]</sup>	0 0 0/6 1/1 * ? *	Expression CRON <a href="#">[CRON]</a> pour la mise à jour des entités, la valeur par défaut est une fois toutes les 6 heures.
failed-update-unavailable-threshold	4	Seuil à partir duquel les services sont marqués comme « Non disponibles » après un certain nombre de tentatives de mise à jour infructueuses. L'intervalle réel dépend de l'horaire configuré de <i>entity-cron-expression</i> .
open-data-batch-size <sup>[1]</sup>	10000	Le nombre d'enregistrements de données ouvertes à télécharger, en lot.
open-data-cleaner-cron-expression <sup>[1]</sup>	0 0 0/12 1/1 * ? *	Expression CRON <a href="#">[CRON]</a> pour supprimer les données ouvertes obsolètes, la valeur par défaut est toutes les 12 heures.
open-data-cron-expression <sup>[1]</sup>	0 0 0/1 1/1 * ? *	Expression CRON <a href="#">[CRON]</a> pour la mise à jour des données ouvertes, par défaut toutes les heures.

Champ	Valeur par défaut	Explication
open-data-offset-days <sup>[1,2]</sup>	10	L'âge, en jours, des données ouvertes les plus récentes à télécharger.
open-data-window-days <sup>[1,2]</sup>	30	Nombre de jours pendant lesquels les données ouvertes doivent être conservées.
operation-delay-seconds <sup>[1]</sup>	0	Délai en secondes entre les mises à jour pour l'équilibrage de charge.
statistics-cron-expression <sup>[1]</sup>	0 0 3 * * ? *	Expression CRON <a href="#">[CRON]</a> pour la mise à jour des statistiques, par défaut tous les jours à 3 heures du matin.
visualization-cron-expression <sup>[1]</sup>	0 0 0/4 1/1 * ? *	Expression CRON <a href="#">[CRON]</a> pour la mise à jour des données du visualiseur.
visualization-data-offset-days <sup>[1]</sup>	1	L'âge, en jours, des données les plus récentes à visualiser.
visualization-data-window-days <sup>[1]</sup>	10	Nombre de jours de données à visualiser.

## [backend]

Champ	Valeur par défaut	Explication
open-data-preview-limit <sup>[2]</sup>	100	Limite du nombre d'enregistrements de données ouvertes pouvant être prévisualisés sur l'interface Web.
visualization-graph-node-radius <sup>[2]</sup>	20	La taille, en pixels, du plus petit nœud du graphique de visualisation.
wSDL-cache-expire-seconds <sup>[2]</sup>	3600	Expiration du cache WSDL en secondes.

## [elasticsearch]

Champ	Valeur par défaut	Explication
address <sup>[1]</sup>		L'hôte ou l'adresse IP du serveur Elasticsearch. Obligatoire.

Champ	Valeur par défaut	Explication
ca-cert-file <sup>[1]</sup>		Le nom de fichier (chemin absolu) du certificat de l'autorité de certification d'Elasticsearch (au format PEM ou DER). Obligatoire en cas d'utilisation du schéma <a href="https://www.elastic.co/guide/en/elasticsearch/reference/current/https.html">https</a> . Répertoire a besoin de ce certificat d'autorité de certification pour vérifier les certificats TLS des nœuds Elasticsearch lors de l'établissement d'une liaison TLS.
cluster-nodes <sup>[1]</sup>	Liste vide	Liste séparée par des virgules des noms des sections des nœuds de la grappe.
connect-timeout <sup>[1]</sup>	15000	Délai d'expiration de connexion du client HTTP Elasticsearch en millisecondes. Un délai de zéro est interprété comme un délai infini.
index <sup>[1]</sup>	uxp-request*	Index (des données de surveillance opérationnelle) créé par le serveur de surveillance UXP. Le caractère générique (*) dans le nom de l'index permet d'effectuer une recherche dans plusieurs index (par exemple, dans le cas du partitionnement de l'index).
password <sup>[1]</sup>		Le mot de passe de l'utilisateur Elasticsearch pour l'authentification de base.
port <sup>[1]</sup>	9200	Le port sur lequel le serveur Elasticsearch écoute les requêtes.
read-timeout <sup>[1]</sup>	60000	Le délai de lecture du client HTTP d'Elasticsearch en millisecondes (qui est le délai d'attente des données, c'est-à-dire une période maximale d'inactivité entre deux paquets de données consécutifs). Un délai de zéro est interprété comme un délai infini.

Champ	Valeur par défaut	Explication
schema <sup>[1]</sup>	http	Si la communication avec Elasticsearch utilise HTTP ou HTTPS. Les valeurs possibles sont http et https.
username <sup>[1]</sup>		Le nom d'utilisateur Elasticsearch pour l'authentification de base.
verify-hostname <sup>[1]</sup>	false	Si le client HTTP Elasticsearch doit vérifier le nom d'hôte du serveur lors de l'établissement d'une liaison TLS dans le cas où le schéma https est utilisé.



La valeur du paramètre n'est pas validée, il faut donc être prudent lorsque l'on modifie la valeur. Par exemple, si le numéro de port est fixé à une valeur non numérique dans la configuration, le système se bloque.

Un exemple de fichier de configuration est présenté dans [Exemple de fichier de configuration Répertoire](#).



La modification des valeurs des paramètres dans les fichiers de configuration nécessite le redémarrage des services correspondants.

<sup>[1]</sup> uxp-directory-updater - Mise à jour de Répertoire UXP

<sup>[2]</sup> uxp-directory-backend - Backend de Répertoire UXP

<sup>[3]</sup> uxp-directory-service - Service de Répertoire UXP

Par exemple :

```
sudo systemctl restart uxp-directory-updater
```

### 3.3.1. Modifier l'intervalle de mise à jour de Répertoire

Les périodes de mise à jour de Répertoire sont définies par les paramètres du système dans la configuration du serveur de répertoire dans les [fichiers INI \[INI\]](#), (/etc/uxp/directory/directory.ini). Les périodes de mise à jour sont définies comme des expressions CRON [Quartz Scheduler CRON expression](#).

#### Pour modifier la période de mise à jour du serveur de Répertoire UXP

- **entités** — modifiez la valeur du paramètre système `entity-cron-expression`
- **statistiques** — modifiez la valeur du paramètre système `statistics-cron-expression`
- **données ouverts** — modifiez la valeur du paramètre système `open-data-cron-`

expression

- **nettoyeur de données ouvertes** — modifiez la valeur du paramètre système `open-data-cleaner-cron-expression`
- **visualisation** — modifiez la valeur paramètre du système `visualization-cron-expression`

### 3.3.2. Se connecter à Elasticsearch

Pour récupérer les statistiques, vous devez configurer la connexion à Elasticsearch du serveur de surveillance UXP.

Répertoire UXP prend en charge les protocoles HTTP et HTTPS pour communiquer avec Elasticsearch. En outre, l'authentification de base HTTP est prise en charge.

Par défaut, Elasticsearch utilise le port **9200** et l'index Elasticsearch `uxp-request`. Vous pouvez modifier ces valeurs dans le fichier de configuration `/etc/uxp/directory/directory.ini` sous la section `[elasticsearch]` section.

```
[elasticsearch]
address=192.168.56.1
port=9200
scheme=http
index=uxp-request*
```

### Configuration de l'authentification de base dans Répertoire UXP

1. Définissez les valeurs correctes des informations d'identification Elasticsearch pour les paramètres `username` et `password` dans la section `[elasticsearch]` du fichier de configuration `/etc/uxp/directory/directory.ini`. Si la valeur `username` ou `password` est vide, aucune authentification de base n'est utilisée.



L'utilisateur configuré doit disposer au minimum des privilèges `read` et `view_index_metadata` sur l'index Elasticsearch configuré (par défaut `uxp-request*`).

Pour en savoir plus sur l'authentification et les privilèges des utilisateurs, consultez la documentation d'Elasticsearch [\[Elastic-Authorization\]](#).

2. Redémarrez le service de mise à jour de Répertoire :

```
sudo systemctl restart uxp-directory-updater
```

### Configuration de la connexion TLS dans Répertoire UXP

1. Définissez la valeur du paramètre `scheme` sur `https` dans la section `[elasticsearch]` du fichier de configuration `/etc/uxp/directory/directory.ini`.

2. Acquérez auprès d'Elasticsearch le certificat CA utilisé pour émettre et signer les certificats TLS des nœuds Elasticsearch. Répertoire UXP a besoin de ce certificat CA pour vérifier les certificats TLS du nœud Elasticsearch lors de l'établissement d'une connexion TLS.
  - a. Ajoutez le fichier de certificat CA (au format PEM ou DER) dans le dossier `/etc/uxp/directory/ssl`.
  - b. Modifiez le propriétaire, le groupe et les autorisations du fichier ajouté :

```
sudo chown uxp-directory:uxp /etc/uxp/directory/ssl/<CA_CERTIFICATE_FILE_NAME>
sudo chmod 640 /etc/uxp/directory/ssl/<CA_CERTIFICATE_FILE_NAME>
```

où `<CA_CERTIFICATE_FILE_NAME>` est le nom du fichier du certificat CA.

- c. Définissez la valeur du paramètre `ca-cert-file` sur le chemin d'accès absolu du fichier de certificat CA (`/etc/uxp/directory/ssl/<CA_CERTIFICATE_FILE_NAME>`).



Définissez la valeur du paramètre `verify-hostname` sur `true` si le Répertoire UXP doit vérifier le nom d'hôte Elasticsearch pendant l'établissement d'une liaison TLS.

3. Redémarrez le service de mise à jour de Répertoire :

```
sudo systemctl restart uxp-directory-updater
```



Répertoire UXP utilise son certificat TLS auto-signé pour se connecter à Elasticsearch. Ajoutez ce certificat à la liste des certificats de confiance dans Elasticsearch lors de la configuration de l'authentification mutuelle TLS. Voir plus de détails dans la documentation Elasticsearch [\[Elastic-Security\]](#).

### 3.3.3. Haute disponibilité entre plusieurs nœuds Elasticsearch

Si vous utilisez une grappe Elasticsearch à plusieurs nœuds, vous pouvez configurer Répertoire UXP pour qu'il se connecte à plusieurs nœuds Elasticsearch sur la grappe. En cas d'indisponibilité d'un nœud, le Répertoire se connectera de manière transparente à un nœud disponible et continuera à fonctionner. Les requêtes adressées aux hôtes disponibles seront acheminées selon un principe de chacun son tour.

Chaque nœud supplémentaire doit avoir sa propre section avec l'adresse du nœud, le port d'écoute et le schéma. Ces noms de section (séparés par des virgules) doivent être définis comme valeur du champ.

```
[elasticsearch]
address=192.168.56.1
port=9200
scheme=https
ca-cert-file=/etc/uxp/directory/ssl/elastic-ca.crt
username=uxp-directory
```



```
password=*****

index=uxp-request*

cluster-nodes=elasticsearch-node-2, elasticsearch-node-3

[elasticsearch-node-2]
address=192.168.56.2
port=9200

[elasticsearch-node-3]
address=192.168.56.3
port=9200
```

### 3.3.4. Configurer la visualisation des données d'instance

La visualisation des données de l'instance donne un aperçu de la façon dont les services sont utilisés sur l'instance. Le graphique montre les services les plus populaires ainsi que les organisations qui les utilisent.

Les graphiques sont compilés à partir de données collectées dans une fenêtre temporelle donnée. La taille de cette fenêtre et la fréquence de mise à jour des données peuvent être configurées à partir du fichier de configuration `/etc/uxp/directory/directory.ini`.

La section `updater` contient les champs configurables pour la page de visualisation des données. Les données de visualisation sont mises à jour en fonction d'une expression CRON définie par le champ `visualization-cron-expression`.

La fenêtre de données est définie par les champs `visualization-data-offset-days` et `visualization-data-window-days`. Le premier champ fait reculer la fenêtre dans le temps d'un nombre de jours donné, tandis que le second définit le nombre de jours à inclure dans la fenêtre, où les données les plus récentes sont définies par le champ de décalage.

Par exemple :

```
[updater]
visualization-cron-expression=0 0 0/4 1/1 * ? *
visualization-data-offset-days=1
visualization-data-window-days=10
```

Dans la configuration présentée, les données de visualisation sont mises à jour toutes les 4 heures. La fenêtre est de 10 jours et les données les plus récentes datent d'un jour. Par conséquent, les données les plus anciennes datent de 11 jours.

Le graphique de visualisation affiché sur l'interface web comporte des nœuds de différentes tailles. Les tailles sont proportionnelles au nombre de transactions auxquelles ils participent. La limite (en pixels) pour le plus petit nœud de ce type peut être définie à l'aide du champ `visualization-graph-node-radius` dans la section `[backend]` du fichier de configuration `/etc/uxp/directory/directory.ini`.

```
[backend]
visualization-graph-node-radius=20
```

### 3.3.5. Configurer les données ouvertes de l'instance

Le Répertoire permet aux membres du public de télécharger des données ouvertes (les statistiques d'échange de données), à des fins de transparence. Ces données sont stockées dans le Répertoire en fonction d'une fenêtre temporelle configurable.

En raison du nombre de transactions de données qui ont pu être effectuées, le Répertoire stocke les données par lots et les met à jour périodiquement, afin de réguler l'utilisation du réseau.

La taille de la fenêtre et les paramètres de stockage des données peuvent être configurés dans la section `updater` du fichier de configuration `/etc/uxp/directory/directory.ini`.

```
[updater]
open-data-cron-expression=0 0 0/1 1/1 * ? *
open-data-batch-size=10000
open-data-offset-days=10
open-data-window-days=30
open-data-cleaner-cron-expression=0 0 0/12 1/1 * ? *
```

Comme pour le visualiseur de données, la fenêtre de données ouverte est décrite par deux champs : le décalage et la taille de la fenêtre. Le décalage déplace la position de la fenêtre dans le temps, l'âge des données les plus récentes dans la fenêtre étant égal au décalage. La taille de la fenêtre est définie par le champ `open-data-window-days`.

Les données ouvertes sont mises à jour en fonction du champ `open-data-cron-expression` configuré. Les données sont téléchargées dans le Répertoire par lots, dont la taille est définie par `open-data-batch-size`.

Toutes les anciennes informations sont effacées en fonction du champ `open-data-cleaner-cron-expression`.

Le nombre d'enregistrements de données ouvertes pouvant être prévisualisés sur l'interface Web est limité par la valeur `open-data-preview-limit` dans la section `[backend]` du fichier de configuration `/etc/uxp/directory/directory.ini`.

```
[backend]
open-data-preview-limit=100
```

## 3.4. Liste noire

La liste noire est utilisée pour filtrer les transactions des statistiques, des données ouvertes et de la visualisation qui appartiennent à un certain sous-système.

Celles-ci peuvent être filtrées en raison de la nature sensible du sous-système dans la

transaction.

Le fichier de liste noire, situé à `/etc/uxp/directory/blacklist`, contient une liste des sous-systèmes à filtrer au format `INSTANCE/MEMBER-CLASS/MEMBER-CODE/SUBSYSTEM-CODE` (chaque élément sur une ligne distincte). L'instance n'est pas obligatoire, car elle est surtout utile pour les instances UXP fédérées, afin d'identifier les membres de l'instance externe. Si ce champ est laissé vide (le premier « / » de l'identifiant reste obligatoire), le Répertoire utilisera par défaut l'instance UXP locale.

```
EXTERNAL-INSTANCE-1/COM/CLIENT1/SUB1
EXTERNAL-INSTANCE-1/COM/CLIENT2/SUB1

EXTERNAL-INSTANCE-2/ORG/CLIENT1/SUB1

LOCAL-INSTANCE/GOV/CLIENT1/SUB1
/GOV/CLIENT1/SUB2
/COM/CLIENT2/SUB2
```



La liste noire est stockée localement et n'est pertinente que pour le serveur du Répertoire sur lequel elle est stockée. Si l'instance possède plusieurs nœuds de Répertoire (grappe), chaque nœud aura sa propre liste noire qui ne pourra être modifiée que manuellement.

## 4. Ajouter un service de Répertoire au serveur de sécurité

---

Sur le serveur de sécurité :

1. Ajoutez le WSDL des services de Répertoire au fournisseur de services de Répertoire :
  - Le WSDL du service de Répertoire se trouve à l'adresse `https://<directory>:7400/DirectoryService?wsdl`, remplacez `<directory>` par l'adresse réelle du Répertoire.
  - Autorisez la mise en ligne des importations WSDL si cela est demandé.
2. Ajoutez l'accès au groupe global **all-subsystems** pour chacun des quatre services SOAP. Le groupe **all-subsystems** est automatiquement mis à jour lorsqu'un nouveau sous-système est enregistré dans l'instance UXP.
3. Activez le WSDL.

Voir le guide de l'utilisateur du serveur de sécurité [\[UXP-UG-SS\]](#) pour plus de détails et des instructions étape par étape.

Si l'intégration a réussi, la liste des services devrait ressembler à ce qui suit :

```
WSDL (https://<directory>:7400/DirectoryService?wsdl)
  setFields (1)
  getFields (1)
  downloadAttachment (1)
  deleteFields (1)
```

## 5. Dépannage

---

### 5.1. Fichiers journaux

Les fichiers journaux aident à résoudre les erreurs qui surviennent et à détecter d'éventuels comportements inattendus. La lecture des fichiers journaux requiert les privilèges de l'administrateur (root).

- Répertoire UXP écrit les journaux dans les fichiers suivants :
  - `/var/log/uxp-directory/directory-updater-jetty.log` — les informations relatives au service de mise à jour et aux statistiques ;
  - `/var/log/uxp-directory/directory-backend-jetty.log` — les informations relatives au service backend et à l'API REST ;
  - `/var/log/uxp-directory/directory-service-jetty.log` — les informations relatives au service SOAP et à l'interaction avec la CLI.
- Un débogage supplémentaire peut être effectué à l'aide de `systemd journal`, par exemple, `journalctl -u uxp-directory-backend`.

# Annexe A: Configuration de base de l'interface utilisateur pour Répertoire UXP

```
{
  "defaultLanguage": "en",
  "languages": ["en", "ua"],
  "title": {
    "en": "UXP Directory",
    "ua": "Каталог веб-сервісів"
  },
  "navTitle": {
    "en": "UXP Directory",
    "ua": "Каталог веб-сервісів"
  },
  "logos": [
    {
      "imageLarge": "directory-logo.svg",
      "imageSmall": "directory-logo.svg",
      "href": "/"
    },
    {
      "imageLarge": "logo-2-lg.png",
      "imageSmall": "logo-2-sm.png",
      "href": "https://cyber.ee"
    }
  ],
  "entryTranslations": {
    "en": {
      "contact-name": "Contact Name",
      "contact-phone": "Contact Phone Number",
      "contact-email": "Contact Email Address"
    },
    "ua": {
      "contact-name": "Контактне ім'я",
      "contact-phone": "Контактний телефонний номер",
      "contact-email": "Електронна пошта"
    }
  },
  "displayedColumns": {
    "members": ["__name", "_subsystems", "_services", "_identifierEnd"],
    "subsystems": ["_identifierEnd", "_memberName", "_services"],
    "services": ["__name", "_identifierEnd", "_subsystemName", "_memberName"]
  },
  "embeddedColumns": {
    "subsystems": ["subsystemName", "_services", "_identifierEnd"]
  },
  "guards": ["/visualization", "/data"]
}
```

# Annexe B: Schéma JSON de base pour Répertoire UXP

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "type": "object",
  "title": "Directory Entry Basic Schema",
  "additionalProperties": false,
  "definitions": {
    "contacts": {
      "type": "array",
      "items": {
        "additionalProperties": false,
        "type": "object",
        "required": [
          "contact-name",
          "contact-phone",
          "contact-email"
        ],
        "properties": {
          "contact-name": {
            "type": "string"
          },
          "contact-phone": {
            "type": "string"
          },
          "contact-email": {
            "type": "string"
          }
        }
      }
    }
  },
  "documentation": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "managedBy": {
        "type": "string"
      },
      "service-guide": {
        "type": "object",
        "additionalProperties": false,
        "properties": {
          "_file": {
            "type": "object"
          }
        }
      }
    }
  }
}
```

```
    }  
  }  
},  
"properties": {  
  "member": {  
    "type": "object",  
    "additionalProperties": false,  
    "properties": {  
      "contacts": {"$ref": "#/definitions/contacts"}  
    }  
  },  
  "subsystem": {  
    "type": "object",  
    "additionalProperties": false,  
    "properties": {  
      "contacts": {"$ref": "#/definitions/contacts"}  
    }  
  },  
  "service": {  
    "type": "object",  
    "additionalProperties": false,  
    "properties": {  
      "contacts": {"$ref": "#/definitions/contacts"},  
      "documentation": {"$ref": "#/definitions/documentation"}  
    }  
  }  
}  
}
```



# Annexe C: Exemple de fichier de configuration de Répertoire

## [common]

```
master-node=true

instance=EXAMPLE

security-server-host=192.168.56.100
security-server-port=443
security-server-use-tls=true
security-server-verify-hostname=false
security-server-tls-cert-file=/etc/uxp/directory/ssl/security-server.crt

metaservice-client-class=GOV
metaservice-client-code=Management
metaservice-client-subsystem=Directory
```

## [updater]

```
entity-cron-expression=0 0 0/6 1/1 * ? *
statistics-cron-expression=0 0 3 * * ? *
operation-delay-seconds=0

open-data-cron-expression=0 0 0/1 1/1 * ? *
open-data-batch-size=10000
open-data-offset-days=10
open-data-window-days=30
open-data-cleaner-cron-expression=0 0 0/12 1/1 * ? *

visualization-cron-expression=0 0 0/4 1/1 * ? *
visualization-data-offset-days=1
visualization-data-window-days=10

failed-update-unavailable-threshold=4
```

## [backend]

```
visualization-graph-node-radius=20
open-data-preview-limit=100
wsdl-cache-expire-seconds=3600
```

## [elasticsearch]

```
address=192.168.56.1
port=9200
scheme=https
username=uxp-directory
```

```
password=*****
ca-cert-file=/etc/uxp/directory/ssl/elastic-ca.crt

verify-hostname=false

connect-timeout=15000
read-timeout=60000

index=uxp-request*

cluster-nodes=elasticsearch-node-2, elasticsearch-node-3

[elasticsearch-node-2]

address=192.168.56.2
port=9200

[elasticsearch-node-3]

address=192.168.56.3
port=9200
```

# Annexe D: Formes valides des identifiants UXP

---

**Les formes valables des identifiants UXP sont les suivantes :**

- pour les membres : Instance/Member\_Class/Member\_Code ;
- pour les sous-systèmes : Instance/Member\_Class/Member\_Code/Subsystem\_Code ;
- pour les services qui ont une version de service :  
Instance/Member\_Class/Member\_Code/Member/Subsystem\_Code/Service\_Code/Service\_Version ;
- pour les services qui n'ont pas de version de service :  
Instance/Member\_Class/Member\_Code/Member/Subsystem\_Code/Service\_Code.

**Exemples d'identifiants UXP valides :**

- Exemple d'identifiant de membre valide :
  - EE/GOV/12345678.
- Exemple d'identifiant valide de sous-système (c'est-à-dire de système d'information) :
  - EE/GOV/12345678/testSystem.
- Exemple de service valide sans identifiant de code de service :
  - EE/GOV/12345678/testSystem/testService.
- Exemple de service valide avec identifiant de code de service :
  - EE/GOV/12345678/testSystem/testService/2.

# Annexe E: Notes de mise à jour de Répertoire UXP

---

## 2.5.5 (11.2025)

- La version 9.x d'Elasticsearch est désormais prise en charge.

## 2.5.4 (09.2025)

- Amélioration des performances des membres, des vues des systèmes d'information et de la fonction de recherche pour les instances comportant un nombre élevé de membres et de sous-systèmes.
- Correction : les métadonnées des sous-systèmes ne sont pas mises à jour correctement pour Serveur de sécurité v1.24.
- Correction : nombre de membres incorrect dans directory-updater-jetty.log.
- Correction : ne pas afficher le métaservice getSecurityServerOperationalDataStats sur la page de visualisation de l'instance lorsque 'Metaservices: Exclude' est sélectionné.

## 2.5.3 (06.2025)

- Ajout de paramètres de délai d'attente Elasticsearch configurables, amélioration de la journalisation et de la gestion des erreurs.

## 2.5.2 (08.2024)

- Correctifs de localisation.

## 2.5.1 (04.2024)

- Correction des fuites de connexion réseau dans le composant de mise à jour.

## 2.5.0 (06.2023)

- 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.
- Amélioration de la prise en charge d'Elasticsearch.
  - La version 8.x d'Elasticsearch est désormais prise en charge.
  - Remplacement du client Java High Level REST d'Elasticsearch obsolète par le client Java API.



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

- L'historique des journaux système est désormais conservé pendant 60 jours au lieu de 30.
- Java Runtime Environment est mis à jour vers la version 17. Mise à jour d'autres bibliothèques et composants tiers afin de garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

#### 2.4.1 (12.2021)

- Par défaut, les données SNI du client ne sont pas vérifiées pour correspondre au CN et au SAN dans le certificat TLS du serveur.

#### 2.4.0 (11.2021)

- Répertoire vérifie désormais le certificat TLS du serveur de sécurité.
  - Les nouveaux paramètres ajoutés dans le fichier de configuration `directory.ini` sont `security-server-tls-cert-file` et `security-server-verify-hostname`.
- Répertoire prend désormais en charge la connexion TLS et l'authentification de base avec Elasticsearch.
  - Ajout de nouveaux paramètres pour configurer le répertoire en toute sécurité vers Elasticsearch. Les nouveaux paramètres dans le fichier `directory.ini` sont `scheme`, `username`, `password`, `ca-cert-file` et `verify-hostname`.
- Amélioration de la validation des entrées.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections mineures et améliorations de sécurité.

#### 2.3.3 (02.2021)

- La vérification du nom d'hôte pendant l'établissement de la connexion TLS est désactivée dans l'interface CLI de Répertoire.

#### 2.3.2 (01.2021)

- Correction des permissions de Répertoire.

#### 2.3.1 (01.2021)

- Emplacement de configuration de l'interface utilisateur modifié pour éviter les conflits d'autorisation. Lien symbolique créé à l'emplacement précédent.

#### 2.3.0 (01.2021)

- Répertoire est désormais compatible avec UXP 1.14.
- Ubuntu 20.04 LTS est désormais une plate-forme prise en charge (et recommandée).
- Fonctionnalité de recherche améliorée pour les correspondances partielles.
- Les services sont désormais marqués comme étant `Indisponibles` lorsqu'il n'est pas possible d'envoyer des requêtes aux serveurs de sécurité correspondants.
- Répertoire peut désormais afficher des informations supplémentaires provenant des WSDL (`<xs:documentation>`).
- Mises à jour de la documentation concernant l'utilisation du groupe global `all-subsystems` dans les serveurs de sécurité pour faciliter la gestion de l'interface CLI de Répertoire.
- Les bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

### 2.2.0 (04.2020)

- Recherche plein texte améliorée avec correspondance de préfixe.
- Correction de l'indexation des onglets dans la page Détails du service.

### 2.1.1 (02.2020)

- Correction de l'expression cron du paramètre *entity-cron-expression* dans le modèle de configuration du répertoire.
- Correction d'une NPE dans l'analyse WSDL.

### 2.1.0 (01.2020)

- Il est possible de visualiser les échanges de données entre les organisations (qui a communiqué avec qui) à l'aide d'un graphique ou d'une carte thermique.
- Il est possible de télécharger une partie des statistiques sur les échanges de données sous forme de données ouvertes.
- Le Répertoire UXP peut maintenant être installé sur une grappe.
- Il est désormais possible de personnaliser l'interface utilisateur (configuration des colonnes du tableau affichées à l'utilisateur).
- Il est désormais possible de mettre en cache les fichiers WSDL téléchargés.
- La version 7 d'Elasticsearch est désormais prise en charge. Les grappes Elasticsearch sont prises en charge.
- Java Runtime Environment a été mis à jour vers la version 11.

### 2.0 (12.2019)

- Première version du nouveau Répertoire UXP. Le produit a été retravaillé avec une nouvelle interface utilisateur et de nouvelles fonctionnalités.
- Il y a maintenant un tableau de bord qui affiche les principales statistiques de l'installation UXP.
- Les pages d'information sur les membres, les systèmes d'information et les services contiennent désormais un onglet présentant des informations statistiques sur le sujet.
- Les propriétaires de serveurs de sécurité peuvent télécharger des informations supplémentaires, telles que les coordonnées et la documentation de service.
- Ubuntu 18.04 LTS est désormais la plate-forme minimale prise en charge.