

Serveur de registre UXP 1.25

Guide de l'utilisateur

UXP-UG-RS

Table des matières

Dernières notes de mise à jour	1
1. Introduction	2
1.1. Public cible	2
1.2. Concepts UXP	2
1.3. URL importantes	5
1.4. Références	6
2. Gestion des utilisateurs	7
2.1. Rôles des utilisateurs	7
2.2. Gestion des utilisateurs	7
2.3. Verrouillage automatique en cas d'échec des tentatives d'authentification	8
3. Systèmes autonomes et à haute disponibilité	9
3.1. Détection du type de déploiement dans l'interface utilisateur	9
3.2. Vérification de l'état des nœuds de la grappe	9
4. Paramètres du système	10
4.1. Gestion des classes de membres	10
4.2. Configuration d'un fournisseur de services de gestion	10
4.2.1. Désigner un fournisseur de services de gestion	11
4.2.2. Enregistrer le fournisseur de services de gestion en tant que client du serveur de sécurité	11
4.2.3. Configurer les services de gestion sur le serveur de sécurité des services de gestion	12
4.3. Configurer l'adresse du Serveur de registre	12
4.3.1. Notes sur la configuration de la haute disponibilité	13
4.3.2. Changer l'adresse du Serveur de registre	13
4.3.3. Gestion des adresses supplémentaires du serveur de registre	14
5. Gestion globale de la configuration	15
5.1. Visualisation des paramètres de configuration	15
5.2. Télécharger une ancre de configuration	15
5.3. Recréer l'ancre de configuration	15
5.4. Changement des clés de signature de la configuration	16
5.4.1. Génération d'une clé de signature de configuration	17

5.4.2. Activation d'une clé de signature de configuration	18
5.4.3. Suppression d'une clé de signature de configuration	18
5.4.4. Afficher les détails de la clé de signature de la configuration	18
5.4.5. Types de clés	19
5.5. Visualisation du contenu d'une partie de configuration	19
5.6. Téléchargement d'une ancre de confiance	20
5.7. Affichage du contenu d'une ancre de confiance	20
5.8. Supprimer une ancre de confiance	20
6. Le système des demandes de gestion	21
6.1. Demandes d'enregistrement	21
6.1.1. Modèle de machine à états finis pour les demandes d'enregistrement	21
6.2. Demandes de suppression	23
6.3. Affichage des détails des demandes de gestion	23
7. Gestion des membres UXP	25
7.1. Ajouter un membre	25
7.2. Visualisation des détails d'un membre	25
7.3. Ajouter un sous-système à un membre UXP	26
7.4. Enregistrer un serveur de sécurité d'un membre	26
7.5. Enregistrer un client sur un serveur de sécurité	28
7.6. Supprimer un client d'un serveur de sécurité	30
7.7. Modification de l'appartenance globale d'un sous-système membre UXP	31
7.8. Supprimer un sous-système	32
7.9. Supprimer un membre UXP	32
8. Gestion des serveurs de sécurité	33
8.1. Affichage des détails du serveur de sécurité	33
8.2. Changer l'adresse du Serveur de sécurité	33
8.3. Modification du port d'écoute (transport) du serveur de sécurité	34
8.4. Enregistrer un certificat d'un serveur de sécurité	34
8.5. Supprimer un certificat d'un serveur de sécurité	36
8.6. Supprimer un serveur de sécurité	36
9. Gestion des groupes globaux	38
9.1. Ajouter un groupe global	38
9.2. Affichage des détails d'un groupe global	38
9.3. Changer la description d'un groupe global	39

9.4. Changer les membres d'un groupe global	39
9.5. Supprimer un groupe global	39
10. Gestion des services de certification agréés	41
10.1. Ajouter un service de certification agréé	41
10.2. Changer un service de certification agréé	41
10.3. Bloquer un service de certification agréé	42
10.4. Supprimer un service de certification agréé	42
11. Gestion des services d'horodatage approuvés	44
11.1. Ajouter un service d'horodatage approuvé	44
11.2. Changer l'URL d'un service d'horodatage approuvé	44
11.3. Bloquer un service d'horodatage approuvé	44
11.4. Supprimer un service d'horodatage approuvé	45
12. Configuration supplémentaire	46
13. Sauvegarde et restauration de la configuration	49
13.1. Sauvegarde de la configuration du système dans l'interface utilisateur	49
13.2. Restauration de la configuration du système dans l'interface utilisateur	49
13.3. Restauration du serveur de registre à partir d'un fichier de sauvegarde d'un autre serveur de registre	50
13.4. Sauvegarde de la configuration du système à partir de la ligne de commande	51
13.5. Restaurer la configuration du système à partir de la ligne de commande	51
14. Remplacement des certificats TLS	54
15. Surveillance	57
15.1. Configuration de la surveillance	57
15.2. Demande de données de surveillance	58
15.3. Format des fichiers de données de surveillance	58
16. Journaux et services du système	60
16.1. Journaux	60
16.2. Services du système	60
16.3. Configuration de la journalisation	61
16.3.1. Configuration des paramètres de journalisation des composants	62
16.4. Journal d'audit	63
16.4.1. Changer la configuration du journal d'audit	64
16.4.2. Archivage du journal d'audit	64
17. Dépannage	66

17.1. Échec de la signature de la configuration interne – clé active manquante.	66
17.2. La signature de la configuration interne a échoué – le PIN de la clé active n’a pas été saisi	66
17.3. La génération de la configuration globale échoue depuis '<timestamp>'	66
17.4. La génération de l’ancree de configuration interne a échoué : Aucune clé de signature de la configuration n’est configurée	67
17.5. Impossible d’approuver ou de refuser une demande de suppression	67
Annexe A: Notes de mise à jour	68

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 de l'utilisateur s'adresse aux administrateurs des serveurs de registre UXP responsables de la gestion quotidienne des serveurs de registre UXP.

Les instructions pour l'installation et la configuration initiale du logiciel Serveur de registre UXP se trouvent dans Serveur de registre UXP : Guide d'installation et de configuration [\[UXP-IG-RS\]](#).

Les instructions relatives à l'installation du serveur de registre dans une grappe afin d'obtenir une haute disponibilité sont décrites dans le guide Serveur de registre : installation de la haute disponibilité [\[UXP-IG-RSHA\]](#).

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

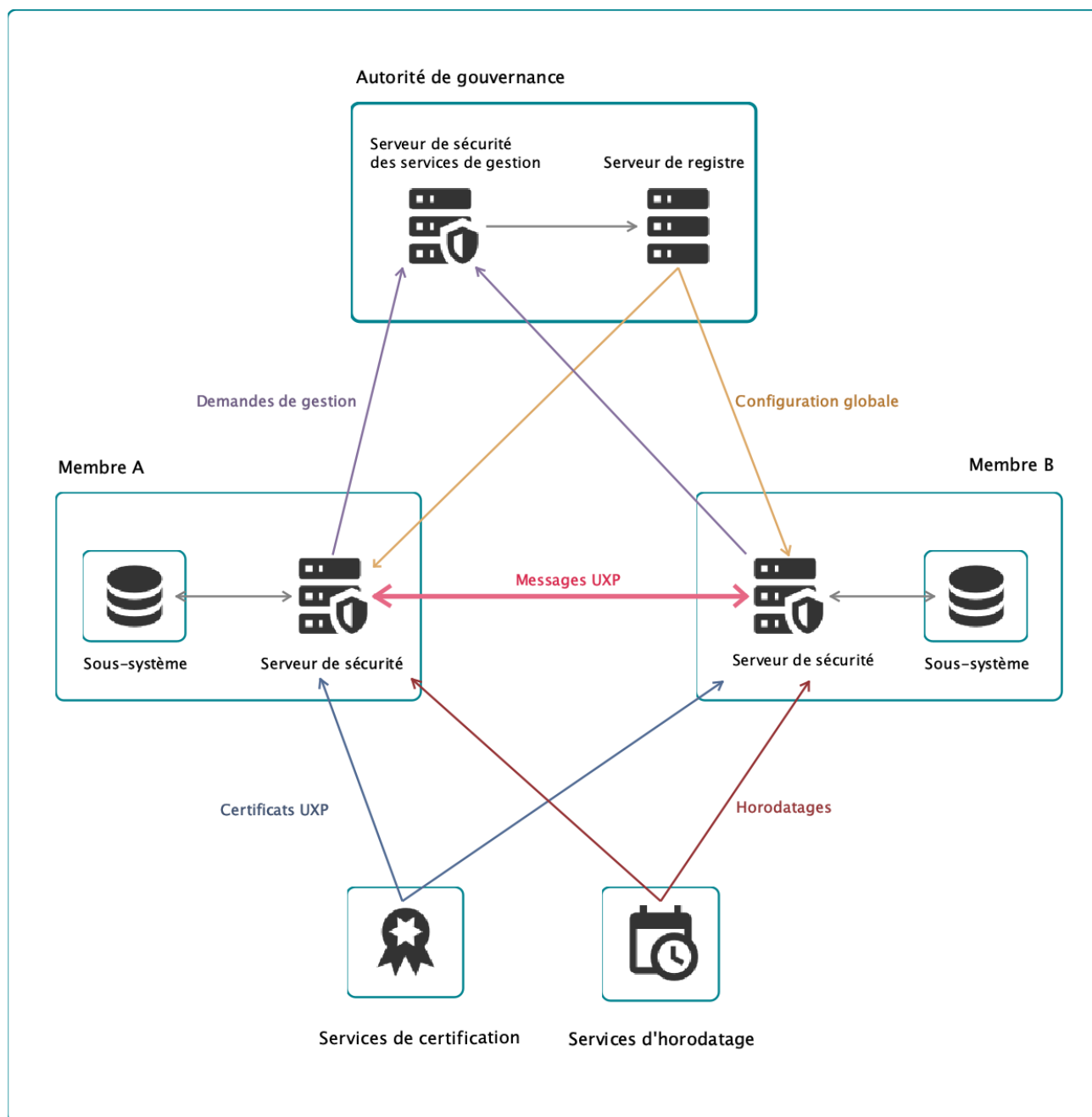


Figure 1. Diagramme montrant les composants d'une instance UXP

1.3. URL importantes

La liste suivante contient les URL les plus couramment utilisées pour interagir avec le serveur de registre.

Dans tous les cas, `<registry-server>` doit être remplacé par l'adresse du serveur de registre.

- **Interface utilisateur de gestion :**

```
https://<registry-server>:4000/
```

- **Configuration interne :**

```
http://<registry-server>/internalconf
```

- **Configuration externe :**

```
http://<registry-server>/externalconf
```

Les URL de configuration sont utilisées par les serveurs de sécurité pour télécharger la configuration globale.

- **Services de gestion :**

```
http://<registry-server>:4400/management-service/
```

- **Services de gestion WSDL :**

```
http://<registry-server>/managementservices.wsdl
```

1.4. Références

- [JSON] Présentation de JSON, <http://json.org/>
- [JSON-SCHEMA] Schéma JSON, <https://json-schema.org/>
- [LOGBACK-PATTERNS] Documentation de Logback. Chapitre 6 : Layouts — Conversion Word Table, <https://logback.qos.ch/manual/layouts.html#conversionWord>
- [NGINX] Nginx – Équilibreur de charge haute performance, serveur Web, & Reverse Proxy, <http://nginx.org/>
- [NIST] Recommandation pour la gestion des clés, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>
- [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-IG-RS] Cybernetica AS. Serveur de registre UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-RS
- [UXP-IG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-SS
- [UXP-SPEC-AL] Cybernetica AS. Événements du journal d'audit UXP Identifiant du document : UXP-SPEC-AL

2. Gestion des utilisateurs

2.1. Rôles des utilisateurs

Le serveur de registre prend en charge les rôles d'utilisateur suivants :

- Le **Responsable d'enregistrement** (uxp-registration-officer) est chargé de traiter les informations relatives aux membres UXP.
- L'**Administrateur système** (uxp-system-administrator) est responsable de l'installation, de la configuration et de la maintenance du serveur de registre.
- Le **Responsable de la sécurité** (uxp-security-officer) est chargé de l'application de la politique de sécurité et des exigences en matière de sécurité.

Un utilisateur peut avoir plusieurs rôles, et plusieurs utilisateurs peuvent remplir le même rôle. Chaque rôle a un groupe système correspondant, créé lors de l'installation du système. Les noms d'utilisateur du système sont utilisés pour se connecter à l'interface utilisateur du serveur de registre.

Le document indique, dans des sections similaires à l'exemple suivant, quel rôle d'utilisateur est requis pour effectuer une action particulière dans l'interface utilisateur. Par exemple

Droits d'accès : Administrateur système



Si l'utilisateur connecté ne dispose pas des privilèges nécessaires pour effectuer une tâche, le bouton qui déclenche l'action est masqué (et il n'est pas non plus possible d'exécuter la tâche à l'aide des combinaisons de touches ou des actions de souris correspondantes). Seules les informations et actions autorisées sont visibles et disponibles pour l'utilisateur.

2.2. Gestion des utilisateurs

Droits d'accès : privilèges de l'utilisateur root

Lors de l'installation, un super utilisateur doté de tous les rôles est créé. Vous pouvez créer des utilisateurs supplémentaires qui ont des droits restreints. La gestion des utilisateurs s'effectue avec les privilèges de l'utilisateur root à l'aide de la ligne de commande.

Pour ajouter un nouvel utilisateur, exécutez la commande suivante :

```
adduser <username>
```

Pour accorder des privilèges à l'utilisateur que vous avez créé, ajoutez-le aux groupes système correspondants, par exemple :

```
adduser <username> uxp-registration-officer
adduser <username> uxp-system-administrator
adduser <username> uxp-security-officer
```

Pour supprimer les privilèges d'un utilisateur, retirez-le du groupe système correspondant, par exemple :

```
deluser <username> uxp-registration-officer
```

Les privilèges de l'utilisateur ne sont appliqués qu'après le redémarrage du service uxp-jetty (voir la section [Journaux et services système](#)).

Pour supprimer un utilisateur, entrez :

```
deluser <username>
```

2.3. Verrouillage automatique en cas d'échec des tentatives d'authentification

Droits d'accès : privilèges de l'utilisateur root

Le serveur de registre limite les tentatives d'authentification des utilisateurs après un certain nombre d'échecs consécutifs.

Par défaut, l'utilisateur est bloqué pendant 10 minutes après trois échecs consécutifs d'authentification en l'espace de 15 minutes. Ces paramètres et d'autres peuvent être modifiés dans le fichier `/etc/security/faillock.conf`. Par exemple, pour modifier le nombre de tentatives d'authentification échouées pour déclencher le verrouillage à 5, vous devez décommenter et modifier le paramètre `deny`.

Avant

```
# Deny access if the number of consecutive authentication failures
# for this user during the recent interval exceeds n tries.
# The default is 3.
# deny = 3
```

Après

```
# Deny access if the number of consecutive authentication failures
# for this user during the recent interval exceeds n tries.
# The default is 3.
deny = 5
```

De même, pour modifier l'intervalle pendant lequel les échecs sont comptés, modifiez le paramètre `fail_interval`. Le paramètre `unlock_time` détermine la durée du verrouillage.

3. Systèmes autonomes et à haute disponibilité

Droits d'accès : privilèges de l'utilisateur root

Le serveur de registre peut être installé et configuré de deux manières :

- Un serveur **autonome**.
- Une grappe de serveurs de registre indépendants (nœuds) offrant une **haute disponibilité** (HA). Dans une configuration HA, le système continue de fonctionner si un ou plusieurs nœuds rencontrent des problèmes ou sont hors service pour des raisons de maintenance.

Dans le cas d'une configuration HA, les modifications apportées aux bases de données de chaque serveur de registre sont répliquées sur les autres nœuds. Toutefois, certains éléments de données (par exemple, les clés de signature de la configuration) ne sont utilisés que sur un nœud particulier. Cette distinction sera explicitement mentionnée tout au long du présent document lorsque cela sera nécessaire.

Dans une configuration HA, si le système est configuré en utilisant différents nœuds en parallèle, l'effet sera similaire à celui de plusieurs personnes mettant à jour en même temps la configuration d'un serveur autonome.

3.1. Détection du type de déploiement dans l'interface utilisateur

Afin de détecter le type de déploiement et le nom du nœud dans la grappe dans le cas d'une configuration HA, l'utilisateur connecté doit vérifier l'identifiant de l'instance affiché dans le coin supérieur gauche de l'interface utilisateur. Dans le cas d'une configuration HA, le nom du nœud est affiché entre parenthèses à droite de l'identifiant de l'instance.

3.2. Vérification de l'état des nœuds de la grappe

Pour vérifier l'état des nœuds dans une configuration HA, le script suivant peut être utilisé dans la ligne de commande :

```
/usr/share/uxp/scripts/check_ha_cluster_status.py
```

4. Paramètres du système

4.1. Gestion des classes de membres

Droits d'accès : Responsable de sécurité

Pour ajouter une classe de membre, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Classes de membre** et cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'ouvre, saisissez le code et la description de la classe de membre. Cliquez sur **OK**.



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

Pour modifier la description d'une classe de membre, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Classes de membre**, sélectionnez une classe de membre et cliquez sur **Modifier**.
3. Dans la fenêtre qui s'ouvre, saisissez la description de la classe de membre et cliquez sur **OK**.

Pour supprimer une classe de membre, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Classes de membre**, sélectionnez une classe de membre et cliquez sur **Supprimer**.

Seules les classes de membre qui ne sont utilisées par aucun des membres de UXP peuvent être supprimées.

4.2. Configuration d'un fournisseur de services de gestion

Le serveur de registre fournit des services de gestion aux serveurs de sécurité qui font partie de l'infrastructure (locale) UXP (voir la section [Le système de demandes de gestion](#)).

Un sous-système d'un membre UXP agissant en tant que fournisseur de services pour les services de gestion doit être :

1. désigné sur le serveur de registre (voir [Désignation du fournisseur de services de gestion](#)) ;
2. enregistré en tant que client du serveur de sécurité des services de gestion (voir [Enregistrement du fournisseur de services de gestion en tant que client du serveur de](#)

sécurité) ;

3. configuré pour fournir les services sur le serveur de sécurité des services de gestion (voir [Configuration des services de gestion dans le serveur de sécurité des services de gestion](#)).

Le serveur de sécurité des services de gestion doit être installé et enregistré sur le serveur de registre avant que le fournisseur de services de gestion puisse être enregistré en tant que client du serveur de sécurité et que les services de gestion puissent être configurés (voir [\[UXP-IG-SS\]](#)).

4.2.1. Désigner un fournisseur de services de gestion

Droits d'accès : Responsable de sécurité

Pour désigner le fournisseur de services de gestion sur le serveur de registre, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Services de gestion** et cliquez sur **Modifier**.
3. Dans la fenêtre qui s'ouvre, recherchez le sous-système d'un membre UXP à désigner comme fournisseur de services de gestion et cliquez sur **OK**.

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

Droits d'accès : Responsable de sécurité

Le fournisseur de services de gestion peut être enregistré en tant que client de serveur de sécurité comme décrit dans cette section uniquement s'il n'est enregistré en tant que client d'aucun 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**.

Pour enregistrer le fournisseur de services de gestion désigné en tant que client du serveur de sécurité des services de gestion, procédez comme suit.

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. Cliquez sur **Soumettre** pour soumettre 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**.

4.2.3. Configurer les services de gestion sur le serveur de sécurité des services de gestion

Droits d'accès : Responsable de services du serveur de sécurité

Les données nécessaires à la configuration des services de gestion sur le serveur de sécurité se trouvent dans la section [URL importantes](#) et sur le serveur de registre dans la section **Gestion → Paramètres système → Services de gestion**.

Pour configurer les services de gestion sur le serveur de sécurité des services de gestion, procédez comme suit.

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.

4.3. Configurer l'adresse du Serveur de registre

Droits d'accès : Responsable de sécurité

Dans la vue Paramètres système, l'adresse DNS publique ou l'adresse IP du serveur de registre s'affiche. Cette adresse est utilisée par les serveurs de sécurité pour accéder aux services fournis par le serveur de registre (téléchargement de la configuration, services de gestion).



Lorsque vous modifiez l'adresse du serveur de registre, veuillez à effectuer toutes les actions suivantes.

Lorsque l'adresse du serveur de registre est modifiée :

- l'adresse des services de gestion sur le serveur de sécurité des services de gestion doit être reconfigurée ;
- l'ancre de configuration interne doit être redistribuée aux administrateurs du serveur de sécurité et aux serveurs de surveillance ;
- l'ancre de configuration externe doit être redistribuée aux partenaires de la fédération.

Les services fournis par le serveur de registre doivent être disponibles à la fois à partir de la nouvelle et de l'ancienne adresse, jusqu'à ce que tous les serveurs utilisant les services aient téléchargé l'ancre de configuration contenant la nouvelle adresse.

4.3.1. Notes sur la configuration de la haute disponibilité

Dans une [configuration de haute disponibilité \(HA\)](#), l'adresse du serveur de registre est locale au nœud en cours de configuration.

Dans une configuration HA, les ancres de configuration internes et externes contiennent des informations sur chaque serveur de registre faisant partie de la grappe. Si l'adresse d'un des serveurs est modifiée, les ancres de configuration seront automatiquement générées à nouveau sur tous les nœuds.

4.3.2. Changer l'adresse du Serveur de registre

Pour changer l'adresse du serveur de registre, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Paramètres du système** et cliquez sur **Modifier**.
3. Saisissez l'adresse du serveur de registre et cliquez sur **OK**.

Lorsque l'adresse est modifiée, le système :

- modifie l'adresse WSDL des services de gestion ;
 - modifie l'adresse des services de gestion ;
 - modifie les adresses sources de configuration ;
 - génère de nouveaux ancrages de configuration pour les sources de configuration internes et externes.
4. Une fois l'adresse du serveur de registre modifiée, procédez comme suit.
 - Téléchargez l'ancre source de configuration interne et distribuez l'ancre ainsi que sa valeur de hachage aux administrateurs du serveur de sécurité de l'infrastructure UXP locale et aux serveurs de surveillance.

- Dans le cas d'instances UXP fédérées, téléchargez l'ancre source de configuration externe et distribuez l'ancre ainsi que sa valeur de hachage aux partenaires de la fédération.
- Reconfigurez les adresses des services de gestion sur le serveur de sécurité des services de gestion.

4.3.3. Gestion des adresses supplémentaires du serveur de registre

Dans un environnement où le serveur de registre se trouve dans plusieurs réseaux physiques ou virtuels que les serveurs de sécurité peuvent utiliser pour télécharger la configuration globale, vous pouvez configurer des adresses supplémentaires.

Pour ajouter une adresse de serveur de registre supplémentaire.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Adresses supplémentaires du serveur de registre** et cliquez sur **Ajouter**.
3. Saisissez l'adresse du serveur de registre supplémentaire et cliquez sur **OK**.

Pour supprimer une adresse de serveur de registre supplémentaire.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Adresses supplémentaires du serveur de registre** et cliquez sur **Supprimer**.

Lorsque des adresses de serveurs de registre supplémentaires sont ajoutées ou supprimées, le système génère de nouvelles ancres de configuration pour les sources de configuration internes et externes.

Après l'ajout ou la suppression d'adresses de serveurs de registre supplémentaires, procédez comme suit.

- Téléchargez l'ancre source de configuration interne et distribuez l'ancre ainsi que sa valeur de hachage aux administrateurs du serveur de sécurité de l'infrastructure UXP locale et aux serveurs de surveillance.
- Dans le cas d'instances UXP fédérées, téléchargez l'ancre source de configuration externe et distribuez l'ancre ainsi que sa valeur de hachage aux partenaires de la fédération.

5. Gestion globale de la configuration

5.1. Visualisation des paramètres de configuration

Droits d'accès : Responsable de sécurité, Administrateur système

La vue **Configuration globale** se compose de trois sections.

- **Configuration interne.** La configuration interne est distribuée par le serveur de registre aux serveurs de sécurité de l'infrastructure UXP locale. Les informations nécessaires au téléchargement et à la vérification de la configuration interne sont incluses dans l'ancre de configuration interne, qui doit être distribuée aux administrateurs des serveurs de sécurité et téléchargée sur les serveurs de sécurité. En plus de l'ancre de configuration interne, la valeur de hachage du fichier d'ancrage doit être distribuée. La valeur de hachage est utilisée par les administrateurs du serveur de sécurité pour vérifier l'intégrité du fichier d'ancrage.
En outre, la configuration interne est utilisée par les serveurs de surveillance.
- **Configuration externe.** La configuration externe est distribuée par le serveur de registre aux partenaires de la fédération (aux serveurs de sécurité). Les informations nécessaires au téléchargement et à la vérification de la configuration externe sont incluses dans l'ancre de configuration externe, qui doit être distribuée à l'administrateur du serveur de registre du partenaire de la fédération et téléchargée sur le serveur de registre. En plus de l'ancre de configuration externe, la valeur de hachage du fichier d'ancrage doit être distribuée. La valeur de hachage est utilisée par les partenaires de la fédération pour vérifier l'intégrité du fichier d'ancrage.
- **Ancres de confiance.** Une ancre de confiance est l'ancre de configuration de la ou des sources de configuration qui distribuent la configuration externe d'un partenaire de la fédération. Lors du chargement de l'ancre de confiance sur le serveur de registre, l'ancre est incluse dans la configuration interne, ce qui permet aux serveurs de sécurité de télécharger la configuration externe d'un partenaire de la fédération ainsi que la configuration interne de l'infrastructure UXP locale.

5.2. Télécharger une ancre de configuration

Droits d'accès : Responsable de sécurité

Pour télécharger une ancre de configuration, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis sélectionnez l'affichage **Configuration interne** ou **Configuration externe**, selon le cas.
2. Dans la section **Ancre**, cliquez sur **Télécharger** et enregistrez le fichier.

5.3. Recréer l'ancre de configuration

Droits d'accès : Responsable de sécurité

Normalement, les ancres de configuration sont générées (et dans une configuration HA, distribuées à chaque nœud) automatiquement par le système en cas de modification des données incluses dans l'ancre (une ou plusieurs adresses de serveur de registre, clés de signature). La recréation d'une ancre n'est nécessaire que pour la restauration suite à des situations d'erreur.

Pour recréer une ancre, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis sélectionnez l'affichage **Configuration interne** ou **Configuration externe**, selon le cas.
2. Dans la section **Ancre**, cliquez sur **Recréer**.

5.4. Changement des clés de signature de la configuration

Droits d'accès : Responsable de sécurité

Le changement des clés peut être de deux types :

- **changement régulier** – la clé est changée périodiquement (par exemple, chaque année) afin de minimiser le risque d'exposition ;
- **changement d'urgence** – la clé et toutes ses copies de sauvegarde ont été détruites ou la clé a été exposée.

Comme le changement de clé doit être effectué efficacement sans perturber le fonctionnement de l'UXP, la procédure se déroule en deux étapes, au cours desquelles l'ancienne clé et la nouvelle clé peuvent coexister.

Notez que dans une configuration HA, chaque nœud possède son propre ensemble de clés de signature de configuration. L'ancienne et la nouvelle clé peuvent exister en parallèle sur chaque nœud. Le changement régulier des clés doit concerner tous les nœuds d'une grappe et la nouvelle ancre de configuration doit être distribuée sur chaque nœud après que les clés ont été changées.

Les étapes du changement de clé sont les suivantes :

- Tout d'abord, une nouvelle clé est générée (sur chaque nœud dans les configurations HA) et l'ancre de configuration contenant la ou les parties de la clé publique est distribuée aux participants UXP. Tant que tous les participants n'ont pas reçu la ou les clés publiques, l'ancienne clé (c'est-à-dire la clé actuelle) est utilisée pour signer la configuration.
- Ensuite, une fois que tous les participants ont reçu et téléchargé la ou les nouvelles clés publiques, l'ancienne ou les anciennes clés sont retirées et la ou les nouvelles clés sont utilisées pour signer la configuration.

Pour effectuer un **changement de clé régulier**, procédez comme suit.

1. Générez, mais n'activez pas, une nouvelle clé de signature de configuration (voir [Génération d'une clé de signature de configuration](#)) (dans une configuration HA, pour chaque nœud).

Le système utilise la ou les anciennes clés (actives) pour signer la configuration. Lors de la génération d'une nouvelle clé, le système génère une nouvelle ancre pour les sources de configuration correspondantes.

2. Téléchargez l'ancre (voir [Téléchargement d'une ancre de configuration](#)) contenant la ou les parties de la clé publique de la ou des nouvelles clés de signature.

Distribuez l'ancre ainsi que la valeur de hachage du fichier d'ancrage soit aux administrateurs du serveur de sécurité et aux serveurs de surveillance (dans le cas d'une ancre de configuration interne), soit aux partenaires de la fédération (dans le cas d'une ancre de configuration externe).

3. Activez la ou les nouvelles clés de signature (voir [Activation d'une clé de signature de configuration](#)).

La ou les nouvelles clés de signature ne doivent être activées que lorsque tous les administrateurs des serveurs concernés ont reçu et téléchargé l'ancre distribuée. Les serveurs de registre utilisent la clé active pour signer la configuration. Si un administrateur de serveur n'a pas téléchargé l'ancre de configuration contenant la partie publique de la nouvelle clé avant l'activation de celle-ci, la vérification de la configuration téléchargée dans les serveurs de sécurité échouera et l'échange de services avec les participants UXP décrit dans la configuration sera interrompu.

4. Supprimez l'ancienne clé de signature (dans une configuration HA, supprimez les anciennes clés sur tous les nœuds) (voir [Suppression d'une clé de signature de configuration](#)).

Lors de la suppression d'une clé, le système génère une nouvelle ancre de configuration.

5. Téléchargez l'ancre générée (elle ne contient pas la ou les parties publiques de l'ancienne ou des anciennes clés de signature).

Distribuez l'ancre ainsi que la valeur de hachage du fichier d'ancrage soit aux administrateurs du serveur de sécurité et aux serveurs de surveillance (dans le cas d'une ancre de configuration interne), soit aux partenaires de la fédération (dans le cas d'une ancre de configuration externe).

Pour effectuer un **changement de clé d'urgence**, la nouvelle clé doit être activée et l'ancienne clé effacée immédiatement après la génération de la nouvelle clé (dans les étapes décrites ci-dessus, l'étape 2 est ignorée). L'ancre de configuration distribuée aux administrateurs des serveurs de sécurité et aux serveurs de surveillance (en cas d'ancre de configuration interne) ou aux partenaires de la fédération (en cas d'ancre de configuration externe) ne doit contenir que la partie clé publique de la nouvelle clé de signature.

5.4.1. Génération d'une clé de signature de configuration

Droits d'accès : Responsable de sécurité

Pour générer une clé de signature de la configuration, procédez comme suit.

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 périphérique de clé, un type de clé approprié, insérez une étiquette pour la clé et cliquez sur **OK**. Pour plus d'informations sur les différents types de clés, voir [Types de clés](#).
4. 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).

5.4.2. Activation d'une clé de signature de configuration

Droits d'accès : Responsable de sécurité

Pour activer une clé de signature de la configuration, procédez comme suit.

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**, sélectionnez une clé inactive et cliquez sur **Activer**.

5.4.3. Suppression d'une clé de signature de configuration

Droits d'accès : Responsable de sécurité

Pour supprimer une clé de signature de configuration, procédez comme suit.

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**, sélectionnez une clé inactive et cliquez sur **Supprimer**.
3. Confirmez la suppression en cliquant sur **Confirmer**.

5.4.4. Afficher les détails de la clé de signature de la configuration

Droits d'accès : Responsable de sécurité

Pour afficher les détails d'une clé de signature de configuration, procédez comme suit.

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**, sélectionnez la clé appropriée et cliquez sur **Détails**.

Les informations suivantes s'affichent à propos de la clé :

- **ID du dispositif** — nom du jeton utilisé pour générer la clé.
- **ID clé** — l'identifiant de la clé.
- **Étiquette de clé** — l'étiquette saisie lors de la génération de la clé.
- **Algorithme de clé** — l'algorithme utilisé pour générer la clé.
- **Taille de la clé** — la taille d'une clé RSA. S'affiche uniquement pour les clés dont l'algorithme est RSA.
- **Nom de la courbe** — nom de la courbe elliptique. S'affiche uniquement pour les clés dont l'algorithme est EC.

5.4.5. Types de clés

Pour générer une clé de signature de configuration sur un jeton logiciel ou matériel, le serveur de registre prend en charge deux algorithmes à courbe elliptique (EC) et l'algorithme RSA avec deux longueurs de clé différentes :

- NIST P-384 (également connu sous le nom de `secp384r1` ou `prime384v1`) ;
- NIST P-521 (également connu sous le nom de `secp521r1` ou `prime521v1`) ;
- RSA (3072) ;
- RSA (4096) ;

Pour tous les algorithmes, la taille de la clé publique détermine à la fois la sécurité des clés et la rapidité d'exécution des opérations avec la clé. Les clés plus longues sont plus sûres mais plus lentes à effectuer des opérations.

Tous les types de clés utilisés par le serveur de registre sont approuvés par le National Institute of Standards and Technology (NIST) [pour être sûrs au-delà de l'année 2030 \[NIST\]](#).

Lorsque vous choisissez un type de clé pour une nouvelle clé, tenez compte des conseils donnés par l'autorité de gouvernance de votre UXP.

5.5. Visualisation du contenu d'une partie de configuration

Droits d'accès : Responsable de sécurité, Administrateur système

Le contenu d'une partie de configuration peut être consulté en téléchargeant le fichier de configuration correspondant.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis sélectionnez l'affichage **Configuration interne** ou **Configuration externe**, selon le cas.
2. Dans la section **Parties de configuration**, sélectionnez une partie de configuration et cliquez sur **Télécharger**.
3. Enregistrez ou ouvrez le fichier demandé.

5.6. Téléchargement d'une ancre de confiance

Droits d'accès : Responsable de sécurité

Pour télécharger une ancre de confiance, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis la vue **Ancre de confiance**.
2. Cliquez sur **Télécharger une ancre**, recherchez l'ancre de configuration externe reçu d'un partenaire de fédération, puis cliquez sur **OK**.
3. Vérifiez l'intégrité du fichier d'ancrage en comparant la valeur de hachage du fichier d'ancrage affichée avec la valeur de hachage fournie par le partenaire de la fédération et confirmez le téléchargement de l'ancre en cliquant sur **Confirmer**.

Si une ancre précédente du même partenaire de la fédération a été téléchargée dans le système, la nouvelle ancre remplacera l'ancienne.

5.7. Affichage du contenu d'une ancre de confiance

Droits d'accès : Responsable de sécurité, Administrateur système

Le contenu d'une ancre de confiance peut être consulté en téléchargeant le fichier de l'ancre.

Pour télécharger un fichier d'ancrage, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis la vue **Ancre de confiance**.
2. Dans la section des ancres, cliquez sur **Télécharger**.
3. Enregistrez ou ouvrez le fichier demandé.

5.8. Supprimer une ancre de confiance

Droits d'accès : Responsable de sécurité

Pour supprimer un fichier d'ancrage, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis la vue **Ancre de confiance**.
2. Dans la section des ancres, cliquez sur **Supprimer**.
3. Confirmez la suppression en cliquant sur **Confirmer**.

6. Le système des demandes de gestion

6.1. Demandes d'enregistrement

L'enregistrement des associations auprès de l'autorité de gouvernance UXP étant critique en termes de sécurité, les mesures suivantes sont appliquées pour renforcer la sécurité :

- La demande d'enregistrement doit être soumise à l'autorité de gouvernance UXP par deux canaux, ou en d'autres termes, le souhait d'enregistrement doit être exprimé par le biais de deux **demandes complémentaires** :
 - Une demande est soumise au serveur de registre via UXP à partir du serveur de sécurité.
 - Une autre demande est soumise à l'autorité de gouvernance UXP par des moyens indépendants de la plate-forme UXP (par exemple, par un courrier électronique signé numériquement). Cette demande doit être formalisée sur le serveur de registre par l'administrateur du serveur de registre.
- L'association doit être approuvée par l'autorité de gouvernance UXP.

Les types de demandes d'enregistrement sont les suivants :

- demande d'enregistrement du certificat d'authentification (voir la section [Enregistrement du certificat d'un serveur de sécurité](#)) et
- demande d'enregistrement du client du serveur de sécurité (voir la section [Enregistrement d'un client auprès d'un serveur de sécurité](#)).

6.1.1. Modèle de machine à états finis pour les demandes d'enregistrement

Une demande d'enregistrement peut se trouver dans l'un des états suivants. Voir la [Figure 2](#) pour le diagramme de la machine à états finis.

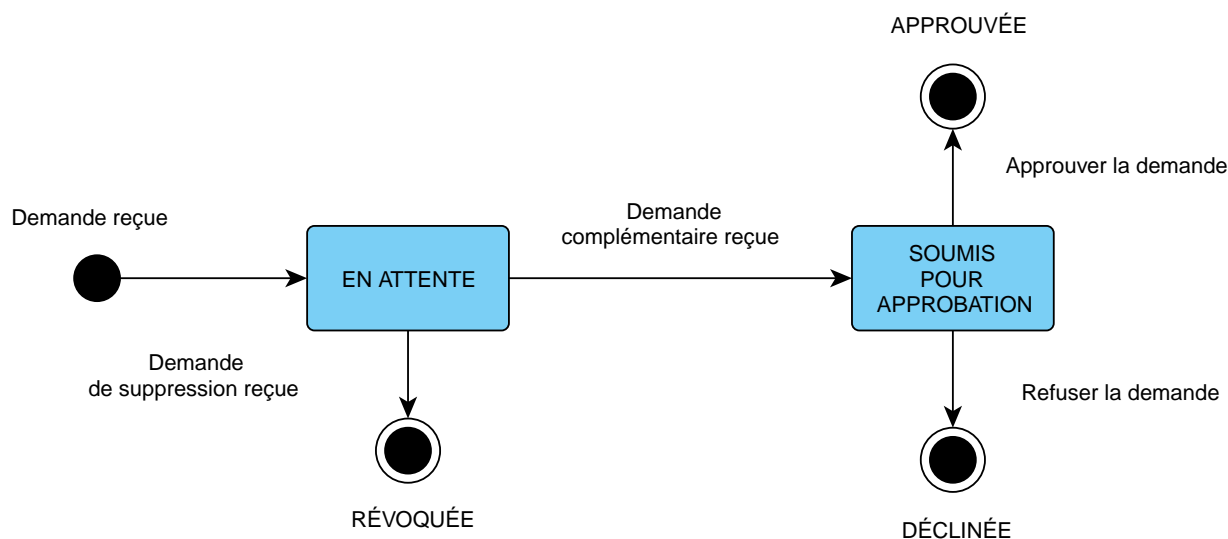


Figure 2. Diagramme d'état pour les demandes d'enregistrement

En attente – une demande d'enregistrement a été soumise par un serveur de sécurité ou formalisée sur le serveur de registre, mais la demande complémentaire n'a pas été soumise. À partir de cet état, la demande peut passer aux états suivants.

- « Soumise pour approbation », si la demande complémentaire est reçue (voir [Enregistrement du serveur de sécurité d'un membre](#), [Enregistrement d'un client sur un serveur de sécurité](#) et [Enregistrement du certificat d'un serveur de sécurité](#)).
- « Révoquée ».
 - Les demandes d'enregistrement reçues d'un serveur de sécurité sont automatiquement révoquées par des demandes de suppression envoyées par le serveur de sécurité ayant une demande d'enregistrement pour même objet.
 - La demande d'enregistrement formalisée sur le serveur de registre peut être révoquée par l'administrateur du serveur de registre sur celui-ci (voir [Enregistrement du serveur de sécurité d'un membre](#), [Enregistrement d'un client sur un serveur de sécurité](#) et [Enregistrement du certificat d'un serveur de sécurité](#)). Une demande de suppression ayant le même objet que celui ayant été soumis pour enregistrement avec la demande d'enregistrement est créée lors de la révocation.

Soumise pour approbation – les deux demandes complémentaires ont été soumises au serveur du registre, mais l'association entre les objets de la demande d'enregistrement n'a pas été approuvée. À partir de cet état, la demande peut passer aux états suivants.

- « Approuvée », si la demande d'enregistrement est approuvée sur le serveur de registre (voir [Enregistrement du serveur de sécurité d'un membre](#), [Enregistrement d'un client auprès d'un serveur de sécurité](#) et [Enregistrement du certificat d'un serveur de sécurité](#)).
- « Refusée », si la demande d'enregistrement est refusée par le serveur de registre (voir [Enregistrement du serveur de sécurité d'un membre](#), [Enregistrement d'un client sur un serveur de sécurité](#) et [Enregistrement du certificat d'un serveur de sécurité](#)).

Approuvée – les demandes d'enregistrement complémentaires ont été approuvées. L'association entre les objets de la demande d'enregistrement a été créée.

Refusée – les demandes d'enregistrement complémentaires ont été refusées.

Révoquée – une demande d'enregistrement a été révoquée.

6.2. Demandes de suppression

Les demandes complémentaires ne sont pas nécessaires pour les demandes de suppression d'association. Les associations sont supprimées sur la base d'une demande unique, qui est soit soumise par l'intermédiaire d'un serveur de sécurité, soit formalisée sur le serveur de registre.

Les types de demandes de suppression sont les suivants :

- demande de suppression du certificat d'authentification (voir la section [Suppression du certificat d'un serveur de sécurité](#)) et
- demande de suppression d'un client du serveur de sécurité (voir la section [Suppression d'un client d'un serveur de sécurité](#)).

6.3. Affichage des détails des demandes de gestion

Droits d'accès : Responsable d'enregistrement

Pour ouvrir la vue détaillée, procédez comme suit.

1. Dans le menu principal, sélectionnez **Gestion**, puis **Demandes de Gestion**.
2. Sélectionnez une demande dans le tableau et double-cliquez dessus ou cliquez sur **Détails**.

La vue comporte trois sections de données.

1. Informations sur la demande :

- ID de la demande – identifiant de la demande ;
- Reçue – la date et l'heure de l'enregistrement de la demande sur le serveur de registre ;
- Source – la source de la demande. La demande peut être soumise par l'intermédiaire d'un serveur de sécurité (SECURITY_SERVER) ou créée dans le serveur de registre (REGISTRY) ;
- État (uniquement pour les demandes d'enregistrement) – l'état de la demande, voir [Figure 2](#) ;
- ID de demande complémentaire/révoquée (uniquement pour les demandes d'enregistrement) – identifiant de la demande qui a entraîné le changement d'état de cette demande de « En attente » à « Soumise pour approbation » ou de « En attente » à « Révoquée » ;

- Commentaires – l'événement source pour la génération automatique de la demande.
Par exemple, lorsqu'un serveur de sécurité est supprimé du serveur de registre, des demandes de suppression sont automatiquement générées pour tous les clients et certificats enregistrés pour ce serveur de sécurité. Dans le champ **Commentaires** des demandes générées, un commentaire avec l'identifiant du serveur est ajouté dans ce cas. Ce champ est laissé vide pour les demandes qui ne sont pas générées automatiquement par le serveur de registre.

2. Informations sur le serveur de sécurité associé à la demande :

- Nom du propriétaire – nom du propriétaire du serveur de sécurité (membre UXP) ;
- Classe du propriétaire – classe de membre du propriétaire du serveur de sécurité ;
- Code du propriétaire – code membre du propriétaire du serveur de sécurité ;
- Code serveur – le code du serveur de sécurité ;
- Adresse – l'adresse du serveur de sécurité. Ce champ n'est rempli que pour les demandes d'enregistrement de certificats d'authentification soumises via un serveur sécurisé.
- Port d'écoute — le port d'écoute (de transport) du serveur de sécurité. Ceci n'est inclus que pour les demandes d'enregistrement de certificats d'authentification envoyées depuis des serveurs de sécurité.

3. Informations sur l'objet de la demande, c'est-à-dire le client ou le certificat à enregistrer ou à supprimer :

- Pour un **client** :
 - Nom – nom du membre UXP qui gère le sous-système ;
 - Classe – la classe du membre UXP qui gère le sous-système ;
 - Code – le code du membre UXP qui gère le sous-système ;
 - Sous-système – le code du sous-système.
- Pour un **certificat** :
 - CA – le nom de l'autorité de certification qui a émis le certificat ;
 - Numéro de série – le numéro de série du certificat ;
 - Objet – tous les attributs du champ `Subject` du certificat ;
 - Expire – la date d'expiration du certificat ;

7. Gestion des membres UXP

7.1. Ajouter un membre

Droits d'accès : Responsable d'enregistrement

Pour ajouter un nouveau membre UXP, suivez les étapes suivantes.

1. Dans le menu **Configuration**, sélectionnez **Membres** et cliquez sur **Ajouter**.
2. Dans la fenêtre qui s'ouvre, saisissez les informations relatives au membre et cliquez sur **OK**. Le nouveau membre apparaît dans la liste des membres.



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

7.2. Visualisation des détails d'un membre

Droits d'accès : Responsable d'enregistrement

Pour ouvrir la vue détaillée, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**.
2. Sélectionnez un membre UXP dans le tableau et double-cliquez dessus ou cliquez sur **Détails**.

La vue se compose de six sections :

1. **Détails du membre** – affiche la classe, le code et le nom du membre.
2. **Serveurs détenus** – affiche les codes des serveurs détenus par ce membre.



Cliquez sur le code d'un serveur pour ouvrir la vue détaillée du serveur.

3. **Appartenance au groupe global** – affiche des informations sur l'appartenance au groupe du membre ou de ses sous-systèmes.



Cliquez sur le code d'un groupe pour ouvrir la vue détaillée du groupe.

4. **Sous-systèmes** – affiche les codes des sous-systèmes du membre, ainsi que le code du serveur de sécurité dont le sous-système est client. Si un sous-système n'est client d'aucun serveur de sécurité, il est affiché en rouge.



Cliquez sur le code du serveur de sécurité concerné pour ouvrir la vue détaillée du serveur de sécurité.

5. **Serveurs utilisés** – affiche des informations sur les serveurs de sécurité qui fournissent un

service d'hébergement aux sous-systèmes du membre. Les informations suivantes sont affichées : le code du serveur de sécurité hébergeant le sous-système, le code du sous-système hébergé et le nom du propriétaire du serveur de sécurité.



Cliquez sur le code du serveur de sécurité pour ouvrir la vue détaillée du serveur.
Cliquez sur le nom du propriétaire pour ouvrir la vue détaillée du propriétaire.

6. **Demandes de gestion** – affiche toutes les demandes de gestion relatives au membre et aux serveurs de sécurité qui lui appartiennent.



Cliquez sur l'identifiant d'une demande pour ouvrir la vue détaillée de la demande.

7.3. Ajouter un sous-système à un membre UXP

Droits d'accès : Responsable d'enregistrement

Pour ajouter un sous-système à un membre UXP, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez le membre auquel vous souhaitez ajouter un sous-système, puis 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_-].

7.4. Enregistrer un serveur de sécurité d'un membre

Droits d'accès : Responsable d'enregistrement

Pour enregistrer un serveur de sécurité d'un membre UXP, les actions suivantes doivent être effectuées.

- Une demande d'enregistrement de certificat d'authentification doit être envoyée du serveur de sécurité au serveur de registre par l'administrateur du serveur de sécurité ;
- La demande d'enregistrement du certificat d'authentification complémentaire doit être formalisée sur le serveur de registre par l'administrateur du serveur de registre, à la demande du propriétaire du serveur de sécurité.
- Les demandes complémentaires doivent être approuvées par l'administrateur du serveur de registre.

Pour formaliser la demande d'enregistrement d'un serveur de sécurité côté serveur de registre, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez un membre dont vous souhaitez enregistrer le serveur de sécurité et cliquez sur **Détails**.

2. Dans la fenêtre qui s'ouvre, sélectionnez la section **Serveurs détenus** et cliquez sur **Ajouter**.
3. Saisissez le code du serveur de sécurité à enregistrer sur le formulaire d'enregistrement.



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

4. Cliquez sur **Télécharger** et localisez le fichier du certificat d'authentification du serveur de sécurité.
5. Cliquez sur **Soumettre** pour soumettre 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 ») et 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 requête soumise via le serveur de sécurité n'est pas arrivée au serveur de registre au moment où la requête côté serveur de registre est soumise.

Les demandes complémentaires sont dans l'état « **Soumise pour approbation** » si la demande soumise via le serveur de sécurité est arrivée au serveur de registre au moment où la demande côté serveur de registre est soumise.

Les demandes d'enregistrement dont le statut est « Soumise pour approbation » peuvent être **approuvée** ou **refusée** par l'administrateur du serveur de registre.

Pour approuver une demande

- ouvrez l'une de ses demandes complémentaires dans la vue détaillée et cliquez sur **Approuver**.

Après l'approbation de la demande :

- 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`.

Pour refuser une demande

- ouvrez l'une de ses demandes complémentaires dans la vue détaillée et cliquez sur **Refuser**. En cas de refus d'une demande, les deux demandes complémentaires passent à l'état « Refusée » ;
- notifiez à l'administrateur du serveur de sécurité que la demande a été refusée.

Les demandes d'enregistrement formalisées sur le serveur de registre qui sont dans l'état « **En attente** » peuvent être **révoquées** (par exemple, si la demande a été soumise par erreur).

Pour révoquer une demande, procédez comme suit.

1. Ouvrez une demande d'enregistrement dans l'état « En attente ». Vous pouvez soit :
 - Localisez la demande dans la liste des demandes de gestion : dans le menu principal, cliquez sur **Gestion**, sur **Demandes de gestion**, puis sur **Détails** ;
 - Localisez la demande dans la section **Demandes de gestion** de la vue détaillée de l'objet associé à la demande (serveur de sécurité ou propriétaire du serveur de sécurité).
2. Cliquez sur **Révoquer**. En cas de révocation d'une demande, une demande de suppression correspondant à la demande d'enregistrement est automatiquement générée et la demande d'enregistrement passe à l'état « Révoquée ».

7.5. Enregistrer un client sur un serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Pour enregistrer un sous-système d'un membre UXP en tant que client du serveur de sécurité, les actions suivantes doivent être effectuées.

- Une demande d'enregistrement de certificat d'authentification doit être envoyée du serveur de sécurité au serveur de registre par l'administrateur du serveur de sécurité ;
- La demande d'enregistrement complémentaire du client du serveur de sécurité doit être formalisée sur le serveur de registre par l'administrateur du serveur de registre, à la demande du propriétaire du serveur de sécurité.
- Les demandes complémentaires doivent être approuvées par l'administrateur du serveur de registre.

La demande d'enregistrement du client côté serveur de registre peut être formalisée soit par la vue détaillée du serveur de sécurité, soit par la vue détaillée d'un membre.

Pour formaliser la demande dans la vue détaillée du membre, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez dans la liste le membre qui souhaite enregistrer son sous-système en tant que client du serveur de sécurité, puis cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, ouvrez la section **Serveurs utilisés** et cliquez sur **Ajouter**.
3. Dans le formulaire de demande d'enregistrement qui s'ouvre, procédez comme suit :
 - saisissez le code du sous-système dans la section **Informations sur le client**, dans le champ **Code du sous-système** ;



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

- localisez la section **Informations sur le serveur de sécurité**, cliquez sur **Rechercher** et, dans la fenêtre qui s'ouvre, sélectionnez le serveur de sécurité approprié.

4. Cliquez sur **Soumettre** pour soumettre la demande d'enregistrement.

Pour formaliser la demande dans la vue détaillée du serveur de sécurité, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, sélectionnez dans la liste un serveur de sécurité sur lequel un nouveau client souhaite s'enregistrer, puis cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, localisez la section **Clients** et cliquez sur **Ajouter**.
3. Sur le formulaire de demande d'enregistrement, localisez la section **Informations sur le client**, cliquez sur **Rechercher** et dans la fenêtre qui s'ouvre, sélectionnez les informations sur le déclarant ou saisissez-les manuellement.
4. Cliquez sur **Soumettre** pour soumettre 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 client ») et 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 requête soumise via le serveur de sécurité n'est pas arrivée au serveur de registre au moment où la requête côté serveur de registre est soumise.

Les demandes complémentaires sont dans l'état « **Soumise pour approbation** » si la demande soumise via le serveur de sécurité est arrivée au serveur de registre au moment où la demande côté serveur de registre est soumise.

Les demandes d'enregistrement dont le statut est « Soumise pour approbation » peuvent être **approuvée** ou **refusée** par l'administrateur du serveur de registre.

Pour approuver une demande

- ouvrez l'une de ses demandes complémentaires dans la vue détaillée et cliquez sur **Approuver**.

Après l'approbation de la demande

- les demandes complémentaires passent à l'état « Approuvée ».
- Les informations relatives au serveur de sécurité s'affichent dans la section **Serveurs utilisés** de la vue détaillée du membre dont le sous-système a été enregistré en tant que client.
- les informations relatives au client sont affichées dans la section **Clients** de la vue détaillée du serveur de sécurité auprès duquel le client a été enregistré.
- le client enregistré est ajouté au groupe global `all-subsystems` s'il n'était pas encore membre de ce groupe.

Pour refuser une demande

- ouvrez l'une de ses demandes complémentaires dans la vue détaillée et cliquez sur **Refuser**. En cas de refus d'une demande, ses demandes complémentaires passent à l'état « Refusée » ;
- notifiez à l'administrateur du serveur de sécurité que la demande a été refusée.

Les demandes d'enregistrement formalisées sur le serveur de registre qui sont dans l'état « **En attente** » peuvent être **révoquées** (par exemple, si la demande a été soumise par erreur).

Pour révoquer une demande, procédez comme suit.

1. Ouvrez une demande d'enregistrement dans l'état « En attente ». Vous pouvez soit :
 - localisez la demande dans la liste des demandes de gestion : dans le menu principal, cliquez sur **Gestion**, sur **Demandes de gestion**, puis sur **Détails** ;
 - localisez la demande dans la section **Demandes de gestion** de la vue détaillée de l'objet associé à la demande (serveur de sécurité ou propriétaire du serveur de sécurité), puis cliquez sur l'ID de la demande.
2. Cliquez sur **Révoquer**. En cas de révocation d'une demande, une demande de suppression correspondant à la demande d'enregistrement est automatiquement générée et la demande d'enregistrement passe à l'état « Révoquée ».

7.6. Supprimer un client d'un serveur de sécurité

Droits d'accès : Responsable d'enregistrement

L'association entre un membre UXP et un serveur de sécurité est supprimée par la demande de suppression du client du serveur de sécurité correspondant. La demande peut être soumise via le serveur de sécurité ou sur le serveur de registre.

L'association entre le propriétaire du serveur de sécurité et le serveur de sécurité ne peut pas être supprimée.

La suppression d'un client du serveur de sécurité peut s'effectuer soit dans la vue détaillée du serveur de sécurité, soit dans la vue détaillée d'un membre.

Pour soumettre une demande de suppression d'un client du serveur de sécurité via la vue détaillée d'un membre, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez le membre dont le sous-système doit être supprimé d'un serveur de sécurité et cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, localisez la section **Serveurs utilisés**, sélectionnez l'association entre le sous-système client et le serveur de sécurité, puis cliquez sur **Supprimer**.
3. Vérifiez les informations affichées sur la demande de suppression du client et cliquez sur **Soumettre** pour soumettre la demande.

4. La demande soumise apparaît dans la section **Demandes de gestion** de la vue détaillée du membre et dans la vue de gestion des demandes (dans le menu principal, sélectionnez **Gestion**, puis **Demandes de gestion**).

Pour soumettre une demande de suppression de client de serveur de sécurité via la vue détaillée du serveur de sécurité, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, sélectionnez un serveur de sécurité à partir duquel le client doit être supprimé et cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, localisez la section **Clients**, sélectionnez le sous-système client et cliquez sur **Supprimer**.
3. Vérifiez les informations affichées sur la demande de suppression du client et cliquez sur **Soumettre** pour soumettre la demande.
4. La demande soumise apparaît dans la section **Demandes de gestion** de la vue détaillée du serveur de sécurité et dans la vue de gestion des demandes (dans le menu principal, sélectionnez **Gestion**, puis **Demandes de gestion**).

Quelle que soit la méthode utilisée, si le sous-système supprimé n'est plus enregistré sur aucun serveur de sécurité en tant que client, il sera supprimé du groupe global `all-subsystems`.

7.7. Modification de l'appartenance globale d'un sous-système membre UXP

Droits d'accès : Responsable d'enregistrement

Pour modifier l'appartenance au groupe des sous-systèmes des membres UXP, deux options sont proposées :

- basée sur les membres – utilisez-la si vous devez modifier l'appartenance à un groupe du sous-système d'un membre UXP spécifique. La procédure est décrite dans cette section ;
- basée sur un groupe – utilisez-la si vous devez modifier la composition d'un groupe spécifique. La procédure est décrite dans la section [Ajout d'un groupe global](#).

Pour ajouter le sous-système d'un membre à un groupe global, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez un membre dont vous souhaitez ajouter le sous-système à un groupe global et cliquez sur **Détails**.
2. Dans la vue qui s'ouvre, localisez la section **Appartenance à un groupe global** et cliquez sur **Ajouter**.
3. Sélectionnez le sous-système dans la liste déroulante **Sous-système**. Dans la liste déroulante **Groupe**, sélectionnez le groupe auquel le sous-système du membre doit être ajouté.
4. Cliquez sur **OK**.

Pour supprimer le sous-système d'un membre d'un groupe global, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez un membre dont vous souhaitez supprimer le sous-système d'un groupe global et cliquez sur **Détails**.
2. Dans la vue qui s'ouvre, localisez la section **Appartenance à un groupe global**.
3. Sélectionnez la ligne contenant l'association entre le sous-système et le groupe global et cliquez sur **Supprimer** pour supprimer le sous-système du groupe sélectionné.
4. Dans la fenêtre de confirmation qui s'ouvre, cliquez sur **Confirmer**.

7.8. Supprimer un sous-système

Droits d'accès : Responsable d'enregistrement

Le sous-système d'un membre UXP ne peut être supprimé du serveur de registre que si le sous-système n'est associé à aucun serveur de sécurité, c'est-à-dire s'il n'est enregistré comme client d'aucun serveur de sécurité. Si le sous-système n'est associé à aucun serveur de sécurité, son code est affiché en rouge.

Pour supprimer le sous-système d'un membre UXP, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez un membre dont vous souhaitez supprimer le sous-système et cliquez sur **Détails**.
2. Dans la vue qui s'ouvre, recherchez dans la section **Sous-systèmes** le sous-système que vous souhaitez supprimer et cliquez sur **Supprimer**.



Le bouton **Supprimer** n'est activé que si le sous-système n'est client d'aucun serveur de sécurité.

7.9. Supprimer un membre UXP

Droits d'accès : Responsable d'enregistrement

Lorsqu'un membre UXP est supprimé, les informations relatives à tous les serveurs de sécurité lui appartenant sont également supprimées.

Pour supprimer un membre UXP, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Membres**, sélectionnez un membre que vous souhaitez supprimer et cliquez sur **Détails**.
2. Dans la vue qui s'ouvre, localisez la section **Détails du membre** et cliquez sur **Supprimer**. Dans la fenêtre de confirmation qui s'ouvre, cliquez sur **Confirmer**.

8. Gestion des serveurs de sécurité

8.1. Affichage des détails du serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Pour ouvrir la vue détaillée, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **Serveurs de sécurité**.
2. Choisissez un serveur de sécurité dans le tableau et double-cliquez dessus ou cliquez sur **Détails**.

La vue comprend cinq sections.

- **Détails du serveur de sécurité** – informations sur le serveur et son propriétaire.
- **Clients** – informations sur les clients enregistrés pour ce serveur de sécurité.



Cliquez sur le code d'un client pour ouvrir sa vue détaillée.

- **Certificats d'authentification** – informations sur les certificats d'authentification enregistrés du serveur de sécurité.



Cliquez sur le numéro de série d'un certificat pour ouvrir sa vue détaillée.

- **Demandes de gestion** – liste de toutes les demandes de gestion associées au serveur de sécurité.



Cliquez sur l'identifiant d'une demande pour ouvrir la vue détaillée de la demande.

8.2. Changer l'adresse du Serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Par défaut, l'adresse du serveur de sécurité est fournie dans la demande d'enregistrement du certificat d'authentification envoyée par le serveur de sécurité. L'adresse doit être modifiée si elle n'a pas été définie lors de l'introduction de la demande ou si elle n'est plus valide.

La définition de l'adresse du serveur de sécurité est importante pour plusieurs raisons.

- Les services relayés par un serveur de sécurité sont disponibles dès que l'adresse du serveur de sécurité est définie.
- En enregistrant les adresses des serveurs de sécurité, les clients du service sont assurés de recevoir une réponse à leurs requêtes dans un délai raisonnable, même si le serveur de sécurité relais est surchargé de demandes de service (par exemple, les requêtes

provenant d'adresses appartenant à des serveurs de sécurité enregistrés sont traitées avant celles provenant d'adresses inconnues).

Pour changer l'adresse du serveur de sécurité, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, sélectionnez le serveur de sécurité dont vous souhaitez modifier l'adresse, puis cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, repérez la section **Détails du serveur de sécurité** et cliquez sur **Modifier** à côté du champ **Adresse**.
3. Saisissez l'adresse du serveur de sécurité et cliquez sur **OK**.

8.3. Modification du port d'écoute (transport) du serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Par défaut, le port d'écoute (transport) du serveur de sécurité est indiqué dans la demande d'enregistrement du certificat d'authentification envoyé par le serveur de sécurité. Après l'enregistrement, le port d'écoute est partagé dans la configuration globale. Le port d'écoute doit être modifié s'il n'est plus valide.

Le port d'écoute défini dans le fichier de configuration du serveur de sécurité (/etc/uxp/conf.d/local.ini) doit correspondre au port d'écoute défini pour le serveur de sécurité dans la configuration globale. Si ces deux ports ne correspondent pas, le serveur de sécurité dans le rôle de fournisseur de services ne peut pas se connecter aux autres serveurs de sécurité.

Ainsi, l'administrateur d'un serveur de sécurité peut vous demander de modifier le port d'écoute qui est partagé avec la configuration globale. Pour changer le port, procédez comme suit :

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, sélectionnez le serveur de sécurité dont vous souhaitez modifier le port d'écoute, puis cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, recherchez la section **Détails du serveur de sécurité** et cliquez sur **Modifier** à côté du champ **Port d'écoute**.
3. Entrez le port d'écoute du serveur de sécurité et cliquez sur **OK**.

8.4. Enregistrer un certificat d'un serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Pour enregistrer un certificat d'authentification sur un serveur de sécurité, les actions suivantes doivent être effectuées.

- Une demande d'enregistrement de certificat d'authentification doit être envoyée par l'administrateur du serveur de sécurité au serveur de registre.

- La demande d'enregistrement du certificat d'authentification complémentaire doit être formalisée sur le serveur de registre par l'administrateur du serveur de registre, à la demande du propriétaire du serveur de sécurité.
- Les demandes complémentaires doivent être approuvées par l'administrateur du serveur de registre.

Pour formaliser une demande d'enregistrement de certificat dans le serveur de registre, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, sélectionnez le serveur de sécurité dont vous souhaitez enregistrer le certificat et cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, localisez la section **Certificats d'authentification** et cliquez sur **Ajouter**.
3. Dans le formulaire de demande d'enregistrement qui s'ouvre, cliquez sur **Télécharger** et localisez le fichier de certificat du serveur de sécurité à enregistrer.
4. Cliquez sur **Soumettre** pour soumettre la demande d'enregistrement.

Si la demande est soumise avec succès, un enregistrement correspondant apparaît dans la vue détaillée du serveur et du propriétaire du serveur dans la section **Demandes de gestion** (type de demande « Enregistrement du certificat d'authentification ») et 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 requête soumise via le serveur de sécurité n'est pas arrivée au serveur de registre au moment où la requête côté serveur de registre est soumise.

Les demandes complémentaires sont dans l'état « **Soumise pour approbation** » si la demande soumise via le serveur de sécurité est arrivée au serveur de registre au moment où la demande côté serveur de registre est soumise.

Les demandes d'enregistrement dont le statut est « Soumise pour approbation » peuvent être **approuvée** ou **refusée** par l'administrateur du serveur de registre.

Pour approuver la demande

- Ouvrez la vue détaillée de l'une de ses demandes complémentaires et cliquez sur **Approuver**.

Après avoir approuvé la demande

- les demandes complémentaires passent à l'état « Approuvée » ;
- le certificat enregistré apparaît dans la vue détaillée du serveur de sécurité, dans la section **Certificats d'authentification**.

Pour refuser la demande

- ouvrez l'une de ses demandes complémentaires dans la vue détaillée et cliquez sur

Refuser. En cas de refus d'une demande, ses demandes complémentaires passent à l'état « Refusée » ;

- notifiez à l'administrateur du serveur de sécurité que la demande a été refusée.

Les demandes d'enregistrement formalisées sur le serveur de registre qui sont dans l'état « **En attente** » peuvent être **révoquées** (par exemple, si la demande a été soumise par erreur).

Pour révoquer une demande, procédez comme suit.

1. Ouvrez une demande d'enregistrement dans l'état « En attente ». Vous pouvez soit :
 - localiser la demande dans la liste des demandes de gestion : Dans le menu principal, sélectionnez **Gestion**, cliquez sur **Demandes de gestion**, puis sur **Détails** ou double-cliquez sur la ligne de la demande ;
 - localisez la demande dans la section d'affichage détaillé des **Demandes de gestion du** serveur de sécurité associé à la demande et cliquez sur l'ID de la demande.
2. Cliquez sur **Révoquer**. Une fois révoquée, la demande passe à l'état « Révoquée ».

8.5. Supprimer un certificat d'un serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Un certificat enregistré pour un serveur de sécurité est supprimé lorsqu'une demande de suppression de certificat est reçue pour ce certificat. La demande peut être soumise via le serveur de sécurité ou sur le serveur de registre.

Pour soumettre une demande de suppression de certificat sur le serveur de registre, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, sélectionnez le serveur de sécurité dont vous souhaitez supprimer le certificat et cliquez sur **Détails**.
2. Dans la vue qui s'ouvre, localisez la section **Certificats d'authentification** et cliquez sur **Supprimer**.
3. Vérifiez les informations affichées sur la demande de suppression et cliquez sur **Soumettre** pour soumettre la demande.
4. La demande soumise apparaît dans la section **Demandes de gestion** de la vue détaillée du serveur de sécurité et de son propriétaire, ainsi que dans la vue de gestion des demandes (dans le menu principal, sélectionnez **Gestion**, puis **Demandes de gestion**).

8.6. Supprimer un serveur de sécurité

Droits d'accès : Responsable d'enregistrement

Pour supprimer un serveur de sécurité, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Serveurs de sécurité**, choisissez dans la liste le

serveur de sécurité que vous souhaitez supprimer et cliquez sur **Détails**.

2. Dans la vue qui s'ouvre, localisez la section **Détails du serveur de sécurité** et cliquez sur **Supprimer**. Confirmez l'action en cliquant sur **Confirmer**.

Si le serveur de sécurité à supprimer a des clients ou des certificats enregistrés, des demandes de suppression pour ces associations sont automatiquement générées.

9. Gestion des groupes globaux

Les groupes globaux sont un moyen pratique de gérer simultanément les droits d'accès à un service pour de nombreux sous-systèmes. Les membres du groupe global héritent de tous les droits d'accès accordés au groupe. Cela signifie également que tout nouveau sous-système ajouté au groupe obtient tous les droits d'accès existants accordés au groupe. Les groupes globaux sont visibles sur les serveurs de sécurité de tous les membres UXP.

Le serveur de registre crée et maintient automatiquement deux groupes globaux :

- Propriétaires de serveurs de sécurité (`security-server-owners`) — tous les propriétaires de serveurs de sécurité. Ce groupe est nécessaire au bon fonctionnement de l'infrastructure UXP.
- Tous les sous-systèmes (`all-subsystems`) — tous les sous-systèmes UXP. Lorsqu'un nouveau sous-système rejoint UXP, il est automatiquement ajouté à ce groupe. Ce groupe est utilisé pour donner accès à un service à tous les sous-systèmes qui ont rejoint UXP.

9.1. Ajouter un groupe global

Droits d'accès : Responsable d'enregistrement

Pour ajouter un nouveau groupe global, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **Groupes globaux** et cliquez sur **Ajouter**.
2. Dans la fenêtre qui s'ouvre, saisissez le code et la description du nouveau groupe, puis cliquez sur **OK**. Le nouveau groupe est ajouté à la liste des groupes globaux.



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

9.2. Affichage des détails d'un groupe global

Droits d'accès : Responsable d'enregistrement

Pour afficher les détails d'un groupe global, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **Groupes globaux**.
2. Sélectionnez un groupe global dans le tableau et double-cliquez dessus ou cliquez sur **Détails**.

Dans la vue détaillée du groupe global, une liste des membres du groupe s'affiche. La vue détaillée permet de modifier la description du groupe, de le supprimer et d'ajouter ou de supprimer ses membres.

9.3. Changer la description d'un groupe global

Droits d'accès : Responsable d'enregistrement

Pour modifier la description d'un groupe global, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **GroupeS globaux**.
2. Sélectionnez un groupe global dans le tableau et cliquez sur **Détails**.
3. Dans la vue qui s'ouvre, cliquez sur **Modifier**, modifiez la description du groupe et cliquez sur **OK**.

9.4. Changer les membres d'un groupe global

Droits d'accès : Responsable d'enregistrement

Notez que les membres des groupeS globaux **all-subsystems** et **security-server-owners** sont gérés automatiquement par le serveur de registre et ne peuvent pas être ajoutés ou supprimés manuellement.

Pour ajouter des sous-systèmeS de membreS UXP à un groupe global, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **GroupeS globaux**.
2. Sélectionnez le groupe global dans le tableau et cliquez sur **Détails**.
3. Dans la vue qui s'ouvre, cliquez sur **Ajouter des membreS**.
4. Localisez et sélectionnez un ou plusieurs sous-systèmeS et cliquez sur **Ajouter la sélection**. Vous pouvez également filtrer une sélection de sous-systèmeS à l'aide de la fonction de recherche et les ajouter tous au groupe en cliquant sur **Ajouter tout**.

Pour supprimer des membreS d'un groupe, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **GroupeS globaux**.
2. Sélectionnez le groupe global dans le tableau et cliquez sur **Détails**.
3. Sélectionnez un ou plusieurs sous-systèmeS dans la liste des membreS du groupe et cliquez sur **Supprimer la sélection**. Vous pouvez également filtrer une sélection de sous-systèmeS à l'aide de la fonction de recherche et les supprimer tous du groupe en cliquant sur **Supprimer tout**.
4. Dans la fenêtre de confirmation qui s'ouvre, cliquez sur **Confirmer**.

9.5. Supprimer un groupe global

Droits d'accès : Responsable d'enregistrement

Pour supprimer un groupe global, procédez comme suit.

1. Dans le menu principal, sélectionnez **Configuration**, puis **GroupeS globaux**.

2. Sélectionnez un groupe global dans le tableau et cliquez sur **Détails**.
3. Dans la vue qui s'ouvre, cliquez sur **Supprimer le groupe** et dans la fenêtre de confirmation, cliquez sur **Confirmer**.

10. Gestion des services de certification agréés

10.1. Ajouter un service de certification agréé

Droits d'accès : Administrateur système

Pour ajouter un service de certification, procédez comme suit.

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 délivre (en plus) d'autres certificats, laissez la case vide.
4. Saisissez le nom complet de la classe Java qui décrit le profil de certificat.
La classe Java doit implémenter l'interface
`ee.cyber.uxp.common.certificateprofile.CertificateProfileInfoProvider`.
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**.

10.2. Changer un service de certification agréé

Droits d'accès : Administrateur système

S'il n'est pas possible de modifier le certificat d'autorité de certification du service de certification, il est en revanche possible de

- modifier les paramètres du service ;
- ajouter, modifier et supprimer les services OCSP de l'autorité de certification ;
- ajouter, modifier et supprimer les certificats et les informations de service OCSP des autorités de certification intermédiaires.

Pour modifier un service de certification, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services de certification**.
2. Sélectionnez dans la liste le service de certification que vous souhaitez modifier et cliquez sur **Modifier**.

10.3. Bloquer un service de certification agréé

Droits d'accès : Administrateur système



Le blocage d'un service de certification rendra inutilisables toutes les clés de signature et d'authentification avec des certificats émis par ce service de certification. Si les membres ne disposent pas de clés alternatives provenant d'autres fournisseurs de services de certification, l'échange de messages sera interrompu. De plus, la vérification des signatures de messages dont le certificat du signataire a été émis par ce service de certification échouera sur les serveurs de sécurité.

Pour bloquer un service de certification, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services de certification**.
2. Sélectionnez dans la liste le service de certification approuvé que vous souhaitez bloquer et cliquez sur **Bloquer**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Confirmer**.

Pour débloquer un service de certification, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services de certification**, sélectionnez un service de certification bloqué dans la liste et cliquez sur **Débloquer**.

Vous pouvez également bloquer les autorités de certification intermédiaires liées à un service de certification.

10.4. Supprimer un service de certification agréé

Droits d'accès : Administrateur système



La suppression d'un service de certification rendra inutilisables toutes les clés de signature et d'authentification des certificats émis par ce service de certification. Si les membres ne disposent pas de clés alternatives provenant d'autres fournisseurs de services de certification, l'échange de messages sera interrompu. De plus, la vérification des signatures de messages dont le certificat du signataire a été émis par ce service de

certification échouera sur les serveurs de sécurité.

Pour supprimer un service de certification de la liste des services approuvés, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services de certification**.
2. Sélectionnez dans la liste le service de certification approuvé que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la fenêtre qui s'ouvre, cliquez sur **Confirmer**.

Vous pouvez annuler la suppression en ajoutant à nouveau les informations relatives au service de certification au serveur de registre.

11. Gestion des services d'horodatage approuvés

11.1. Ajouter un service d'horodatage approuvé

Droits d'accès : Administrateur système

Pour ajouter un service d'horodatage approuvé, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services d'horodatage** et cliquez sur **Ajouter**.
2. Dans la fenêtre qui s'ouvre, entrez l'URL du service d'horodatage et cliquez sur **Télécharger** pour localiser le fichier de certificat du service d'horodatage.
3. Vérifiez que vous avez chargé le bon certificat et cliquez sur **OK**. Des informations sur le nouveau service d'horodatage apparaissent dans la liste.



Si le serveur de registre détecte un fournisseur de services d'horodatage qui a déjà été ajouté, il ajoute un numéro au nom du fournisseur pour rendre le nom du service unique.

11.2. Changer l'URL d'un service d'horodatage approuvé

Droits d'accès : Administrateur système

Pour changer l'URL du service d'horodatage, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services d'horodatage**, sélectionnez un service d'horodatage dans la liste et cliquez sur **Modifier**.
2. Dans la fenêtre qui s'ouvre, modifiez l'URL et cliquez sur **OK**.

11.3. Bloquer un service d'horodatage approuvé

Droits d'accès : Administrateur système



Le blocage d'un service d'horodatage empêchera les serveurs de sécurité d'utiliser ce service d'horodatage. Si les membres n'ont pas choisi d'autres services d'horodatage pour leurs serveurs de sécurité, l'échange de messages sera interrompu. En outre, la vérification des horodatages provenant de ce service d'horodatage échouera sur les serveurs de sécurité.

Pour bloquer un service d'horodatage, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services d'horodatage**, sélectionnez un service d'horodatage dans la liste et cliquez sur **Bloquer**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Confirmer**.

Pour débloquent un service d'horodatage, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services d'horodatage**, sélectionnez un service d'horodatage bloqué dans la liste et cliquez sur **Débloquer**.

11.4. Supprimer un service d'horodatage approuvé

Droits d'accès : Administrateur système



Supprimer un service d'horodatage empêchera les serveurs de sécurité d'utiliser ce service d'horodatage. Si les membres n'ont pas choisi d'autres services d'horodatage pour leurs serveurs de sécurité, l'échange de messages sera interrompu. En outre, la vérification des horodatages provenant de ce service d'horodatage échouera sur les serveurs de sécurité.

Pour supprimer un service d'horodatage approuvé, procédez comme suit.

1. Dans le menu **Configuration**, sélectionnez **Services d'horodatage**, sélectionnez un service d'horodatage dans la liste et cliquez sur **Supprimer**.
2. Dans la fenêtre qui s'ouvre, cliquez sur **Confirmer**.

Vous pouvez annuler la suppression en ajoutant à nouveau les informations relatives au service d'horodatage au serveur de registre.

12. Configuration supplémentaire

Droits d'accès : privilèges de l'utilisateur root

Les paramètres de configuration supplémentaires sont définis dans la base de données du serveur de registre, à laquelle on peut accéder à l'aide de l'utilitaire psql en utilisant la commande suivante (le mot de passe de la base de données se trouve à l'adresse /etc/uxp/db.properties) :

```
psql -U uxpreistry -h localhost uxpreistry
```

La valeur par défaut d'un paramètre système peut être remplacée en ajoutant le nom et la valeur du paramètre au tableau system_parameters :

```
INSERT INTO system_parameters (key, value, created_at, updated_at)
VALUES ('parameter_name', 'parameter_value',
(now() at time zone 'utc'), (now() at time zone 'utc'));
```

Pour modifier la valeur d'un paramètre système déjà inséré dans le tableau system_parameters :

```
UPDATE system_parameters
SET value = 'parameter_value', updated_at = (now() at time zone 'utc')
WHERE key = 'parameter_name';
```

Pour rétablir la valeur par défaut d'un paramètre système, supprimez le paramètre du tableau system_parameters :

```
DELETE FROM system_parameters
WHERE key = 'parameter_name';
```



La modification ou la suppression de paramètres système autres que ceux énumérés ci-dessous entraînera un plantage du système.



Il est fortement déconseillé de modifier les valeurs des paramètres système, car cela pourrait entraîner un comportement inattendu du système.

Les paramètres définissant les algorithmes sont les suivants :

1. confHashAlgoUri– URI de l'algorithme utilisé pour calculer les valeurs de hachage des fichiers de configuration globale. Les valeurs possibles sont

- <http://www.w3.org/2001/04/xmlenc#sha256>,
 - <http://www.w3.org/2001/04/xmlenc#sha512> (par défaut).
2. `confSignDigestAlgoId` – Identifiant de l'algorithme de hachage utilisé pour signer la configuration globale. Les valeurs possibles sont :
- SHA-256,
 - SHA-384,
 - SHA-512 (par défaut).
3. `confSignCertHashAlgoUri` – URI de l'algorithme utilisé pour calculer la valeur de hachage du certificat utilisé pour signer la configuration globale. Les valeurs possibles sont :
- <http://www.w3.org/2001/04/xmlenc#sha256>,
 - <http://www.w3.org/2001/04/xmlenc#sha512> (par défaut).
4. `securityServerAuthCertHashAlgoUri` – URI de l'algorithme utilisé pour calculer la valeur de hachage des certificats d'authentification des serveurs de sécurité. Les valeurs possibles sont :
- <http://www.w3.org/2000/09/xmldsig#sha1>,
 - <http://www.w3.org/2001/04/xmldsig-more#sha224>,
 - <http://www.w3.org/2001/04/xmlenc#sha256>,
 - <http://www.w3.org/2001/04/xmldsig-more#sha384>,
 - <http://www.w3.org/2001/04/xmlenc#sha512> (par défaut).

Les valeurs distribuées aux serveurs de sécurité via la configuration globale sont définies par les paramètres suivants :

1. `ocspFreshnessSeconds` – Si la valeur `nextUpdate` n'est pas présente dans la dernière réponse OCSP, spécifie la durée (en secondes) pendant laquelle les réponses OCSP pour un certificat de signature restent valides après avoir été récupérées auprès du répondeur OCSP. Les réponses OCSP antérieures à la période de validité sont considérées comme expirées et ne peuvent pas être utilisées pour la vérification du certificat.

Ce paramètre détermine également l'intervalle entre les appels du répondeur OCSP pour la signature des certificats. Pour garantir un rafraîchissement suffisamment fréquent des réponses OCSP, l'intervalle d'appel du répondeur OCSP est fixé à `ocspFreshnessSeconds/10` (avec la restriction que l'intervalle d'appel du répondeur ne peut être inférieur à 5 secondes). La valeur par défaut est de 28 800 secondes (8 heures).

2. `authOcspFreshnessSeconds` – Si la valeur `nextUpdate` n'est pas présente dans la dernière réponse OCSP, spécifie la durée (en secondes) pendant laquelle les réponses OCSP pour un certificat d'authentification restent valides après avoir été récupérées auprès du répondeur OCSP. Les réponses OCSP antérieures à la période de validité sont considérées comme expirées et ne peuvent pas être utilisées pour la vérification du certificat.

Ce paramètre détermine également l'intervalle entre les appels de réponse OCSP pour les

certificats d'authentification. Pour garantir un rafraîchissement suffisamment fréquent des réponses OCSP, l'intervalle d'appel du répondeur OCSP est fixé à `authOcspFreshnessSeconds/10` (avec la restriction que l'intervalle d'appel du répondeur ne peut être inférieur à 5 secondes). La valeur par défaut est de 28 800 secondes (8 heures).

3. `timeStampingIntervalSeconds` – Définit l'intervalle d'horodatage des appels de service. Intervalle en secondes après lequel les enregistrements du journal des messages doivent être horodatés. L'intervalle doit être compris entre 60 et 86 400 secondes.



Cette valeur doit être inférieure à `ocspFreshnessSeconds`. La valeur par défaut est de 60 secondes.

Le paramètre définissant la durée de validité de la configuration globale est le suivant :

- `confExpireIntervalSeconds` – Durée en secondes de la validité de la configuration après sa création. La valeur par défaut est de 259 200 secondes (72 heures).

13. Sauvegarde et restauration de la configuration

Le serveur de registre sauvegarde

- la base de données (à l'exception du tableau `schema_migrations` et du schéma de la base de données) et
- les répertoires `/etc/uxp/` et `/etc/nginx/sites-enabled/`.

13.1. Sauvegarde de la configuration du système dans l'interface utilisateur

Droits d'accès : Administrateur système

Pour sauvegarder la configuration, procédez comme suit.

1. Dans le menu **Gestion**, sélectionnez **Sauvegarde et restauration**.
2. Cliquez sur **Sauvegarder la configuration** pour lancer le processus de sauvegarde.
3. Une fenêtre s'ouvre et affiche les résultats du script de sauvegarde ; cliquez sur **OK** pour la fermer.
4. Une fois cette opération effectuée, le fichier de sauvegarde de la configuration et la valeur de hachage correspondante apparaissent dans la liste des fichiers de sauvegarde de la configuration.

Vous pouvez soit conserver le fichier de sauvegarde sur le serveur de registre, soit le télécharger pour le stocker hors du serveur de registre.

13.2. Restauration de la configuration du système dans l'interface utilisateur

Droits d'accès : Administrateur système



Veillez noter que le processus de restauration entraînera la déconnexion du jeton de sécurité sur lequel la clé de signature de la configuration globale est stockée. Après la restauration, vous devez saisir le code PIN du jeton dans l'interface utilisateur du serveur de registre.

Pour restaurer la configuration, procédez comme suit.

1. Dans une **configuration HA**, vous devez vous assurer que les **autres nœuds** de la grappe de serveurs de registre ne provoquent aucune modification de la base de données au cours du processus de restauration. Pour ce faire, arrêtez le service `uxp-jetty` sur tous les autres nœuds avant de restaurer la configuration du système :

```
sudo systemctl stop uxp-jetty
```

2. Dans le menu **Gestion** du serveur de registre que vous allez restaurer, sélectionnez **Sauvegarder et restaurer**.
3. Choisissez un fichier dans la liste des fichiers de sauvegarde.
4. Cliquez sur **Restaurer**.
5. Cliquez sur **Confirmer** pour continuer.
6. Une fenêtre s'ouvre et affiche les résultats du script de restauration ; cliquez sur **OK** pour la fermer.
7. Saisissez le code PIN du jeton de sécurité.
8. Dans une **configuration HA**, après une restauration réussie, redémarrez le service `uxp-jetty` sur tous les **autres nœuds** :

```
sudo systemctl start uxp-jetty
```



Dans les rares cas où le mot de passe de la base de données a changé depuis la création de la sauvegarde, le processus de restauration aboutira à une erreur `Server not responsive` et l'interface utilisateur peut devenir indisponible. Pour résoudre ce problème, accédez au CLI et redémarrez le processus `uxp-jetty` :

```
sudo systemctl restart uxp-jetty
```

13.3. Restauration du serveur de registre à partir d'un fichier de sauvegarde d'un autre serveur de registre

Droits d'accès : Administrateur système

Pour restaurer un serveur de registre à partir d'un fichier de sauvegarde d'un autre serveur, procédez comme suit dans la vue **Sauvegarder et restaurer** des serveurs de registre :

1. [Sauvegardez la configuration](#) du serveur de registre que vous souhaitez utiliser pour restaurer un autre serveur de registre.
2. Télécharger le fichier de sauvegarde.
3. Enregistrez le hachage du fichier de sauvegarde téléchargé afin de vérifier ultérieurement que le fichier n'a pas été modifié pendant le processus de transfert.
4. Téléchargez le fichier de sauvegarde sur l'autre serveur de registre.
5. Si vous avez enregistré la valeur de hachage du fichier de sauvegarde avant de le télécharger à partir du premier serveur, comparez-la à celle calculée lors du téléchargement.
Si les hachages diffèrent, le fichier a été modifié. Il est fortement déconseillé de restaurer le serveur de registre à partir d'un fichier de sauvegarde dont les modifications sont inconnues.

6. [Restaurez le serveur de registre cible](#) à partir du fichier de sauvegarde téléchargé.

13.4. Sauvegarde de la configuration du système à partir de la ligne de commande

Droits d'accès : privilèges de l'utilisateur root

Le processus de sauvegarde créera un fichier contenant toute la configuration du serveur de registre. Vous pouvez ensuite utiliser le fichier pour restaurer l'état du serveur de registre au moment de la sauvegarde.

Pour créer un fichier de sauvegarde pour un serveur de registre, utilisez la commande :

```
sudo -u uxp /usr/share/uxp/scripts/backup_uxp_registry_configuration.sh -i <instance-ID> \
[-n <node-name>] -f <backup-file-location-and-name>
```

Vous pouvez utiliser le dossier `/var/lib/uxp/backup/` pour stocker des fichiers de sauvegarde.

Par exemple (sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/backup_uxp_registry_configuration.sh -i AA \
-f /var/lib/uxp/backup/rs_backup_`date +%Y%m%d-%H%M%S` .tar
```

Le script calcule et renvoie le hachage (digest) du fichier de sauvegarde. Enregistrez le hachage pour vérifier ultérieurement que le fichier de sauvegarde n'a pas été modifié.

13.5. Restaurer la configuration du système à partir de la ligne de commande

Droits d'accès : privilèges de l'utilisateur root

Pour restaurer la configuration à partir de la ligne de commande, les données suivantes doivent être disponibles :

- l'identifiant d'instance du serveur de registre ;
- un fichier de sauvegarde du serveur de registre et
- **dans la configuration HA**, le nom du nœud du serveur de registre.

Si le fichier de sauvegarde ne se trouve pas sur le serveur, déplacez-le d'abord du stockage externe vers le serveur. Vous pouvez le placer dans le répertoire `/var/lib/uxp/backup/`. Définissez les bons privilèges pour le fichier avec `sudo chown uxp:uxp <path-to-backup-file>`.



Veuillez noter que le processus de restauration entraînera la déconnexion du jeton de sécurité dans lequel la clé de signature de la configuration globale est stockée. Après la

restauration, vous devez saisir le code PIN du jeton dans l'interface utilisateur du serveur de registre.



Comparez le hachage (digest) calculé à celui calculé lors de la création de la sauvegarde afin de vous assurer que le fichier n'a pas été modifié.
Il est fortement déconseillé de restaurer le serveur de registre à partir d'un fichier de sauvegarde dont les modifications sont inconnues.

Utilisez la commande suivante pour restaurer la configuration dans une **configuration non-HA** :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh -i <instance-ID> \
-f <backup-file-location-and-name>
```

Dans une **configuration HA**, vous devez vous assurer que les autres nœuds de la grappe de serveurs de registre ne provoquent aucune modification de la base de données au cours du processus de restauration. Pour ce faire, arrêtez le service `uxp-jetty` sur tous les autres nœuds avant de restaurer la configuration du système :



```
sudo systemctl stop uxp-jetty
```

Après une restauration réussie, redémarrez le service `uxp-jetty` sur tous les autres nœuds :

```
sudo systemctl start uxp-jetty
```

Dans une **configuration HA**, cette commande comporte un paramètre obligatoire supplémentaire, le nom du nœud :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh -i <instance-ID> \
-n <node-name> -f <backup-file-location-and-name>
```

Par exemple (tous sur une seule ligne, configuration non-HA) :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh -i AA \
-f /var/lib/uxp/backup/rs_backup_20140707-200916.tar
```

Par exemple (sur une seule ligne, configuration HA) :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh -i AA -n node_0 \
-f /var/lib/uxp/backup/rs_backup_20140707-200916.tar
```

S'il est absolument nécessaire de restaurer le système à partir d'une sauvegarde effectuée sur un autre serveur de registre, le mode forcé de la commande de restauration peut être

utilisé avec l'option `-F`. Par exemple (sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh -F \  
-f /var/lib/uxp/backup/rs_backup_20140707-200916.tar
```

14. Remplacement des certificats TLS

Droits d'accès : privilèges de l'utilisateur root

Lors de l'installation, un certificat TLS interne et un certificat TLS Nginx sont générés pour le serveur de registre.

Le certificat TLS interne est utilisé pour la communication HTTPS avec les serveurs de sécurité.

Le [serveur Web Nginx \[NGINX\]](#) est utilisé pour afficher l'interface utilisateur du serveur de registre et le certificat TLS Nginx est utilisé pour la communication HTTPS entre le navigateur Web de l'utilisateur et Nginx.

Voici quelques-unes des situations qui nécessitent le remplacement d'un certificat :

- changement d'hôte ou d'adresse IP du serveur de registre ;
- la clé privée du certificat est compromise ;
- le certificat nécessite un nouvel algorithme cryptographique différent.

Pour remplacer l'un ou l'autre certificat ultérieurement, utilisez le script `generate_certificate.sh`.

Utilisation du script :

```
Usage: /usr/share/uxp/scripts/generate_certificate.sh -n <basename> -s "<certificate DN>"
[-a "<subjectAltName>"|-f] [-d <path>] [-p] [-c] [-2|-3|-4|-e <EC>]
```

Generate ssl certificate (by default NIST P-256).

OPTIONS:

```
-h      Show this message
-n      basename, like 'internal' or 'nginx'
-d      working/output directory. default is /etc/uxp/ssl
-m      multiple certs generation support (cert is generated to the '<basename>-<epoch-
millis>' sub directory)
-f      fill subjectAltName automatically from hostname and IP addresses
-S      fill Subject with /CN=${HOST} value
-s      subject, optional. Format "/C=EE/O=Company/CN=server.name.tld"
-x      extension basename, like 'internal' or 'nginx', defaults to basename value
-a      subjectAltName, optional. Format
"DNS:serverAlt.name.tld,IP:1.1.1.1,IP:2.2.2.2"
-p      generate .p12 also, friendly name and password will default to basename value
-c      configuration directory containing openssl.cnf
-2      generate 2k RSA key
-3      generate 3k RSA key
-4      generate 4k RSA key
-e      generate EC key. Possible values: 'p256' (NIST P-256 aka secp256r1), 'p384'
```

(NIST P-384 aka secp384r1), 'p521' (NIST P-521 aka secp521r1)

Génération du certificat TLS Nginx

Utilisez l'option `-n nginx` pour indiquer que vous générez le certificat TLS Nginx.

L'option `-m` ne doit pas être utilisée pour le certificat TLS Nginx.

L'un des paramètres `-s` ou `-S` est obligatoire. L'option `-S` remplit le champ Objet avec le nom de l'hôte. Utilisez `-s` si vous souhaitez remplir vous-même le champ Objet (voir la description des options pour connaître le format correct).

`-a` prend en charge un nombre illimité de noms DNS et/ou d'adresses IP (voir la description des options pour connaître le format correct).

Le répertoire de travail/sortie par défaut (`/etc/uxp/ssl`) convient pour générer le certificat TLS Nginx.

Exemple d'exécution du script :

```
sudo /usr/share/uxp/scripts/generate_certificate.sh -n nginx -s <subject> \
-a <subjectAltName>
```

Une fois le nouveau certificat TLS Nginx généré, le service `nginx` doit être rechargé :

```
sudo systemctl reload nginx
```

Génération d'un certificat TLS interne

Utilisez l'option `-n internal` pour spécifier que vous générez le certificat TLS interne.

L'option `-m` ne doit pas être utilisée pour le certificat TLS interne.

L'un des paramètres `-s` ou `-S` est obligatoire. L'option `-S` remplit le champ Objet avec le nom de l'hôte. Utilisez `-s` si vous souhaitez remplir vous-même le champ Objet (voir la description des options pour connaître le format correct).

`-a` prend en charge un nombre illimité de noms DNS et/ou d'adresses IP (voir la description des options pour connaître le format correct).

L'option `-p` doit être utilisée pour le certificat TLS interne.

Le répertoire de travail/sortie par défaut (`/etc/uxp/ssl`) convient pour générer le certificat TLS interne.

Exemple d'exécution du script :

```
sudo /usr/share/uxp/scripts/generate_certificate.sh -n internal -s <subject> \
-a <subjectAltName> -p
```

Après la génération d'un nouveau certificat TLS interne, le service uxp-jetty doit être rechargé :

```
sudo systemctl reload uxp-jetty
```

15. Surveillance

Droits d'accès : privilèges de l'utilisateur root

La solution de surveillance standard du serveur de registre utilise le serveur de surveillance UXP et Zabbix (voir [\[UXP-IG-MS\]](#)).

Le serveur de surveillance récupère périodiquement les paramètres spécifiques à UXP auprès du serveur de registre (en récupérant un fichier JSON disponible à l'adresse suivante : `https://<registry-server>:4001/monitoring/data.json`), vérifie la disponibilité et la validité de la configuration globale du serveur de registre et envoie toutes les informations de surveillance collectées à Zabbix. Actuellement, le serveur de registre surveille et expose uniquement un paramètre spécifique à UXP : l'existence du fichier de licence UXP (paramètre `license_file_exists`). D'autres paramètres seront ajoutés dans les prochaines versions d'UXP.

Parallèlement, Zabbix recueille également des données de surveillance au niveau du système d'exploitation par l'intermédiaire de l'agent Zabbix installé sur le serveur de registre.

Les sections suivantes traitent de la configuration et de l'utilisation de cette surveillance spécifique à UXP.

15.1. Configuration de la surveillance

Droits d'accès

Les droits d'accès au fichier de données de surveillance sont accordés en fonction de l'adresse IP. Par défaut, seul localhost a accès au fichier de données. Pour accorder des droits d'accès au serveur de surveillance ou à un autre système, ajoutez l'adresse IP de l'hôte correspondant au fichier de configuration Nginx `/etc/uxp/nginx/monitoring-access-list`:

```
allow 127.0.0.1;
allow 192.168.1.100;
```

Notez que chaque déclaration `allow` doit se terminer par un point-virgule.



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

```
sudo systemctl reload nginx
```

Intervalle de collecte des données de surveillance

L'intervalle de collecte des données de surveillance par défaut est de 180 secondes (3 minutes). Pour le modifier, remplacez la valeur du paramètre de configuration `params-collecting-interval-seconds` en modifiant la section `[registry-monitor]` du fichier `/etc/uxp/conf.d/local.ini`:

```
[registry-monitor]
```

```
params-collecting-interval-seconds=120
```



Après avoir modifié la configuration, vous devez redémarrer le service `uxp-registry-monitor` :

```
sudo systemctl restart uxp-registry-monitor
```

15.2. Demande de données de surveillance

Le fichier de données de surveillance `data.json` est partagé de manière statique via HTTPS.

Les hôtes autorisés peuvent accéder aux données de surveillance en envoyant une requête GET à l'URL :

```
https://<registry-server>:4001/monitoring/data.json
```

où `<registry-server>` est l'adresse réelle du serveur de registre.

15.3. Format des fichiers de données de surveillance

Les données de surveillance sont formatées sous forme de fichier JSON [JSON file \[JSON\]](#). Le [schéma \[JSON-SCHEMA\]](#) de ce fichier est le suivant :

```
{
  "title" : "Registry Server Monitoring Data Schema",
  "type": "object",
  "properties": {
    "meta": {
      "description": "Metadata",
      "type": "object",
      "properties": {
        "timestamp": {
          "description": "The monitoring data UNIX timestamps (in seconds)",
          "type": "integer"
        }
      }
    },
    "required": ["timestamp"]
  },
  "data": {
    "description": "Monitoring data",
    "type": "object",
    "properties": {
      "license_file_exists": {
        "description": "True if registry server license file exists",
        "type": "boolean"
      }
    }
  }
}
```

```
    }  
  }  
},  
"required": ["meta", "data"]  
}
```


16. Journaux et services du système

Droits d'accès : privilèges de l'utilisateur root ou appartenance au groupe système adm

16.1. Journaux

Pour lire les journaux, vous devez avoir les droits d'utilisateur root ou appartenir au groupe système adm.

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

16.2. Services du système

Les services les plus importants du serveur de registre sont les suivants :

Services	Objectif	Journal
uxp-jetty	Le serveur d'application qui fournit l'interface utilisateur et le service d'acceptation des demandes.	/var/log/uxp/jetty/

Services	Objectif	Journal
uxp-registry-monitor	Processus de surveillance.	/var/log/uxp/registry-monitor.log
uxp-signer	Le service qui gère les paramètres clés.	/var/log/uxp/signer.log
nginx	Le serveur Web qui distribue la configuration et met en œuvre le protocole TLS dans l'interface utilisateur.	/var/log/nginx/

Les services système sont gérés via la fonctionnalité `systemd`.

Pour démarrer un service :

```
sudo systemctl start <service>
```

Pour arrêter un service :

```
sudo systemctl stop <service>
```

Pour vérifier l'état du service :

```
sudo systemctl status <service>
```

Pour vérifier les journaux des services du système :

```
sudo journalctl -u <service>
```

16.3. Configuration de la journalisation

Le système **Logback** est utilisé pour la journalisation.

Dans Logback, les niveaux de journalisation sont classés du plus bas au plus haut en fonction de leur gravité :

TRACE < DEBUG < INFO < WARN < ERROR.

Notez qu'il n'est pas recommandé de définir un niveau de journalisation inférieur à `INFO` sur les systèmes de production pendant plus longtemps que nécessaire, car la verbosité excessive des niveaux inférieurs peut épuiser les ressources de votre système.

Les paramètres par défaut de la journalisation sont les suivants :

- les enregistrements sont consignés au niveau `INFO` ;
- une nouvelle archive ZIP des enregistrements du journal est créée une fois par jour ou lorsque la taille du fichier journal atteint 100 Mo (`maxFileSize` dans la politique de roulement) ;

- les enregistrements sont conservés pendant 60 jours (`maxHistory`) ou jusqu'à ce que 1 Go d'espace de stockage (`totalSizeCap`) ait été utilisé.

16.3.1. Configuration des paramètres de journalisation des composants

Chaque composant UXP possède son propre fichier de configuration **Logback**

Services	Fichier de configuration
uxp-jetty	/etc/uxp/conf.d/registry-jetty-logback.xml
uxp-registry-monitor	/etc/uxp/conf.d/registry-monitor-logback.xml
uxp-signer	/etc/uxp/conf.d/signer-logback.xml

Tous les fichiers de configuration de la journalisation suivent la même structure générale. Par exemple, pour chaque fichier journal produit par un composant, il existe une section qui configure la politique de stockage des anciens fichiers journaux :

```
<appender name="FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${logOutputPath}/jetty.log</file>
  <rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
    <fileNamePattern>${logOutputPath}/jetty.%d{yyyy-MM-dd}.%i.log.zip</fileNamePattern>
    <!-- each file should be at most 100MB, keep 60 days worth of history, but at
    most 1GB -->
    <maxFileSize>100MB</maxFileSize>
    <maxHistory>60</maxHistory>
    <totalSizeCap>1GB</totalSizeCap>
  </rollingPolicy>
  <encoder>
    <pattern>%d [%thread] %-5level %logger{36} - %msg%n</pattern>
    <charset>UTF-8</charset>
  </encoder>
</appender>
```

Pour modifier la taille des archives ZIP et la durée de stockage des archives, modifiez les paramètres `maxFileSize`, `maxHistory` et `totalSizeCap` dans la section `rollingPolicy`.

En outre, le paramètre `pattern` décrit le modèle de journalisation utilisé pour les entrées du fichier journal. Elle peut être configurée conformément à [\[LOGBACK-PATTERNS\]](#).

16.4. Journal d'audit

Droits d'accès : privilèges de l'utilisateur root

Le serveur de registre conserve un journal d'audit des événements effectués par l'administrateur du serveur de registre. Les événements du journal d'audit sont générés par l'interface utilisateur lorsque l'utilisateur modifie l'état ou la configuration du système. Les actions de l'utilisateur sont enregistrées indépendamment du fait que le résultat de l'action soit un succès ou un échec. La liste complète des événements du journal d'audit est décrite dans [\[UXP-SPEC-AL\]](#).

Les actions qui modifient l'état ou la configuration du système, mais qui ne sont pas effectuées à l'aide de l'interface utilisateur, ne sont pas consignées dans le journal d'audit (par exemple, l'installation et la mise à jour du logiciel UXP, la création d'utilisateurs et l'octroi de privilèges, ainsi que la modification des fichiers de configuration dans le système de fichiers).

Un enregistrement du journal d'audit contient :

- l'acteur qui a réalisé l'événement,
- la date et l'heure de l'événement,
- la description de l'événement,
- le serveur où l'événement a eu lieu,
- la version du logiciel Serveur de registre UXP.

Par exemple, l'ajout d'un nouveau membre dans le serveur de registre produit l'enregistrement suivant :

```
{
  "actor": {
    "remoteAddress": "[fd53:dac3:30b7::]",
    "sessionIdHash": "787f6341ba3dc95db737641f890131a195014ae780b848fe454afa0103f1e827",
    "username": "johnsmith"
  },
  "createdAt": "2024-09-04T14:53:12.136+0300",
  "event": {
    "data": {
      "memberClass": "COM",
      "memberCode": "3948372839",
      "memberName": "Acme Inc"
    },
    "name": "Add member",
    "result": "SUCCESS"
  },
  "hostname": "registryserver1",
  "version": "1.22.0"
}
```

L'enregistrement de l'événement d'action échouée comprend le message d'erreur. Par exemple :

```
{
  "actor": {
    "remoteAddress": "[fd53:dac3:30b7::]",
    "sessionIdHash": "787f6341ba3dc95db737641f890131a195014ae780b848fe454afa0103f1e827",
    "username": "johnsmith"
  },
  "createdAt": "2024-09-04T14:57:41.670+0300",
  "event": {
    "data": {
      "memberClass": "COM",
      "memberCode": "3948372839",
      "memberName": "Acme Inc"
    },
    "error": "Member with class 'COM' and code '3948372839' already exists",
    "name": "Add member",
    "result": "FAILURE"
  },
  "hostname": "registryserver1",
  "version": "1.22.0"
}
```

Par défaut, le journal d'audit est situé dans le fichier `/var/log/uxp/audit.log`.

16.4.1. Changer la configuration du journal d'audit

Le logiciel UXP écrit le journal d'audit dans `syslog` (`rsyslog`) à l'aide de l'interface UDP (le port par défaut est 514). La configuration correspondante se trouve dans le fichier `/etc/rsyslog.d/90-udp.conf`

Les enregistrements du journal d'audit sont rédigés avec le niveau `INFO` et l'origine `LOCAL0`. Par défaut, les enregistrements de ce niveau et de cette origine sont sauvegardés dans le fichier d'audit UXP `/var/log/uxp/audit.log`

Le comportement par défaut peut être modifié en éditant le fichier de configuration `rsyslog` de `/etc/rsyslog.d/40-uxp.conf`

Redémarrez le service `rsyslog` pour appliquer les modifications apportées au fichier de configuration

```
sudo systemctl restart rsyslog
```

Le journal d'audit fait l'objet d'une rotation mensuelle par `logrotate`. Pour configurer la rotation du journal d'audit, modifiez le fichier de configuration `logrotate` de `/etc/logrotate.d/uxp-registry`

16.4.2. Archivage du journal d'audit

Afin d'économiser de l'espace sur le disque dur et d'éviter la perte des enregistrements du journal d'audit en cas de panne du serveur de registre, il est recommandé d'archiver périodiquement les fichiers du journal d'audit sur un support de stockage externe ou sur un serveur de journalisation.

Le logiciel UXP n'offre pas d'outils spéciaux pour l'archivage du journal d'audit. `rsyslog` peut être configuré pour rediriger le journal d'audit vers un emplacement externe.

17. Dépannage

17.1. Échec de la signature de la configuration interne – clé active manquante

Droits d'accès : Responsable de sécurité

Si vous voyez cette erreur, cela signifie que le serveur de registre n'a pas de clé pour signer la configuration globale. Accédez à la page **Configuration globale** et générez une nouvelle clé de signature pour la configuration interne.

Si vous voyez la même erreur pour la configuration externe, générez une nouvelle clé pour la configuration externe.

17.2. La signature de la configuration interne a échoué – le PIN de la clé active n'a pas été saisi

Droits d'accès : Responsable de sécurité

Si vous voyez cette erreur, cela signifie que le serveur de registre n'a pas accès à la clé de signature de la configuration globale car le jeton contenant la clé est déconnecté. Accédez à la page de **configuration globale** et saisissez le code PIN du jeton.

Si vous voyez la même erreur pour la configuration externe, entrez le code PIN pour la clé de signature de la configuration externe.

17.3. La génération de la configuration globale échoue depuis '<timestamp>'

Droits d'accès : Responsable de sécurité

Les raisons possibles de l'échec de la génération de la configuration globale sont les suivantes :

- La signature de la configuration a échoué. Si c'est le cas, le serveur de registre affiche une autre erreur précisant la raison. Les raisons les plus courantes sont l' [absence de la clé de signature](#) ou le fait que le [code PIN n'a pas été saisi](#).
- Le fournisseur de services de gestion n'est pas configuré. Vérifiez si un fournisseur de services de gestion est défini sur la page **Paramètres du système**. Pour plus d'informations sur le fournisseur de services de gestion, consultez la section [Configuration d'un fournisseur de services de gestion](#).

17.4. La génération de l'ancre de configuration interne a échoué : Aucune clé de signature de la configuration n'est configurée

Droits d'accès : Responsable de sécurité

Si vous voyez cette erreur, cela signifie que le serveur de registre n'a pas de clé pour signer la configuration globale. Accédez à la page **Configuration globale** et générez une nouvelle clé de signature pour la configuration interne.

Si vous voyez la même erreur pour la configuration externe, générez une nouvelle clé pour la configuration externe.

17.5. Impossible d'approuver ou de refuser une demande de suppression

Droits d'accès : Responsable d'enregistrement

Les demandes de suppression, contrairement aux demandes d'enregistrement, sont automatiques. Ainsi, les demandes de suppression envoyées par les serveurs de sécurité s'appliquent instantanément et ne nécessitent pas de confirmation de la part de l'administrateur du serveur de registre.

Annexe A: 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-confcli` sur les serveurs de surveillance) de l'instance UXP ont été mis à jour vers la version actuelle.

- Ajout de la prise en charge des clés EC pour Nginx et les certificats TLS internes.
- Ajout de la prise en charge de clés RSA plus longues (3072 et 4096 bits).
- Amélioration de la communication TLS.
 - Ajout de la prise en charge de TLS 1.3 (désormais protocole par défaut). TLS 1.2 est toujours pris en charge par défaut pour des raisons de compatibilité ascendante.
 - Ajout de suites de chiffrement TLS plus puissantes activées par défaut.
 - Il est désormais possible de configurer les suites de chiffrement activées pour la

communication TLS entre le serveur de sécurité et le système d'information.

- Le serveur de sécurité utilise désormais une connexion de bouclage lorsque la demande du client de service est traitée par le même serveur de sécurité.
- Amélioration de la procédure de modification du certificat TLS interne du serveur de sécurité.
 - Il est désormais possible de modifier le certificat en toute simplicité.
 - Il est désormais possible d'importer un certificat (généré par une autorité de certification externe) et la clé privée correspondante sous la forme d'un magasin de clés PKCS#12.
- Le port d'écoute côté serveur entre les serveurs de sécurité est désormais distribué avec l'adresse du serveur de sécurité via la configuration globale. Il permet de modifier le port d'écoute du serveur de sécurité sans interrompre les connexions avec d'autres serveurs de sécurité.



Cette fonctionnalité ne peut être utilisée que lorsque tous les serveurs de registre et les serveurs de sécurité de l'instance UXP ont été mis à jour vers la version actuelle.

- Le type de connexion du propriétaire du serveur de sécurité pour les serveurs dans le rôle de consommateur de services est maintenant fixé à HTTPS pour améliorer la sécurité.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Ubuntu 20.04 LTS est désormais une plate-forme supportée (et recommandée). Consultez le guide de mise à jour Ubuntu UXP-UPG-UB20.
- Plusieurs corrections et améliorations mineures.

1.12.2 (04.2020)

- Ajout d'un profil de certificat.

1.12.1 (03.2020)

- Plusieurs corrections et améliorations mineures.

1.12.0 (02.2020)

- Il y a un nouveau composant Vérificateur UXP. Il permet de consulter le contenu du journal des messages stocké sur le serveur de sécurité, ainsi que de télécharger et de vérifier des messages individuels signés.
- L'API pour le téléchargement de documents signés (ASiC) exige désormais l'utilisation du protocole HTTPS afin d'éviter toute violation de la confidentialité dans le réseau interne.
- Il y a un nouvel en-tête HTTP `Uxp-Transaction-ID`. Il est généré automatiquement par le serveur de sécurité et contient une valeur unique pour chaque message traité par le serveur de sécurité. L'identifiant de la transaction est également enregistré dans le journal des messages et peut être utilisé pour identifier de manière unique les messages UXP.

- Une nouvelle option de configuration permet de désactiver l'enregistrement des messages techniques (services de surveillance et metainfo) dans le journal des messages. Cela peut permettre d'économiser de l'espace disque s'il n'est pas nécessaire de créer une valeur probante pour les échanges qui n'impliquent pas de données commerciales.
- La version 7.x des outils Elasticsearch et Kibana est désormais prise en charge pour la surveillance locale.
- La grappe multi-nœuds Elasticsearch est désormais pris en charge.
- L'ancien document de statistiques sur les demandes (l'ancien format pour les statistiques UXP) n'est plus pris en charge dans le suivi local.
- Ubuntu 18.04 est désormais la plus ancienne plate-forme prise en charge.
- Java Runtime Environment est mis à jour vers la version 11. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

1.11.4 (12.2019)

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

1.11.3 (12.2019)

- Ajout de la prise en charge du mécanisme de signature PKCS#11 CKM_RSA_PKCS_PSS et configuration du modèle de création de clé.

1.11.2 (10.2019)

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

1.11 (08.2019)

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

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

1.10 (12.2018)

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

1.9 (06.2018)

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

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

1.8 (10.2017)

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

1.7 (06.2017)

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

1.6 (05.2017)

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

1.5 (03.2017)

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

1.4 (10.2016)

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

1.3 (07.2016)

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

1.2 (04.2016)

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

1.1 (03.2016)

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

1.0 (12.2015)

- Première publication des composants principaux UXP.