# Contrôle de l'utilisateur avec ISE/ISE-PIC

Les rubriques suivantes traitent de la façon d'effectuer la sensibilisation et le contrôle des utilisateurs avec ISE/ISE-PIC :



# Source d'identité ISE/ISE-PIC

Vous pouvez intégrer votre déploiement de Cisco Identity Services Engine (ISE) ou de votre connecteur ISE Passive Identity (ISE-PIC) au système pour utiliser ISE/ISE-PIC pour l'authentification passive.

ISE/ISE-PIC est une source d'identité faisant autorité et fournit des données de connaissance des utilisateurs pour les utilisateurs qui s'authentifient à l'aide d'Active Directory (AD), LDAP, RADIUS ou RSA. En outre, vous pouvez effectuer un contrôle utilisateur sur les utilisateurs Active Directory. ISE/ISE-PIC ne signale pas les tentatives de connexion échouées ni l'activité des utilisateurs des services invités ISE.

En plus de la sensibilisation et du contrôle de l'utilisateur, si vous utilisez ISE ISE pour définir et utiliser les balises de groupes de sécurité (SGT) pour classer le trafic dans un réseau Cisco TrustSec, vous pouvez rédiger des règles de contrôle d'accès qui utilisent SGT comme critères de correspondance de source et de destination. Cela vous permet de bloquer ou d'autoriser l'accès en fonction de l'appartenance à un groupe de sécurité plutôt que d'adresses IP ou d'objets réseau. Pour plus de renseignements, consultez Configurer les conditions d'attributs dynamiques reportez-vous également à Lignes directrices et limites ISE/ISE-PIC, à la page 4.

**Remarque** Le système n'analyse pas l'authentification de la machine IEEE 802.1x, mais il *analyse* l'authentification des utilisateurs 802.1x. Si vous utilisez 802.1x avec ISE, vous devez inclure l'authentification des utilisateurs. L'authentification machine 802.1x ne fournira pas d'identité d'utilisateur à centre de gestion qui peut être utilisée dans la politique.

Pour en savoir plus sur Cisco ISEet l'ISE-PIC, consultez Guide de l'administrateur de Cisco Identity Services Engine Passive Identity Connector ou Guide de l'administrateur de services d'identité Cisco Identity Services Engine.

**Remarque** Nous vous recommandons fortement d'utiliser la dernière version de ISEou ISE-PIC pour obtenir le dernier ensemble de fonctionnalités et le plus grand nombre de correctifs.

# Correspondance des balises de groupe de sécurité (Security Group Tag ou SGT) de la source et de la destination

Si vous utilisez ISE pour définir et utiliser les balises de groupes de sécurité (SGT) pour classer le trafic dans un réseau Cisco TrustSec, vous pouvez rédiger des règles de contrôle d'accès qui utilisent SGT comme critères de correspondance de source et de destination. Cela vous permet de bloquer ou d'autoriser l'accès en fonction de l'appartenance à un groupe de sécurité plutôt que d'adresses IP ou d'objets réseau. Pour plus de renseignements, consultez Configurer les conditions d'attributs dynamiques

La correspondance sur les balises SGT offre les avantages suivants :

- Le centre de gestion peut s'abonner aux mappages de Security Group Tag eXchange Protocol (SXP) à partir d'ISE.

  ISE utilise SXP pour propager la base de données de mappage IP-SGT vers les périphériques gérés. Lorsque vous configurez centre de gestion pour utiliser un serveur ISE, vous activez l'option pour qu'il écoute le sujet SXP d'ISE. Ainsi, centre de gestion se renseigne sur les balises et les mappages des groupes de sécurité directement à partir d'ISE. centre de gestion publie ensuite les groupes SGT et les mappages sur les périphériques gérés.

  Le sujet SXP reçoit des balises de groupes de sécurité en fonction des mappages statiques et dynamiques appris par le biais du protocole SXP entre ISE et d'autres périphériques conformes SXP (comme les commutateurs).

  Vous pouvez créer des balises de groupe de sécurité dans ISE et attribuer des adresses IP d'hôte ou de réseau à chaque balise. Vous pouvez également affecter des SGT aux comptes utilisateur, et la SGT est affectée au trafic de l'utilisateur. Si les commutateurs et les routeurs du réseau sont configurés pour le faire, ces balises sont ensuite affectées aux paquets à mesure qu'ils entrent dans le réseau contrôlé par ISE, le nuage Cisco TrustSec.

  SXP n'est *pas* pris en charge par ISE-PIC.

- Les centre de gestion et les périphériques gérés peuvent obtenir des informations sur les mappages SGT sans déployer de politique supplémentaire. (En d'autres termes, vous pouvez afficher les événements de connexion pour les mappages SGT sans déployer de politique de contrôle d'accès.)

- Prend en charge Cisco TrustSec, qui vous permet de segmenter votre réseau pour protéger les ressources commerciales essentielles.

- Lorsqu'un périphérique géré évalue SGT comme critères de correspondance de trafic pour une règle de contrôle d'accès, il utilise la priorité suivante :

  1. La balise SGT source définie dans le paquet, le cas échéant.

Pour que la balise SGT se trouve dans le paquet, les commutateurs et les routeurs du réseau doivent être configurés pour les ajouter. Consultez la documentation ISE pour obtenir des renseignements sur la mise en œuvre de cette méthode.

Pour que la balise SGT se trouve dans le paquet, les commutateurs et les routeurs du réseau doivent être configurés pour les ajouter. Consultez la documentation ISE pour obtenir des renseignements sur la mise en œuvre de cette méthode.

2. La balise SGT attribuée à la session utilisateur, telle que téléchargée à partir du répertoire de session ISE. La balise SGT peut être mise en correspondance avec la source ou la destination.
3. Le mappage SGT-adresse IP téléchargé à l'aide de SXP. Si l'adresse IP fait partie de la plage prévue pour une balise SGT, le trafic correspond à la règle de contrôle d'accès qui utilise la balise. La balise SGT peut être mise en correspondance avec la source ou la destination.

Exemples :

- Dans ISE, créez une balise SGT nommée Guest Users (utilisateurs invités) et associez-la au réseau 192.0.2.0/24.

  Par exemple, vous pourriez utiliser Utilisateurs invités comme condition SGT de source dans votre règle de contrôle d'accès et restreindre l'accès à certaines URL, catégories de sites Web ou réseaux de toute personne qui accède à votre réseau.

- Dans ISE, créez une balise SGT nommée Réseaux restreints et associez-la au réseau 198.51.100.0/8.

  Par exemple, vous pourriez utiliser Réseaux restreints comme condition de règle SGT de destination et bloquer l'accès des utilisateurs invités et d'autres réseaux dont les utilisateurs ne sont pas autorisés à accéder au réseau.

### Sujets connexes

Lignes directrices et limites ISE/ISE-PIC, à la page 4

# Exigences de licence pour ISE/ISE-PIC

### Licence de défense contre les menaces

N'importe lequel

### Licence traditionnelle

Contrôle

# Exigences et conditions préalables pour ISE/ISE-PIC

### Domaines pris en charge

N'importe quel

### Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

# Lignes directrices et limites ISE/ISE-PIC

Utilisez les directives décrites dans cette section lors de la configuration d'ISE/ISE-PIC.

### Compatibilité des versions ISEet ISE-PIC et des configurations

Votre version et configuration ISE/ISE-PIC affectent son intégration et son interaction avec Cisco Secure Firewall Management Center, comme suit :

- Nous vous recommandons fortement d'utiliser la dernière version d'ISEou ISE-PIC pour obtenir le dernier ensemble de fonctionnalités.
- Synchronisez l'heure sur le serveur ISE/ISE-PIC et Cisco Secure Firewall Management Center. Sinon, le système pourrait provoquer des expirations de délai d'utilisateur à des intervalles inattendus.
- Pour mettre en œuvre le contrôle par l'utilisateur à l'aide des données d'ISE ou d'ISE-PIC, configurez et activez un domaine pour le serveur ISE en utilisant le persona pxGrid, comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- Chaque Cisco Secure Firewall Management Center nom d'hôte qui se connecte à un serveur ISE doit être unique; Sinon, la connexion à l'un des Cisco Secure Firewall Management Centersera abandonnée.
- Si vous configurez l'ISE/ISE-PIC pour surveiller un grand nombre de groupes d'utilisateurs, le système pourrait abandonner les mappages d'utilisateurs en fonction des groupes en raison des limites de mémoire du périphérique géré. Par conséquent, les règles assorties de conditions de domaine ou d'utilisateur peuvent ne pas fonctionner comme prévu.

  Pour tout périphérique exécutant la version 6.7 ou une version ultérieure, vous pouvez éventuellement utiliser la commande **configure identity-subnet-filter** pour limiter le nombre de sous-réseaux que le périphérique géré surveille. Pour obtenir plus d'informations, reportez-vous à la Référence des commandes de défense contre les menaces de Cisco Secure Firewall.

  Vous pouvez également configurer un objet réseau et appliquer cet objet en tant que filtre de mappage d'identité dans la politique d'identité. Consultez Créer une politique d'identité.

Pour les versions précises de l'ISEet de l'ISE-PIC compatibles avec cette version du système, consultez Guide de compatibilité de Cisco Firepower.

### Prise en charge d'IPv6

- Les versions compatibles d'ISEet d'ISE-PIC version 2.x prennent en charge les points terminaux compatibles avec IPv6.
- La version 3.0 (correctif 2) ou les versions ultérieures d'ISE/ISE-PIC activent la communication IPv6 entre ISE/ISE-PIC et centre de gestion.

### Séquence du serveur mandataire

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais.

### Approuver les clients dans ISE

Avant d'établir une connexion entre le serveur ISE et centre de gestion, vous devez approuver manuellement les clients dans ISE. (En général, il y a deux clients : un pour le test de connexion et un autre pour l'agent ISE.)

Vous pouvez également activer **approuver automatiquement les nouveaux comptes** dans ISE, comme indiqué dans le chapitre sur la gestion des utilisateurs et des sources d'identité externes *du Guide de l'administrateur de Cisco Identity Services Engine*.

### Les sessions inaccessibles sont supprimées

Si une session utilisateur dans ISE/ISE-PIC est signalée comme inaccessible, Cisco Secure Firewall Management Center supprime cette session afin qu'un autre utilisateur avec la même adresse IP ne puisse pas correspondre aux règles d'identité de l'utilisateur inaccessible.
Vous pouvez contrôler ce comportement dans ISE/ISE-PIC en accédant à **Fournisseurs** > **Sondes de point terminaux**, puis en cliquant sur l'un des éléments suivants :

- **Activé** pour qu'ISE/ISE-PIC surveille les connexions des points terminaux et, par conséquent, Cisco Secure Firewall Management Center pour supprimer la session d'un utilisateur inaccessible.
- **Désactivé** pour qu'ISE/ISE-PIC ignore les connexions des points terminaux.

### Balise du groupe de sécurité (SGT)

Une balise de groupe de sécurité (SGT) spécifie les privilèges d'une source de trafic dans un réseau sécurisé. Cisco ISE et Cisco TrustSec utilisent une fonctionnalité appelée Security Group Access (SGA) pour appliquer les attributs SGT aux paquets lors de leur entrée sur le réseau. Ces SGT correspondent au groupe de sécurité assigné à un utilisateur dans ISE ou Nokia. Si vous configurez ISE comme source d'identité, le système Firepower peut utiliser ces SGT pour filtrer le trafic.

Les étiquettes de groupes de sécurité peuvent être utilisées comme critères de correspondance de source et de destination dans les règles de contrôle d'accès.

**Remarque** Pour mettre en œuvre le contrôle de l'utilisateur à l'aide uniquement de la balise d'attribut ISE SGT, vous n'avez pas besoin de configurer de domaine pour le serveur ISE. Les conditions d'attributs ISE SGT peuvent être configurées dans des politiques avec ou sans politique d'identité associée.

**Remarque** Dans certaines règles, des conditions SGT personnalisées peuvent correspondre au trafic marqué par des attributs SGT qui n'ont *pas* été attribués par ISE. Cela n'est pas considéré comme un contrôle de l'utilisateur et ne fonctionne que si vous n'utilisez pas ISEou ISE-PIC comme source d'identité; voir Conditions SGT personnalisées.

Pour mettre en correspondance des balises SGT de destination en plus des balises SGT source, les conditions suivantes s'appliquent :

Version d'ISE requise : 2.6 correctif 6 ou version ultérieure, 2.7 correctif 2 ou version ultérieure

Prise en charge de routeur : tout routeur Cisco qui prend en charge le balisage en ligne SGT sur Ethernet. Pour en savoir plus, consultez des références comme la version de la plateforme de politiques de groupes et de la matrice de capacités de Cisco

Restrictions :

- La politique de qualité de service (QoS) utilise uniquement la mise en correspondance SGT de source; elle n'utilise *pas* la correspondance SGT de destination
- Le VPN d'accès à distance ne reçoit pas les mappages SGT directement par l'intermédiaire de RADIUS

**ISE et Haute disponibilité**

Lorsque le serveur ISE/ISE-PIC principal tombe en panne, les événementssuivants se produisent :

En raison de l'intégration avec pxGrid v2, les échanges circulaires centre de gestion entre les deux hôtes ISE configurés jusqu'à ce que l'un d'eux accepte la connexion.

En cas de perte de la connexion, centre de gestion reprend les tentatives d'intermittence sur les hôtes connectés.

**Emplacement du point terminal (ou IP d'emplacement)**

Un attribut d'emplacement de point terminal est l'adresse IP du périphérique réseau qui a utilisé ISE pour authentifier l'utilisateur, tel qu'identifié par ISE.

Vous devez configurer et déployer une politique d'identité pour contrôler le trafic en fonction de **l'emplacement du point terminal (adresse IP de l'emplacement)**.

**Attributs ISE**

La configuration d'une connexion ISE remplit la base de données Cisco Secure Firewall Management Center avec des données d'attributs ISE. Vous pouvez utiliser les attributs ISE suivants pour sensibiliser et contrôler l'utilisateur. Cette fonction n'est pas prise en charge avec ISE-PIC.

**profil du point terminal/(ou type de périphérique)**

Un attribut de profil de point terminal est le type de périphérique du point terminal de l'utilisateur, tel qu'il est identifié par ISE.

Vous devez configurer et déployer une politique d'identité pour contrôler le trafic en fonction du **profil de point terminal (type de périphérique)**.

# Comment configurer ISE/ISE-PIC pour le contrôle utilisateur

Vous pouvez utiliser ISE/ISE-PIC dans l'une des configurations suivantes :

- Avec un domaine, une politique d'identité et une politique de contrôle d'accès associée.

  Utilisez un domaine pour contrôler l'accès des *utilisateurs* aux ressources réseau dans la politique. Vous pouvez toujours utiliser les métadonnées des balises de groupe de sécurité ISE/ISE-PIC (SGT) dans vos politiques.

- Avec une politique de contrôle d'accès seulement. Aucun domaine ou aucune politique d'identité ne sont nécessaires.

  Utilisez cette méthode pour contrôler l'accès réseau à l'aide des métadonnées SGT uniquement.

### Sujets connexes

Comment configurer ISE sans domaine, à la page 7
Configurer ISE/ISE-PIC pour le contrôle utilisateur à l'aide d'un domaine, à la page 8

# Comment configurer ISE sans domaine

Cette rubrique fournit un aperçu global des tâches que vous devez effectuer pour configurer ISE afin de pouvoir autoriser ou bloquer l'accès au réseau à l'aide des balises SGT.

### Procédure

| | Commande ou action | Objectif |
|---|---|---|
| **Étape 1** | Correspondance SGT : activez SXP sur ISE. | Cela permet à centre de gestion de recevoir des mises à jour d'ISE lorsque les métadonnées de la balise SGT sont modifiées. |
| **Étape 2** | Exporter les certificats de système à partir de ISE/ISE-PIC. | Les certificats sont nécessaires pour une connexion sécurisée entre le pxGrid ISE/ISE-PIC, les serveurs de surveillance (MNT) et centre de gestion. Voir la section Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 13. |
| **Étape 3** | Importez les certificats dans centre de gestion. | Les certificats doivent être importés comme suit :<br>• Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**)<br>• Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**) |

| | Commande ou action | Objectif |
|---|---|---|
| | | • Certificat MNT : autorité de certification de confiance |
| **Étape 4** | Créez la source d'identité ISE/ISE-PIC. | La source d'identité ISE/ISE-PIC vous permet de contrôler l'activité des utilisateurs à l'aide des étiquettes de groupe de sécurité (SGT) fournies par ISE/ISE-PIC. Voir Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 16. |
| **Étape 5** | Créez une règle de contrôle d'accès | La règle de contrôle d'accès spécifie une action à entreprendre (par exemple, autoriser ou bloquer) si le trafic correspond aux critères de la règle. Vous pouvez utiliser les métadonnées SGT source et de destination comme critères de correspondance dans la règle de contrôle d'accès. Consultez Introduction aux règles de contrôle d'accès. |
| **Étape 6** | Déployer la politique de contrôle d'accès sur les périphériques gérés. | Avant que votre politique ne puisse prendre effet, elle doit être déployée sur les périphériques gérés. Consultez Déployer les modifications de configuration. |

### Prochaine étape

Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 13

# Configurer ISE/ISE-PIC pour le contrôle utilisateur à l'aide d'un domaine

### Avant de commencer

Cette rubrique fournit un aperçu général des tâches que vous devez effectuer pour configurer ISE/ISE-PIC pour le contrôle utilisateur et pour pouvoir autoriser ou bloquer l'accès d'un utilisateur ou d'un groupe au réseau. Les utilisateurs et les groupes peuvent être stockés sur n'importe quel serveur répertorié dans Serveurs pris en charge pour les domaines.

### Procédure

| | Commande ou action | Objectif |
|---|---|---|
| **Étape 1** | Destination SGT uniquement : activer SXP sur ISE. | Cela permet à centre de gestion de recevoir des mises à jour d'ISE lorsque les métadonnées de la balise SGT sont modifiées. |
| **Étape 2** | Exporter les certificats de système à partir d'ISE/ISE-PIC. | Les certificats sont nécessaires pour une connexion sécurisée entre le pxGrid ISE/ISE-PIC, les serveurs de surveillance |

| | Commande ou action | Objectif |
|---|---|---|
| | | (MNT) et centre de gestion. Consultez les documents suivants :<br>• Certificat du serveur pxGrid et du serveur MNT : Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 13<br>• Certificat client pxGrid : Générer un certificat autosigné, à la page 15 |
| **Étape 3** | Importez les certificats dans centre de gestion. | Les certificats doivent être importés comme suit :<br>• Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**)<br>• Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**)<br>• Certificat MNT : autorité de certification de confiance |
| **Étape 4** | (Facultatif) Créez une séquence de serveur mandataire à utiliser avec le domaine ainsi qu'avec ISE/ISE-PIC. | Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.<br>Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais. |
| **Étape 5** | Créez un domaine. | Vous devez créer un domaine uniquement pour contrôler l'accès au réseau des utilisateurs et des groupes de votre choix. |

| | Commande ou action | Objectif |
|---|---|---|
| | | Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine. |
| **Étape 6** | Téléchargez les utilisateurs et les groupes pour le domaine | Le téléchargement d'utilisateurs et de groupes vous permet de les utiliser dans les règles de contrôle d'accès. Consultez Synchroniser les utilisateurs et les groupes. |
| **Étape 7** | Créez la source d'identité ISE/ISE-PIC. | La source d'identité ISE/ISE-PIC vous permet de contrôler l'activité des utilisateurs à l'aide des étiquettes de groupe de sécurité (SGT) fournies par ISE/ISE-PIC. Voir Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 16. |
| **Étape 8** | Créez une politique d'identité | Une politique d'identité est un conteneur pour une ou plusieurs règles d'identité. Consultez Créer une politique d'identité. |
| **Étape 9** | Créez une règle d'identité | Une règle d'identité spécifie comment un domaine est utilisé pour contrôler l'accès au réseau par les utilisateurs et les groupes. Consultez Créer une règle d'identité. |
| **Étape 10** | Associez la politique d'identité à une politique de contrôle d'accès. | Cela permet à la politique de contrôle d'accès d'utiliser les utilisateurs et les groupes au sein du domaine. |
| **Étape 11** | Créez une règle de contrôle d'accès | La règle de contrôle d'accès spécifie une action à entreprendre (par exemple, autoriser ou bloquer) si le trafic correspond aux critères de la règle. Vous pouvez utiliser les métadonnées SGT source et de destination comme critères de correspondance dans la règle de contrôle d'accès. Consultez Introduction aux règles de contrôle d'accès. |
| **Étape 12** | Déployer la politique de contrôle d'accès sur les périphériques gérés. | Avant que votre politique ne puisse prendre effet, elle doit être déployée sur les périphériques gérés. Consultez Déployer les modifications de configuration. |

### Prochaine étape

Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 13

# Configurer ISE/ISE-PIC

Les rubriques suivantes expliquent comment configurer le serveur ISE/ISE-PIC à utiliser avec les politiques d'identité dans centre de gestion.

Les rubriques traitent de comment :

- Exporter les certificats du serveur ISEou ISE-PIC pour vous authentifier à l'aide de centre de gestion.
- Publier les rubriques SXP afin que centre de gestion puisse être mis à jour avec les balises de groupe de sécurité (SGT) sur le serveur ISE.

### Sujets connexes

Configurer les groupes de sécurité et la publication SXP dans ISE, à la page 11
Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 13

# Configurer les groupes de sécurité et la publication SXP dans ISE

Vous devez effectuer de nombreuses configurations dans Cisco Identity Services Engine (ISE) pour créer la politique TrustSec et les balises de groupes de sécurité (SGT). Veuillez consulter la documentation ISE pour des informations plus complètes sur la mise en œuvre de TrustSec.

La procédure suivante sélectionne les points saillants des paramètres principaux que vous devez configurer dans ISE pour que le périphérique Défense contre les menaces puisse télécharger et appliquer les mappages statiques SGT-à-adresse IP, qui peuvent ensuite être utilisés pour la mise en correspondance SGT source et destination dans les règles de contrôle d'accès. Consultez la documentation d'ISE pour obtenir des informations détaillées.

Les captures d'écran de cette procédure sont basées sur ISE 2.4. Les chemins d'accès exacts à ces fonctionnalités pourraient changer dans les versions ultérieures, mais les concepts et les exigences seront les mêmes. Bien que la version 2.4 ou ultérieure d'ISE soit recommandée, de préférence la version 2.6 ou ultérieure, la configuration devrait fonctionner à partir du correctif 1 d'ISE 2.2.

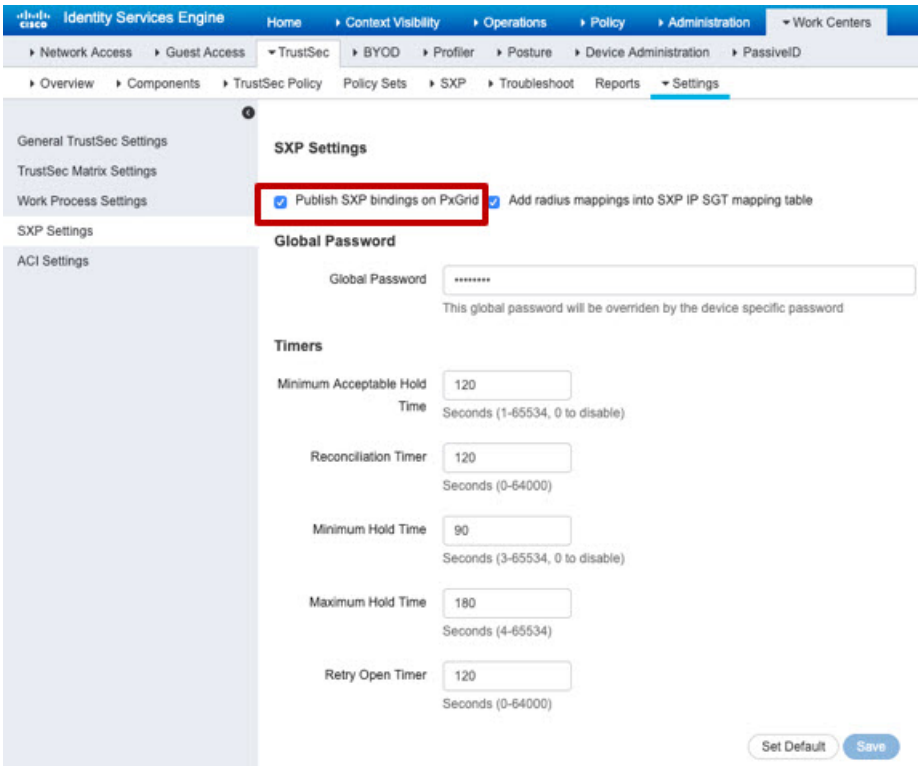
### Avant de commencer

Vous devez posséder la licence ISE Plus pour publier les mappages statiques SGT-adresses IP et pour obtenir les mappages utilisateur session-SGT afin que le périphérique Défense contre les menaces puisse les recevoir.

### Procédure

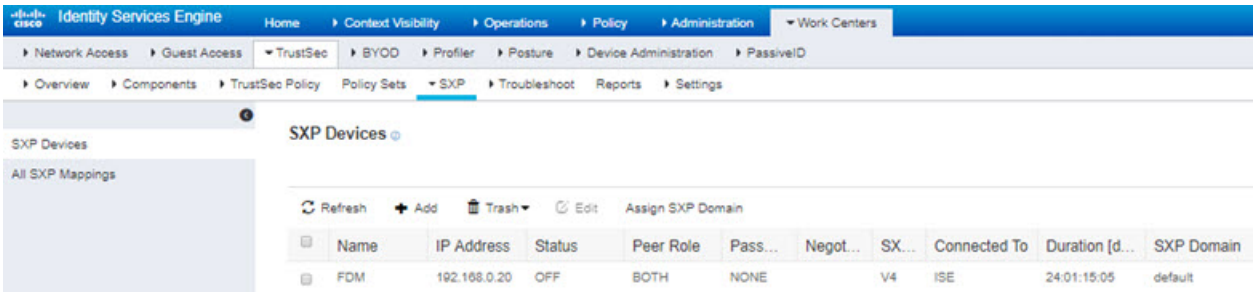
**Étape 1** Choisissez **Work Centers** > **TrustSec** > **Settings** > **SXP Settings (paramètres SXP)**, puis sélectionnez l'option **Publish SXP Bindings on PxGrid** (Publier les liens SXP sur PxGrid).

Cette option permet à ISE d'envoyer les mappages SGT à l'aide de SXP. Vous devez sélectionner cette option pour que le périphérique défense contre les menaces puisse « écouter » n'importe quel élément, de la liste au sujet SXP. Cette option doit être sélectionnée pour que le périphérique défense contre les menaces reçoive des informations de mappage SGT vers l'adresse IP statique. Ce n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets, ou les balises SGT qui sont attribuées à une session utilisateur.

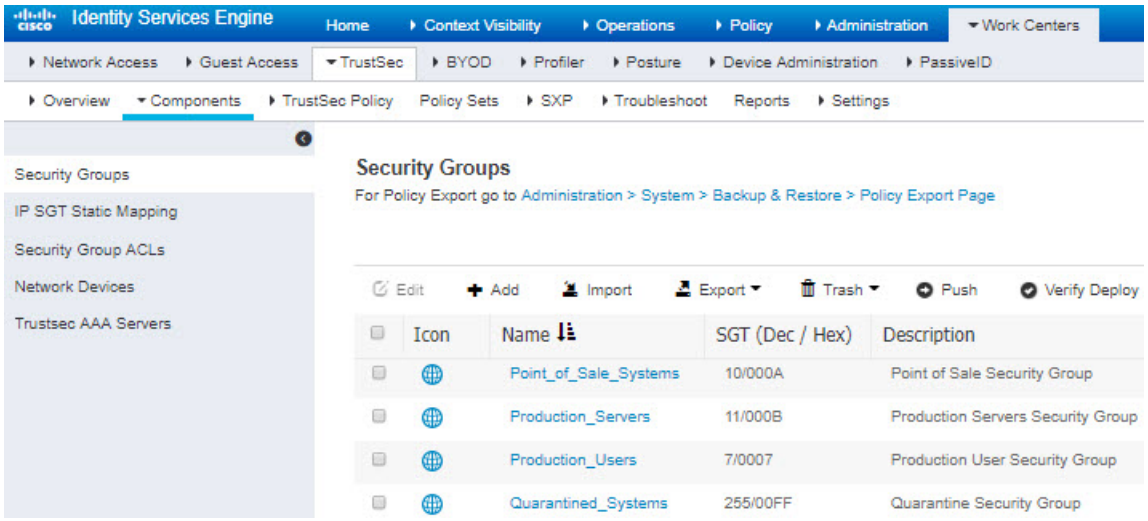



**Étape 2** Choisissez **Work Centers** > **TrustSec** > **SXP** > **SXP Devices** (Centres de travail > TrustSec > SXP > Périphériques SXP) et ajoutez un périphérique.

Il n'est pas nécessaire que ce soit un périphérique réel, vous pouvez même utiliser l'adresse IP de gestion du périphérique Défense contre les menaces. La table a simplement besoin d'au moins un périphérique pour amener ISE à publier les mappages statiques SGT- vers adresses IP. Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.

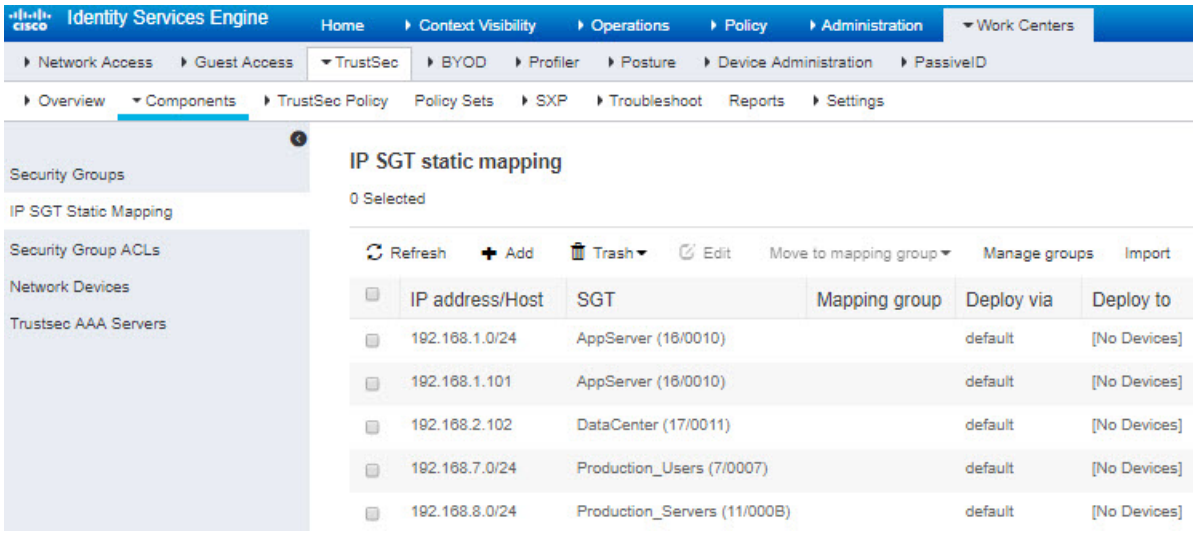



**Étape 3** Choisissez **Work Centers** > **TrustSec** > **Components** > **Security Groups** (Centres de travail > TrustSec > Composants > Groupes de sécurité) et vérifiez que des balises de groupes de sécurité sont définies. Créez-en de nouveaux si nécessaire.




**Étape 4** Choisissez **Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mapping** (Centres de travail > TrustSec > Composants > Mappage statique SGT IP) et mapper les adresses IP de l'hôte et du réseau aux balises du groupe de sécurité.

Cette étape n'est pas nécessaire si vous souhaitez simplement utiliser les balises SGT définies dans les paquets ou les balises SGT qui sont attribuées à une session utilisateur.




# Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion

Les sections suivantes expliquent comment :

- Exportez les certificats système à partir du serveur ISEou ISE-PIC.

Ces certificats sont nécessaires pour une connexion sécurisée au serveur ISEou ISE-PIC. Vous devrez peut-être exporter un ou trois certificats, selon la configuration de votre système ISE :

- Un certificat pour le serveur pxGrid
- Un certificat pour le serveur de surveillance (MNT)
- Un certificat, y compris la clé privée, pour le client pxGrid (c'est-à-dire centre de gestion)

  Contrairement aux deux premiers certificats, il s'agit d'un certificat autosigné.

- Importez ces certificats dans le centre de gestion :
  - Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**)
  - Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**)
  - Certificat MNT : autorité de certification de confiance

### Sujets connexes

Exporter un certificat système, à la page 14
Importer des certificats ISE/ISE-PIC, à la page 16

## Exporter un certificat système

Vous pouvez exporter un certificat système ou un certificat et sa clé privée associée. Si vous exportez un certificat et sa clé privée à des fins de sauvegarde, vous pouvez les réimporter ultérieurement au besoin.

### Avant de commencer

Pour effectuer la tâche suivante, vous devez être un super administrateur ou un administrateur de système.

### Procédure

**Étape 1** Dans l'interface graphique utilisateur de Cisco ISE, cliquez sur l'icône de **menu** (☰) et sélectionnez **Administration** > **Système** > **Certificats** > **Certificats système**.

**Étape 2** Cochez la case à côté du certificat que vous souhaitez exporter et cliquez sur **Exporter**.

**Étape 3** Choisissez si vous souhaitez exporter uniquement le certificat ou le certificat et sa clé privée associée.

**Astuces** Nous vous déconseillons d'exporter la clé privée associée à un certificat, car sa valeur peut être exposée. Si vous devez exporter une clé privée (par exemple, lorsque vous exportez un certificat de système à caractère générique à importer dans les autres nœuds Cisco ISE pour la communication entre les nœuds), spécifiez un mot de passe de chiffrement pour la clé privée. Vous devez préciser ce mot de passe lors de l'importation de ce certificat dans un autre nœud Cisco ISE pour déchiffrer la clé privée.

**Étape 4** Saisissez le mot de passe si vous avez choisi d'exporter la clé privée. Le mot de passe doit comporter au moins 8 caractères.

**Étape 5** Cliquez sur **Export** (exporter) pour enregistrer le certificat dans le système de fichiers qui exécute votre navigateur client.

Si vous exportez uniquement le certificat, le certificat est stocké au format PEM. Si vous exportez à la fois le certificat et la clé privée, le certificat est exporté en tant que fichier au format .zip qui contient le certificat au format PEM et le fichier de clé privée chiffré.

## Générer un certificat autosigné

Ajoutez un nouveau certificat local en générant un certificat autosigné. Cisco vous recommande d'utiliser uniquement des certificats autosignés pour vos besoins en matière de tests et d'évaluation internes. Si vous prévoyez déployer Cisco ISE dans un environnement de production, utilisez chaque fois que possible des certificats signés par une autorité de certification pour assurer une acceptation plus uniforme dans l'ensemble du réseau de production.

**Remarque** Si vous utilisez un certificat autosigné et que vous souhaitez modifier le nom d'hôte de votre nœud Cisco ISE, connectez-vous au portail d'administration de votre nœud Cisco ISE, supprimez le certificat autosigné qui porte l'ancien nom d'hôte et générez un nouveau certificat -certificat signé. Sinon, Cisco ISE continue d'utiliser le certificat autosigné avec l'ancien nom d'hôte.

### Avant de commencer

Pour effectuer la tâche suivante, vous devez être un super administrateur ou un administrateur de système.

### Procédure

**Étape 1** Dans l'interface graphique utilisateur de Cisco ISE, cliquez sur l'icône de **menu** (☰) et sélectionnez **Administration** > **Système** > **Certificats** > **Certificats système**.

Pour générer un certificat autosigné à partir d'un nœud secondaire, sélectionnez **Administration** > **Système** > **Certificat du serveur**.

**Étape 2** Dans l'interface graphique utilisateur de ISE-PIC, cliquez sur l'icône de **menu** (☰) et sélectionnez **Certificats** > **Certificats système**.

**Étape 3** Cliquez sur **Generate Self Signed Certificate** (générer un certificat autosigné) et saisissez les détails dans la fenêtre qui s'affiche.

**Étape 4** Cochez les cases dans la zone **utilisation** en fonction du service pour lequel vous souhaitez utiliser ce certificat.

**Étape 5** Cliquez sur **Submit** (Envoyer) pour générer le certificat.

Pour redémarrer les nœuds secondaires, à partir de l'interface de ligne de commande, saisissez les commandes suivantes dans l'ordre suivant :

a) **application stop ise**
b) **application start ise**

## Importer des certificats ISE/ISE-PIC

Cette procédure est facultative. Vous pouvez également importer des certificats de serveur ISE lorsque vous créez la source d'identité ISE/ISE-PIC, comme indiqué dans la section Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 16.

### Avant de commencer

Exportez les certificats du serveur ISEou ISE-PIC comme indiqué dans le Exporter un certificat système, à la page 14. Les certificats et la clé doivent être présents sur la machine à partir de laquelle vous vous connectez à centre de gestion.

Vous devez importer les certificats comme suit :

- Certificat client pxGrid : certificat interne avec clé (**Objets** > **Gestion des objets** > **PKI** > **Certifications internes**)
- Certificat du serveur pxGrid : Autorité de certification de confiance (**Objets** > **Gestion des objets** > **PKI** > **Autorités de certification de confiance**)
- Certificat MNT : autorité de certification de confiance

### Procédure

**Étape 1** Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.

**Étape 2** Cliquez sur **Objects(Objets)** > **Object Management** (Gestion d'objets).

**Étape 3** Développez **PKI**.

**Étape 4** Cliquez sur **Internal Certs** (Certificats internes).

**Étape 5** Cliquez sur **Add Internal Certs** (Ajouter des certificats internes).

**Étape 6** Suivez les instructions à l'écran pour importer le certificat et la clé privée.

**Étape 7** Cliquez sur **Trusted CAs** (Autorités de certification de confiance).

**Étape 8** Cliquez sur **Add Trusted CAs** (Ajouter des autorités de certification de confiance).

**Étape 9** Suivez les invites à l'écran pour importer le certificat du serveur pxGrid.

**Étape 10** Répétez les étapes précédentes, au besoin, pour importer l'autorité de certification de confiance du serveur MNT.

### Prochaine étape

Configurer ISE/ISE-PIC pour le contrôle utilisateur, à la page 16

# Configurer ISE/ISE-PIC pour le contrôle utilisateur

La procédure suivante explique comment configurer la source d'identité ISE/ISE-PIC. Vous devez être dans le domaine global pour effectuer cette tâche.

**Historique de la fonctionnalité Défense contre les menaces**

7.2 : ajoutez éventuellement un serveur mandataire, qui est une connexion à un ou plusieurs Cisco Defense Orchestrator dans l'éventualité où Cisco Defense Orchestrator ne peut pas communiquer avec le serveur ISE/ISE-PIC. .

### Avant de commencer

- Pour obtenir des sessions d'utilisateur à partir d'un serveur Active Directory de Microsoft ou d'un serveur LDAP pris en charge, configurez et activez un domaine pour le serveur ISE, en supposant le persona pxGrid, comme indiqué dans la section Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- Pour obtenir tous les mappages définis dans ISE, y compris les mappages SGT-adresses IP publiés par SXP, utilisez la procédure suivante. Comme alternative, vous avez les options suivantes :
  - Pour utiliser les informations SGT dans les paquets uniquement, et ne pas utiliser les mappages téléchargés à partir d'ISE, ignorez les étapes décrites dans Créer et modifier les règles de contrôle d'accès. Notez que dans ce cas, vous pouvez utiliser les balises SGT comme condition de source uniquement; ces balises ne correspondront jamais aux critères de destination.
  - Pour utiliser SGT uniquement dans les paquets et les mappages utilisateur-adresse IP/SGT, ne vous abonnez pas à la rubrique SXP dans la source d'identité ISE et ne configurez pas ISE pour publier les mappages SXP. Vous pouvez utiliser ces informations pour les conditions de correspondance de source et de destination.
- Exportez les certificats du serveur ISEou ISE-PIC et importez-les éventuellement dans le centre de gestion comme indiqué dans la section Certificats d'exportation du serveur ISE/ISE-PIC pour utilisation dans Centre de gestion, à la page 13.
- Pour publier des rubriques SXP de sorte que centre de gestion puisse être mis à jour avec les balises de groupe de sécurité (SGT) sur le serveur ISE, consultez Configurer ISE/ISE-PIC, à la page 11.

### Procédure

**Étape 1** Connectez-vous au centre de gestion.

**Étape 2** Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Identity Sources (sources d'identité)**.

**Étape 3** Cliquez sur **Identity Services Engine** pour le **type de service** afin d'activer la connexion ISE.

**Remarque** Pour désactiver la connexion, cliquez sur **None** (Aucun).

**Étape 4** Saisissez un **nom d'hôte ou une adresse IP principal(e)** et, éventuellement, un **nom d'hôte ou une adresse IP secondaire**.

**Étape 5** Cliquez sur les autorités de certification appropriées dans les listes d'autorité de certification de serveur **pxGrid Server CA** et **MNT Server CA**, et le certificat approprié des listes de certificats respectivement client et serveur **pxGrid Client Certificate**. Vous pouvez également cliquer sur **Ajouter** (+) pour ajouter un certificat.

**Remarque** Le certificat **pxGrid Client Certificate** doit inclure la valeur d'utilisation de clé étendue **clientAuth** ou ne doit inclure aucune valeur d'utilisation de clé étendue.

**Étape 6** (Facultatif) Saisissez un **filtre de réseau ISE** en utilisant la notation de bloc d'adresse CIDR.

**Étape 7** Dans la section S'abonner à, vérifiez les éléments suivants :

- **La rubrique du répertoire de session** afin de recevoir des renseignements sur la session d'utilisateur d'ISE du serveur ISE.
- **Le sujet SPX** afin de recevoir des mises à jour pour les mappages SGT à IP à partir du serveur ISE, le cas échéant. Cette option est requise pour utiliser les étiquettes SGT de destination dans les règles de contrôle d'accès.

**Étape 8** (Facultatif) Dans la liste **Proxy** (serveur mandataire), cliquez sur un périphérique géré ou sur une séquence proxy (de serveur mandataire).
Si CDO ne peut pas communiquer avec votre serveur ISE/ISE-PIC, vous pouvez choisir un périphérique géré ou une séquence de serveur mandataire pour le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.

**Étape 9** Pour tester la connexion, cliquez sur **Tester**.

Si le test échoue, cliquez sur **journaux supplémentaires** pour obtenir plus d'informations sur l'échec de connexion.

### Prochaine étape

- Précisez les utilisateurs à contrôler et d'autres options à l'aide d'une politique d'identité, comme décrit dans Créer une politique d'identité.
- Associez la règle d'identité à une politique de contrôle d'accès, qui filtre et inspecte éventuellement le trafic, comme indiqué dans Association d'autres politiques au contrôle d'accès.
- Utiliser les balises de groupe de sécurité (SGT) de Cisco ISE en tant qu'attributs dynamiques dans les politiques de contrôle d'accès.

  Pour en savoir plus, consultez Configurer les conditions d'attributs dynamiques.
- Déployez vos politiques de contrôle d'identité et de contrôle d'accès sur les périphériques gérés, comme indiqué dans Déployer les modifications de configuration.
- Surveillez l'activité de l'utilisateur, .

### Sujets connexes

Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec, à la page 20
Objets autorité de certification approuvée
Objets de certificat interne

# Champs de configuration ISE/ISE-PIC

Les champs suivants sont utilisés pour configurer une connexion à /ISE-PIC.

**Nom d'hôte ou adresse IP principal ou secondaire**

Le nom d'hôte ou l'adresse IP des serveurs principaux et, le cas échéant, des serveurs ISE pxGrid secondaires.

Les ports utilisés par les noms d'hôte que vous spécifiez doivent être accessibles à la fois par ISE et par centre de gestion.

**Autorité de certification du serveur pxGrid**

L'autorité de certification de confiance pour le cadre pxGrid. Si votre déploiement comprend un nœud pxGrid principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.

**Autorité de certification du serveur MNT**

L'autorité de certification de confiance pour le certificat ISE lors des téléchargements en bloc. Si votre déploiement comprend un nœud MNT principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.

**Certificat client pxGrid**

Le certificat interne et la clé que Cisco Secure Firewall Management Center doit fournir à /ISE-PIC pour se connecter à /ISE-PIC ou pour effectuer des téléchargements en bloc.

**Remarque** Le certificat **pxGrid Client Certificate** doit inclure la valeur d'utilisation de clé étendue clientAuth ou ne doit inclure aucune valeur d'utilisation de clé étendue.

**Filtre réseau du moteur de services de vérification des identités (ISE)**

Filtre facultatif que vous pouvez définir pour restreindre les données qu'ISE signale à Cisco Secure Firewall Management Center. Si vous fournissez un filtre de réseau, ISE transmet les données des réseaux dans ce filtre. Vous pouvez définir un filtre comme suit :

- Laissez le champ vide pour indiquer **`any`** (tout).
- Saisissez un seul bloc d'adresses IPv4 en utilisant la notation CIDR.
- Saisissez une liste de blocs d'adresses IPv4 en utilisant la notation CIDR, séparés par des virgules.

**Remarque** Cette version du système ne prend pas en charge le filtrage à l'aide d'adresses IPv6, quelle que soit votre version d'ISE.

**S'abonner à :**

**Session Directory Topic** : cochez cette case pour vous abonner aux informations sur la session utilisateur du serveur ISE. Comprend la balise SGT et les métadonnées de point terminal.

**SXP Topic** : cochez cette case pour vous abonner aux mappages SXP à partir du serveur ISE.

**Serveur mandataire**

Vous pouvez éventuellement choisir un périphérique géré ou une séquence proxy pour communiquer avec ISE/ISE-PIC si CDO n'est pas en mesure de le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.

**Sujets connexes**

Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec, à la page 20
Objets autorité de certification approuvée
Objets de certificat interne

# Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec

### Dépannage des problèmes Cisco TrustSec

Une interface de périphérique peut être configurée pour propager les balises de groupe de sécurité (SGT) à partir d'ISE/ISE-PIC ou d'un périphérique Cisco sur le réseau (appelé Cisco TrustSec). Dans la page de gestion des périphériques (**Devices** > **Device Management**), la case **Propagate Security Group Tag** (propager la balise de groupe de sécurité) pour une interface est cochée après le redémarrage du périphérique. Si vous ne souhaitez pas que l'interface propage les données TrustSec, décochez la case.

### Résoudre les problèmes de Cisco ISEet ISE-PIC

Pour d'autres renseignements relatifs au dépannage, consultez Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs et Dépannage du contrôle d'utilisateur.

Si vous rencontrez des problèmes avec la connexion ISE ou ISE-PIC, vérifiez les éléments suivants :

- La fonctionnalité de mappage d'identité pxGrid dans ISE doit être activée avant de pouvoir intégrer avec succès ISE au système.
- Lorsque le serveur principal tombe en panne, vous devez promouvoir manuellement le serveur secondaire en serveur principal. il n'y a pas de basculement automatique.
- Avant d'établir une connexion entre le serveur ISE et centre de gestion, vous devez approuver manuellement les clients dans ISE. (En général, il y a deux clients : un pour le test de connexion et un autre pour l'agent ISE.)

  Vous pouvez également activer **Approuver automatiquement les nouveaux comptes** dans ISE, comme discuté dans le chapitre sur la gestion des utilisateurs et des sources d'identité externes dans Guide de l'administrateur de services d'identité Cisco Identity Services Engine.
- Le certificat **pxGrid Client Certificate** doit inclure la valeur d'utilisation de clé étendue **clientAuth** ou ne doit inclure aucune valeur d'utilisation de clé étendue.
- L'heure de votre serveur ISE doit être synchronisée avec l'heure affichée sur Cisco Secure Firewall Management Center. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.
- Si votre déploiement comprend un nœud pxGrid principal et un secondaire,
  - Les certificats des deux nœuds doivent être signés par la même autorité de certification.
  - Les ports utilisés par le nom d'hôte doivent être accessibles à la fois par le serveur ISE et par centre de gestion.
- Si votre déploiement comprend un nœud MNT principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.

Pour exclure des sous-réseaux de la réception des mappages utilisateur-IP et SGT (Security Group Tag)-IP d'ISE, utilisez la commande **configure identity-subnet-filter** {**add** | **remove**}. Vous devez généralement effectuer cette opération pour les périphériques gérés disposant de moins de mémoire afin d'éviter les erreurs de mémoire du moniteur d'intégrité d'identité Snort.

Si vous rencontrez des problèmes avec les données des utilisateurs signalées par ISE ou ISE-PIC, tenez compte des éléments suivants :

- Une fois que le système a détecté une activité d'un utilisateur ISE dont les données ne sont pas encore dans la base de données, le système récupère les informations à propos du serveur. L'activité vue par l'utilisateur ISE n'est *pas* gérée par les règles de contrôle d'accès et n'est *pas* affichée dans l'interface Web tant que le système n'a pas récupéré les informations la concernant lors d'un téléchargement d'utilisateur.
- Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.
- centre de gestion ne reçoit pas les données d'utilisateur pour les utilisateurs des services invités de Cisco ISE.
- Si ISE surveille les mêmes utilisateurs que l'agent TS, le centre de gestion priorise les données de ce dernier. Si l'agent des services TS et ISE signalent une activité identique à partir de la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.
- Votre version et votre configuration d'ISE ont une incidence sur la façon dont vous pouvez l'utiliser dans le système. Pour en savoir plus, consultez Source d'identité ISE/ISE-PIC, à la page 1.
- Si la haute disponibilité centre de gestion est configurée et que le serveur principal tombe en panne, consultez la section sur ISE et la haute disponibilité dans Lignes directrices et limites ISE/ISE-PIC, à la page 4.
- ISE-PIC ne fournit pas de données d'attributs ISE.
- ISE-PIC ne peut pas effectuer les corrections ANC ISE.
- Les sessions FTP actives sont affichées comme utilisateur **Unknown** dans les événements. Cette situation est normale car, dans le protocole FTP actif, c'est le serveur (et non le client) qui lance la connexion et aucun nom d'utilisateur ne devrait être associé au serveur FTP. Pour plus d'informations sur le FTP actif, consultez RFC 959.

Si vous rencontrez des problèmes avec les fonctionnalités prises en charge, consultez Source d'identité ISE/ISE-PIC, à la page 1 pour obtenir plus d'informations sur la compatibilité des versions.

### Délai d'expiration de l'utilisateur ISE/ISE-PIC

Si vous configurez ISE/ISE-PIC sans domaine, sachez qu'il y a un délai d'expiration de session utilisateur qui affecte la façon dont les utilisateurs sont vus par Cisco Secure Firewall Management Center. Pour obtenir plus de renseignements, consultez Champs de domaine.

# Historique pour ISE/ISE-PIC

| Fonctionnalités | Centre de gestion Minimum | Défense contre les menaces Minimum | Détails |
|---|---|---|---|
| Serveur mandataire | N'importe lequel | 7.2.0 | Un ou plusieurs périphériques gérés qui peuvent communiquer avec Cisco Defense Orchestrator dans l'événement Cisco Defense Orchestrator ne peuvent pas communiquer avec le serveur ISE/ISE-PIC.<br>**Nouvel écran ou écran mis à jour** : **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Proxy Sequence (séquences de proxy)** |
| pxGrid 2.0 est la valeur par défaut pour les versions ISE/ISE-PIC prises en charge | N'importe lequel | 6.7.0 | Tenez compte des points suivants :<br>• Versions ISE / ISE-PIC prises en charge : 2.6 correctif 6 ou version ultérieure, 2.7 correctif 2 ou version ultérieure<br>• Les politiques de contrôle de réseau adaptatif (Adaptive Network Control ou ANC) remplacent les corrections du service de protection des points terminaux (EPS). Si des politiques de PSE sont configurées dans le centre de gestion, vous devez les migrer pour utiliser la norme ANC. |
| Si vous le souhaitez, excluez des sous-réseaux de la réception des mappages utilisateur-IP et SGT (Security Group Tag)-IP d'ISE. Vous devez généralement effectuer cette opération pour les périphériques gérés disposant de moins de mémoire afin d'éviter les erreurs de mémoire du moniteur d'intégrité d'identité Snort. | N'importe lequel | 6.7.0 | Nouvelle commande : **configure identity-subnet-filter** {**add** \| **remove**} |

| Fonctionnalités | Centre de gestion Minimum | Défense contre les menaces Minimum | Détails |
|---|---|---|---|
| Correspondance des balises de groupe de sécurité (Security Group Tag ou SGT) de la destination | N'importe lequel | 6.5.0 | Fonctionnalité introduite. Vous permet d'utiliser des balises ISE SGT pour les critères de correspondance de source et de destination dans les règles de contrôle d'accès.<br>Les balises SGT sont des mappages balise-hôte/réseau obtenus par ISE.<br>Écrans nouveaux ou modifiés :<br>• Nouvelles options pour configurer la correspondance SGT de destination : **Système** > **Intégration** > **Sources d'identité** > **ISE/ISE-PIC**<br>• **Sujet de l'annuaire de sessions** : abonnez-vous aux informations de session de l'utilisateur ISE.<br>• **Sujet SXP** : abonnez-vous aux mises à jour des balises SGT sur le serveur ISE.<br>• Colonnes nouvelles et renommées dans **Analyses** > **Connexions** > **Événements**<br>• Renommé : les balises des groupes de sécurité ont été renommées SGT Source<br>• Nouveau : SGT de destination |
| Intégration à ISE-PIC | N'importe lequel | 6.2.1 | Vous pouvez maintenant utiliser les données d'ISE-PIC. |
| Balises SGT pour le contrôle par l'utilisateur. | N'importe lequel | 6.2.0 | Vous n'avez plus besoin de créer un domaine ou une politique d'identité pour effectuer un contrôle utilisateur en fonction des données de la balise de groupe de sécurité de Cisco ISE (SGT). |
| Intégration avec ISE. | N'importe lequel | 6.0 | Fonctionnalité introduite. En s'abonnant à Platform Exchange Grid (PxGrid) de Cisco, le centre de gestion Cisco Firepower Management Center (FMC) peut télécharger des données utilisateur, des types de périphériques et des données d'emplacement du périphérique supplémentaires, ainsi que des balises de groupes de sécurité (Security Group Tags), une méthode utilisée par ISE pour fournir le contrôle d'accès au réseau. |

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.