Intégrer le moteur de services de vérification des identités de Cisco (ISE)/contrôleur d'identité passif ISE (ISE-PIC)

Cette rubrique contient les sections suivantes :

Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC)

Le moteur de services de vérification des identités (ISE) et le connecteur d'identité passive (ISE-PIC) de Cisco sont des applications qui s'exécutent sur des serveurs distincts de votre réseau pour fournir une gestion de l'identité améliorée. Secure Web Appliance peut accéder aux informations d'identité de l'utilisateur à partir d'un serveur ISE ou ISE-PIC. Lorsqu'ISE ou ISE-PIC est configuré, les informations sont récupérées (noms d'utilisateur et étiquettes Groupe sécurisé associée d'ISE, noms d'utilisateur et groupes Active Directory d'ISE-PIC) pour les profils d'identification configurés correctement, afin de permettre une identification transparente de l'utilisateur dans les politiques configurées d'utiliser ces profils.

- Vous pouvez élaborer des politiques d'accès à l'aide d'étiquettes Groupe sécurisé et de groupes Active Directory.
- Pour les utilisateurs qui échouent à l'identification transparente avec ISE/ISE-PIC, vous pouvez configurer l'authentification de secours avec des domaines basés sur Active Directory. Consultez Authentification secondaire, on page 5.

- Vous pouvez configurer l'authentification des utilisateurs dans les environnements de bureaux virtuels (Citrix, services de bureau partagé ou à distance de Microsoft, etc.). Consultez Authentification des utilisateurs VDI (Virtual Desktop Infrastructure) dans les intégrations ISE/ISE-PIC, on page 16.

Note

- Le service ISE/ISE-PIC n'est pas disponible en mode Connector.
- ISE/ISE-PIC version 2.4 et PxGrid version 2.0 sont pris en charge.
- La page de configuration ISE de l'interface Web de Secure Web Appliance est utilisée pour configurer les serveurs ISE ou ISE-PIC, pour charger des certificats et pour la connexion aux services ISE ou ISE-PIC. Les étapes de configuration d'ISE ou d'ISE-PIC sont similaires, et tous les détails spécifiques aux configurations ISE-PIC ont été mentionnés, le cas échéant.

Pour en savoir plus sur le tableau de prise en charge des versions de Cisco Secure Web Appliance ISE, consulter les informations sur le tableau de compatibilité ISE.

Table 1: Secure Web Appliance - Tableau de prise en charge de la gamme ISE

Modèles	Échelle de session sans groupe AD activé	Échelle de session avec le groupe AD activé	
-	Nombre maximal de sessions actives prises en charge	Nombre maximal de sessions actives prises en charge	Nombre maximal de terminaux pris en charge (Entrées du groupe AD pour chaque utilisateur et point d'extrémité dans la base de données ISE.)
S680*, S690, S695	200 000	125 000	400 000
S380*, S390, S600V	150 000	50 000	150 000
S190, S195, S300V	50 000	50 000	75 000
S100V	50 000	40 000	50 000

Note *Les modèles S380 et S680 ne sont pas pris en charge.

Thèmes connexes

- À propos de pxGrid, on page 3
- À propos du déploiement et du basculement du serveur ISE/ISE-PIC, on page 3

À propos de pxGrid

La plateforme Platform Exchange Grid (pxGrid) de Cisco permet la collaboration entre les composants de l'infrastructure réseau, notamment les systèmes de supervision de la sécurité et de détection du réseau, les plateformes de gestion de l'identité et des accès, etc. Ces composants peuvent utiliser pxGrid pour échanger des informations par une méthode de publication/abonnement.

Il existe essentiellement trois composants pxGrid : le serveur de publication pxGrid, le client pxGrid et le contrôleur pxGrid.

- pxGrid Publisher : Fournit des informations sur le ou les clients pxGrid.
- Client pxGrid : tout système, comme le Secure Web Appliance, qui s'abonne aux informations publiées; dans ce cas, la balise de groupe de sécurité (SGT), les groupes Active Directory, le groupe d'utilisateurs et les informations de profilage.
- Contrôleur pxGrid : Dans ce cas, le nœud pxGrid ISE/ISE-PIC qui contrôle les processus d'enregistrement/de gestion et de sujet/abonnement du client.

Des certificats approuvés sont requis pour chaque composant et ceux-ci doivent être installés sur chaque plateforme hôte.

À propos du déploiement et du basculement du serveur ISE/ISE-PIC

La configuration d'un seul nœud ISE/ISE-PIC est appelée un déploiement autonome, et ce nœud unique exécute le service d'administration et des politiques. Pour prendre en charge le basculement et améliorer les performances, vous devez configurer plusieurs nœuds ISE/ISE-PIC dans un déploiement distribué. La configuration ISE/ISE-PIC distribuée minimale requise pour prendre en charge le basculement ISE/ISE-PIC sur votre Secure Web Appliance est de :

- Deux nœuds pxGrid
- Deux nœuds d'administration
- Un nœud de service de politique

Cette configuration est appelée « déploiement dans un réseau de taille moyenne » dans le *Guide d'installation du matériel de Cisco Identity Services Engine*. Reportez-vous à la section sur les déploiements réseau de ce guide d'installation pour en savoir plus.

Thèmes connexes

- Certificats ISE/ISE-PIC, on page 4
- Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 5
- Se connecter aux services ISE/ISE-PIC, on page 8
- Résolution des problèmes du service Cisco de vérification des identités, on page 16

Certificats ISE/ISE-PIC

Note Cette section décrit les certificats nécessaires pour une connexion ISE/ISE-PIC. Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 5 fournit des informations détaillées sur ces certificats. Certificate Management fournit des informations générales sur la gestion des certificats pour AsyncOS.

Un ensemble de deux certificats est requis pour l'authentification mutuelle et la communication sécurisée entre le Secure Web Appliance et chaque serveur ISE/ISE-PIC :

- **Certificat client d'appliance Web** – Utilisé par le serveur ISE/ISE-PIC pour authentifier Secure Web Appliance.
- **Certificat ISE pxGrid** : utilisé par Secure Web Appliance pour authentifier un serveur ISE/ISE-PIC sur le port 5222 pour Secure Web Appliance - Abonnement aux données ISE/ISE-PIC (requêtes publication/abonnement continues sur le serveur ISE/ISE-PIC).

Ces deux certificats peuvent être signés par l'autorité de certification (CA) ou autosignés. AsyncOS offre la possibilité de générer un certificat client d'appareil Web autosigné ou une requête de signature de certificat (CSR), si un certificat signé par une autorité de certification est nécessaire. De même, le serveur ISE/ISE-PIC offre la possibilité de générer des certificats pxGrid ISE/ISE-PIC autosignés, ou des requêtes de signature de certificat (CSR), si des certificats signés par une autorité de certification sont nécessaires.

Thèmes connexes

- Utilisation de certificats autosignés, on page 4
- Utilisation de certificats signés par une autorité de certification, on page 5
- Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC), on page 1
- Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 5
- Se connecter aux services ISE/ISE-PIC, on page 8

Utilisation de certificats autosignés

Lorsque des certificats autosignés sont utilisés sur le serveur ISE/ISE-PIC, le certificat ISE/ISE-PIC pxGrid développé sur le serveur ISE/ISE-PIC, ainsi que le certificat client d'appliance Web développé sur le Secure Web Appliance doivent être ajoutés dans le magasin des certificats approuvés sur le serveur ISE/ISE-PIC [sur **ISE** - Administration > Certificates > Trusted Certificates > Import (Administration > Certificats > Certificats approuvés > Importer); sur **ISE-PIC** - Certificates > Trusted Certificates > Import (Certificats > Certificats approuvés > Importer)].

Caution Nous vous déconseillons d'utiliser des certificats autosignés pour l'authentification, car leur sécurité n'est pas aussi élevée que les autres méthodes d'authentification. De plus, un certificat autosigné ne prend pas en charge la politique de révocation.

Utilisation de certificats signés par une autorité de certification

Dans le cas de certificats signés par une autorité de certification :

- Sur le serveur ISE/ISE-PIC, assurez-vous que le certificat racine de l'autorité de certification approprié pour le certificat client d'appliance Web est présent dans le magasin des certificats approuvés [Administration > Certificates > Trusted Certificates (Administration > Certificats > Certificats approuvés)].
- Sur le Secure Web Appliance, assurez-vous que les certificats racine de l'autorité de certification appropriés sont présents dans la liste des certificats approuvés [Network > Certificate Management > Manage Trusted Root Certificates (Réseau > Gestion des certificats > Gérer les certificats racine approuvés)].
- Sur la page de moteur ISE (Network (Réseau) > Identity Services Engine), veillez à télécharger le certificat racine de l'autorité de certification pour le certificat ISE/ISE-PIC pxGrid.

Authentification secondaire

Pour les informations utilisateur qui ne sont pas disponibles dans ISE/ISE-PIC, vous pouvez configurer une authentification de secours. Assurez-vous de disposer des éléments suivants pour réussir l'authentification de secours.

- Profil d'identification configuré avec une option de repli de domaine basé sur Active Directory.
- Politique d'accès avec le profil d'identification approprié qui contient l'option de secours.

Tâches relatives à l'intégration du service ISE/ISE-PIC

Note

- ISE/ISE-PIC version 2.4 et PxGrid version 2.0 sont pris en charge.
- Pour continuer à utiliser les politiques d'accès existantes avec ISE-PIC, vous devez modifier les profils d'identification respectifs pour utiliser ISE-PIC et identifier les utilisateurs de manière transparente. Cela s'applique aux profils d'identification qui utilisent CDA. Si vous migrez d'une identification CDA à une identification basée sur ISE-PIC, vous devez modifier les profils d'identification respectifs.

Note

- Reconfigurez ISE sur Secure Web Appliance si vous effectuez une mise à niveau depuis AsyncOS 11.5 ou versions antérieures vers AsyncOS 11.7 ou versions ultérieures.
- Le certificat doit être généré par le périphérique ISE/ISE-PIC et le certificat généré doit être téléchargé vers Secure Web Appliance.

Étape	Tâche	Liens vers les rubriques et les procédures
1	Générer un certificat à l'aide d'un périphérique ISE/ISE-PIC	Génération de certificats par ISE/ISE-PIC, on page 6
2	Configurez l'ISE/ISE-PIC pour l'accès Secure Web Appliance.	Configuration du serveur ISE/ISE-PIC pour l'accès Secure Web Appliance , on page 7
3	Configurez et activez les services ISE/ISE-PIC dans Secure Web Appliance.	Se connecter aux services ISE/ISE-PIC, on page 8
4	Si le certificat client Secure Web Appliance est autosigné, importez-le dans ISE/ISE-PIC.	Importer le certificat client Secure Web Appliance autosigné dans le déploiement autonome ISE/ISE-PIC, on page 10 Importer le certificat client Secure Web Appliance autosigné dans le déploiement distribué ISE/ISE-PIC, on page 10
5	Si nécessaire, configurez la journalisation dans Secure Web Appliance.	Configuration de la journalisation pour ISE/ISE-PIC, on page 12
6	Obtenez les détails du serveur ISE/ISE-PIC ERS.	Acquisition de détails sur le serveur ERS ISE/ISE-PIC provenant d'ISE/ISE-PIC, on page 12

Thèmes connexes

- Survol du moteur du service de vérification des identités Identity Services Engine (ISE) et du service du connecteur d'identité passive ISE (ISE-PIC), on page 1
- Certificats ISE/ISE-PIC, on page 4
- Résolution des problèmes du service Cisco de vérification des identités, on page 16

Génération de certificats par ISE/ISE-PIC

Remarque Le certificat généré par le périphérique ISE ou ISE-PIC doit être au format PKCS12.

- **ISE/ISE-PIC :**

Étape 1 Choisissez **Work Centres** > **PassiveID** > **Subscribers** > **Certificates** (Postes de travail > PassiveID > Abonnés > Certificats).

Étape 2 Choisissez le **format PKCS 12** dans la liste déroulante **Certificate Download Format** (Format de téléchargement de certificat). Saisissez d'autres informations appropriées dans l'onglet **Certificates** (Certificats), puis générez un certificat pxGrid.

Étape 3 Extrayez l'autorité de certification racine, le certificat client de l'appliance Web et la clé client de l'appliance Web du fichier XXX.pk12 généré à l'aide de la commande `openssl` :

- **Autorité de certification racine :** openssl pkcs12 -in XXX.p12 -cacerts -nokeys -chain -out RootCA.pem
- **Certificat client pour appliance Web :** openssl pkcs12 -in XXX.p12 -clcerts -nokeys -out publicCert.pem
- **Clé client de l'appliance Web :** openssl pkcs12 -in XXX.p12 -nocerts -nodes -out privateKey.pem

Remarque Utilisez le même mot de passe de certificat que celui que vous avez saisi sur l'interface Web d'ISE lors de l'exécution de l'étape 2.

Remarque Suivez les mêmes étapes pour générer l'autorité de certification racine secondaire, le certificat client de l'appliance Web et la clé client de l'appliance Web au moyen du serveur ISE secondaire/de basculement.

Configuration du serveur ISE/ISE-PIC pour l'accès Secure Web Appliance

- **ISE**
  - Chaque serveur ISE doit être configuré pour permettre aux abonnés au sujet de l'identité (comme Secure Web Appliance) d'obtenir le contexte de session en temps réel.
    1. Choisissez **Administration** > **pxGrid Services** > **Settings** > **pxGrid Settings** (Administration > Services pxGrid > Paramètres > Paramètres pxGrid).
    2. Assurez-vous que la case **Automatically approve new certificate-based accounts** (Approuver automatiquement les nouveaux comptes basés sur des certificats) est cochée.

    Supprimez tous les anciens Secure Web Appliance configurés qui ne participent à aucune authentification à l'aide d'ISE/ISE-PIC.

    Assurez-vous que le pied de page du serveur ISE est vert et indique **Connected to pxGrid** (Connecté à pxGrid).

- **ISE-PIC**
  - Chaque serveur ISE-PIC doit être configuré pour permettre aux abonnés à la rubrique d'identité (comme Secure Web Appliance) d'obtenir le contexte de session en temps réel.
    1. Choisissez **Subscribers** > **Settings** (Abonnés > Paramètres).
    2. Assurez-vous que la case **Automatically approve new certificate-based accounts** (Approuver automatiquement les nouveaux comptes basés sur des certificats) est cochée.

    Supprimez tous les anciens Secure Web Appliance configurés qui ne participent à aucune authentification à l'aide d'ISE/ISE-PIC.

    Assurez-vous que le pied de page du serveur ISE est vert et indique **Connected to pxGrid** (Connecté à pxGrid).

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Se connecter aux services ISE/ISE-PIC

Note Si l'administrateur ISE, les certificats pxGrid et MNT sont signés par votre certificat d'autorité de certification racine, téléchargez le certificat de l'autorité de certification racine dans les champs de certificat de nœud ISE pxGrid sur l'appliance [**Network** > **Identity Services Engine** (Réseau > Identity Services Engine)].

Before you begin

- Assurez-vous que chaque serveur ISE/ISE-PIC est configuré correctement pour l'accès Secure Web Appliance; voir Tâches relatives à l'intégration du service ISE/ISE-PIC, on page 5.
- Obtenir des clés et des certificats valides liés à ISE/ISE-PIC. Voir les informations connexes dans Génération de certificats par ISE/ISE-PIC, on page 6.
- Importez le fichier RootCA.pem obtenu dans Secure Web Appliance [**Network** > **CertificateManagement** > **TrustedRootCertificate** > **Client on ManageTrustedRootCertificate** (Réseau > CertificateManagement > TrustedRootCertificate > Client sur ManageTrustedRootCertificate)]. Pour extraire l'autorité de certification racine, le certificat client de l'appliance Web et la clé du client de l'appliance Web du fichier XXX.pk12 généré, consultez Génération de certificats par ISE/ISE-PIC, on page 6.

Note Suivez la même procédure pour le fichier rootCA.pem extrait du fichier XXXX.pk12 secondaire (si le serveur ISE secondaire ou de basculement est disponible).

- La page de configuration ISE de l'interface Web de Secure Web Appliance est utilisée pour configurer les serveurs ISE ou ISE-PIC, pour charger des certificats et pour la connexion aux services ISE ou ISE-PIC. Les étapes de configuration d'ISE ou d'ISE-PIC sont identiques, et tous les détails spécifiques aux configurations ISE-PIC ont été mentionnés, le cas échéant.
- Activez ERS si vous concevez des politiques d'accès à l'aide des groupes Active Directory fournis par ISE/ISE-PIC.

Étape 1 Choisissez **Network > Identification Service Engine** (Réseau > Moteur du service d'identification).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Si vous configurez ISE/ISE-PIC pour la première fois, cliquez sur **Enable and Edit Settings** (Activer et modifier les paramètres).

Étape 3 Cochez la case **Enable ISE service** (Activer le service ISE).

Étape 4 Identifiez le **nœud d'administration principal** à l'aide de son nom d'hôte ou de son adresse IPv4 et saisissez les informations suivantes dans l'onglet du **nœud pxGrid ISE principal** sur Secure Web Appliance.

a) Fournissez un **certificat de nœud pxGrid ISE** pour un Secure Web Applianceabonnement données -ISE/ISE-PIC (requêtes continues au serveur ISE/ISE-PIC).

Recherchez et sélectionnez le certificat (ou la chaîne de certificats qui comprend tout certificat intermédiaire) généré à partir du serveur ISE principal en tant qu'autorité de certification racine (c.-à-d. RootCA.pem); consultez

Génération de certificats par ISE/ISE-PIC, on page 6, puis cliquez sur **Upload File**(Charger le fichier). Voir Chargement d'un certificat et d'une clé pour de plus amples informations.

Étape 5 Si vous utilisez un deuxième serveur ISE/ISE-PIC pour le basculement, identifiez son **nœud d'administration principal** à l'aide de son nom d'hôte ou de son adresse IPv4 et fournissez les informations suivantes dans l'onglet **Secondary ISE pxGrid Node** (Nœud pxGrid ISE secondaire) sur le Secure Web Appliance en utilisant son nom d'hôte ou son adresse IPv4 .

a) Fournissez le **certificat de nœud ISE secondaire pxGrid**.

Recherchez et sélectionnez le certificat (ou la chaîne de certificats qui comprend tous les certificats intermédiaires) qui est généré à partir du serveur ISE secondaire en tant qu'autorité de certification racine (c.-à-d. **RootCA.pem**); consultez Génération de certificats par ISE/ISE-PIC, on page 6, puis cliquez sur **Upload File** (Charger le fichier); consultez Chargement d'un certificat et d'une clé pour obtenir des renseignements supplémentaires.

Note Pendant le basculement du serveur ISE principal vers les serveurs ISE secondaires, tout utilisateur qui ne figure pas dans le cache SGT ISE existant devra s'authentifier ou se verra attribuer une autorisation d'invité, selon votre configuration de Secure Web Appliance. Une fois le basculement ISE terminé, l'authentification ISE normale reprend.

Étape 6 Fournissez un **certificat client d'appliance Web** pour l'authentification mutuelle des serveurs Secure Web Appliance-ISE/ISE-PIC :

- **Utiliser le certificat et la clé chargés**

  Pour le certificat et la clé, cliquez sur Choose (Choisir) et accédez au fichier correspondant.

  Note Sélectionnez et chargez les fichiers publicCert.pem et privateKey.pem générés par le biais du périphérique ISE/ISE-PIC. Consultez Génération de certificats par ISE/ISE-PIC, on page 6.

  Si la **clé est chiffrée**, cochez cette case.

  Cliquez sur **Upload Files** (Charger des fichiers). (Voir Chargement d'un certificat et d'une clé pour en savoir plus sur cette option.)

Étape 7 Activez le service ISE SGT eXchange Protocol (SXP).

Pour plus d'informations sur l'activation de Secure Web Appliance en vue de récupérer les rubriques de liaison SXP à partir des services ISE, consultez Activation du protocole ISE-SXP pour le mappage des adresses SGT vers les adresses IP, on page 14.

Étape 8 Activez le service ERS (External Restful Service) ISE.

- Saisissez le nom d'utilisateur et le mot de passe de l'administrateur ERS. Voir Acquisition de détails sur le serveur ERS ISE/ISE-PIC provenant d'ISE/ISE-PIC, on page 12.
- Si le service ERS est disponible sur les mêmes nœuds ISE/ISE-PIC pxGrid, cochez la case **Server name same as ISE pxGrid Node** (Nom de serveur identique au nœud pxGrid ISE/ISE). Sinon, entrez les noms d'hôte ou les adresses IPv4 des serveurs principal et secondaires (si ceux-ci sont configurés).

Étape 9 Cliquez sur **Start Test** (Démarrer le test) pour tester la connexion avec le ou les nœuds pxGrid ISE/ISE-PIC.

Étape 10 Cliquez sur **Submit** (Soumettre).

What to do next

- Classification des utilisateurs et logiciels clients
- Créer des politiques pour contrôler les demandes Internet

Informations connexes

- http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html, en particulier « Comment intégrer Cisco Secure Web Appliance à l'aide d'ISE/ISE-PIC et TrustSec à l'aide de pxGrid. »

Importer le certificat client Secure Web Appliance autosigné dans le déploiement autonome ISE/ISE-PIC

Les étapes élémentaires sont les suivantes :

- **Nœud d'administration ISE**
  - Choisissez **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Administration > Certificats > Gestion des certificats > Certificats approuvés > Importer).

  Assurez-vous que les options suivantes sont cochées :
  - Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
  - Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
  - Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)
- **Nœud d'administration ISE-PIC**
  - Choisissez **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Certificats > Gestion des certificats > Certificats approuvés > Importer).

    Assurez-vous que les options suivantes sont cochées :
    - Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
    - Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
    - Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Importer le certificat client Secure Web Appliance autosigné dans le déploiement distribué ISE/ISE-PIC

Les étapes élémentaires sont les suivantes :

- **Nœud d'administration ISE :**
  - Choisissez **Administration** > **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Administration > Certificats > Gestion des certificats > Certificats approuvés > Importer).

Assurez-vous que les options suivantes sont cochées :

- Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
- Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
- Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)

- **Nœud d'administration ISE-PIC :**
  - Choisissez **Certificates** > **Certificate Management** > **Trusted Certificates** > **Import** (Certificats > Gestion des certificats > Certificats approuvés > Importer).

    Assurez-vous que les options suivantes sont cochées :
    - Trust for Authentication within ISE (Confiance pour l'authentification au sein d'ISE)
    - Trust for client authentication and syslog (Confiance pour l'authentification du client et syslog)
    - Trust for authentication of Cisco services (Confiance pour l'authentification des services Cisco)

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Remarque Dans un déploiement ISE distribué, Secure Web Appliance communique avec les nœuds MNT, PAN et PxGrid. Dans ce cas, les certificats ou l'émetteur de tous les certificats doivent être disponibles dans le « certificat racine extrait », c'est-à-dire dans l'autorité de certification racine qui est générée par le périphérique ISE ou ISE-PIC. Consultez Génération de certificats par ISE/ISE-PIC, à la page 6.

Étape 1 Suivez les étapes dans Génération de certificats par ISE/ISE-PIC, à la page 6 pour générer l'autorité de certification racine, le certificat client de l'appliance Web et la clé du client de l'appliance Web.

Étape 2 Sur le **nœud d'administration ISE/ISE-PIC**, exportez manuellement les certificats auto-signés en sélectionnant **ISE/ISE-PIC** > **Administration** > **System** > **Certificates** > **System Certificates** (ISE /ISE-PIC > Administration > Système > Certificats > Certificats système)

1. Sélectionnez un certificat qui est « Utilisé par » parmi les suivants : [pxGrid, EAP Authentication, Admin, Portal, RADIUS DTLS].
2. Cliquez sur **Export** (Exporter) et enregistrez le fichier .pem généré.

Répétez les étapes ci-dessus pour tous les nœuds distribués ISE/ISE-PIC.

Étape 3 Ajoutez manuellement les fichiers de certificat téléchargés dans RootCA.pem à l'aide des commandes `openssl`. Pour générer et extraire des fichiers de certificat dans rootCA.pem à l'aide du périphérique ISE/ISE-PIC, consultez Génération de certificats par ISE/ISE-PIC, à la page 6.

1. Exécutez la commande suivante sur le certificat téléchargé :

```
Example:

openssl x509 -in <DownloadCertificate>.pem -text | egrep "Subject:|Issuer:

Exemple (sortie) :
```

```
Issuer: CN=isehcamnt2.node
Subject: CN=isehcamnt2.node
```

2. Modifiez le contenu comme suit :

```
Example:
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

3. Ajoutez la ligne suivante dans le fichier RacineCA.pem :

```
Attributs du panier : <Empty Attributes>
```

4. Ajoutez l'objet et l'émetteur de l'étape (2) dans le fichier RootCA.pem avec l'étape (3).

```
Example:
Bag Attributes: <Empty Attributes>
Subject=/CN=isehcamnt2.node
Issuer=/CN=isehcamnt2.node
```

5. Copiez tout le contenu du fichier de certificat téléchargé et collez-le à la fin de l'autorité de certification racine, après les données de l'étape (4).

   Répétez les étapes (1) à (5) pour tous les certificats téléchargés de nœuds ISE/ISE-PIC distribués et enregistrez le certificat RacineCA modifié.

Étape 4 Chargez le fichier RootCA.pem modifié dans la page de configuration ISE de Secure Web Appliance. Consultez Se connecter aux services ISE/ISE-PIC, à la page 8.

Configuration de la journalisation pour ISE/ISE-PIC

- Ajoutez le champ personnalisé %m aux journaux d'accès pour consigner le mécanisme d'authentificationPersonnalisation des journaux d'accès : .
- Vérifiez que le journal de service ISE/ISE-PIC a été créé; si ce n'est pas le cas, créez-le —Ajout et modification d'abonnements aux journaux.
- Définissez les profils d'identification qui accèdent à ISE/ISE-PIC pour l'identification et l'authentification des utilisateurs—Classification des utilisateurs et des logiciels client, à la page 117.
- Configurez des politiques d'accès qui utilisent l'identification ISE/ISE-PIC pour définir les critères et les actions relatives aux demandes des utilisateurs—Configuration des politiques, à la page 191.

Acquisition de détails sur le serveur ERS ISE/ISE-PIC provenant d'ISE/ISE-PIC

- Activez l'API REST de Cisco ISE dans ISE/ISE-PIC (les API utilisent le port HTTPS 9060).

Note Vous devez activer le service externe de repos (ERS) d'ISE sur Secure Web Appliance [Network > Identity Services Engine (Réseau > Moteur ISE)] pour configurer des politiques de sécurité basées sur les groupes. Cela s'applique à la version 11.7 et ultérieure.

- **ISE**

- Choisissez **Administration** > **Settings** > **ERS Settings** > **ERS settings for primary admin node** > **Enable ERS** (Administration > Paramètres > Paramètres ERS pour le nœud d'administration principal > Activer ERS).

  Activez **ERS for Read for All Other Nodes** (Lecture ERS pour tous les autres nœuds), s'il y a des nœuds secondaires.

- **ISE-PIC**
  - Choisissez **Settings** > **ERS Settings** > **Enable ERS** (Paramètres > Paramètres ERS) > Activer ERS).

- Assurez-vous d'avoir créé un administrateur ISE avec le bon groupe de services RESTful externes. Le groupe d'administration des services RESTful externe a un accès complet à toutes les API du serveur ERS (GET, POST, DELERE, PUT). Cet utilisateur peut créer, lire, mettre à jour et supprimer des demandes d'API ERS. L'opérateur de services RESTful externe dispose d'un accès en lecture seule (demande GET uniquement).
  - **ISE**
    - Choisissez **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Users** (Administration > Système > Accès admin > Administrateurs > Utilisateurs admin).
  - **ISE-PIC**
    - Choisissez **Administration** > **Admin Access** > **Admin Users** (Administration > Accès admin > Utilisateurs admin).

Si le service ERS est disponible sur des serveurs distincts, et non sur les nœuds pxGrid ISE/ISE-PIC, vous aurez besoin des noms d'hôte ou adresses IPv4 des serveurs principal et secondaire (si configurés).

Pour plus d'informations, consultez la documentation de Cisco *Identity Services Engine*.

Configurer l'intégration d'ISE-SXP

Cette section aborde les points suivants :

À propos du protocole ISE-SXP pour le mappage SGT vers les adresses IP

SGT Exchange Protocol (SXP) est un protocole développé pour propager les liaisons IP-SGT sur les périphériques réseau. Une balise de groupe de sécurité (SGT) spécifie les privilèges d'une source de trafic dans un réseau sécurisé.

Vous pouvez intégrer le déploiement de Cisco Identity Services Engine (ISE) à Cisco Secure Web Appliance pour une authentification passive. Secure Web Appliance peut s'abonner aux mappages SXP à partir d'ISE. ISE utilise SXP pour propager la base de données de mappage SGT-adresses IP vers les périphériques gérés. Lorsque vous configurez Secure Web Appliance pour utiliser le serveur ISE, vous activez l'option pour qu'il écoute le sujet SXP d'ISE. Ainsi, Secure Web Appliance en apprendra davantage sur les serveurs SGT et les mappages d'adresses IP directement à partir d'ISE.

Secure Web Appliance génère des adresses IP d'authentification d'utilisateur fictives, qui comprennent l'adresse IP de la grappe ISE ainsi que l'adresse IP du client. Par conséquent, plusieurs adresses IP de clients peuvent être authentifiées sur l'adresse IP de la grappe.

Lignes directrices et limites relatives à la licence

Le protocole ISE-SXP pour le mappage SGT-adresses IP comprend les directives et les limites suivantes :

- Les terminaux compatibles avec IPv6 ne sont pas pris en charge dans la version 14.5 de Secure Web Appliance.
- Dans Secure Web Appliance la version 14.5, les noms d'utilisateur et le mappage de groupe ne sont pas disponibles dans les mappages SGT-adresses IP. Par conséquent, l'administrateur ne peut pas créer de politiques basées sur les utilisateurs et les groupes ISE dans Secure Web Appliance. Cependant, il peut être créé avec des balises SGT.
- Pour planifier l'horodatage de redémarrage pour le processus de téléchargement en bloc, vous devez configurer l'heure au format HH::MM dans les 24 heures pour redémarrer le processus configuré.

Remarque Il est recommandé de configurer l'heure à laquelle le processus d'authentification de l'utilisateur est indiqué comme étant inférieur à la journée. Par exemple, à 00:00 heure.

Prérequis

Le protocole ISE-SXP pour le mappage SGT-à-adresse IP nécessite la condition préalable suivante :

- Nécessite un certificat racine approuvé. Pour ajouter un certificat racine approuvé, consultez Gestion des certificats racine approuvés.

Activation du protocole ISE-SXP pour le mappage des adresses SGT vers les adresses IP

Tous les mappages définis dans ISE, y compris les mappages SGT-adresses IP peuvent être publiés par SXP. Vous pouvez récupérer les informations d'ISE-SXP à l'aide des mécanismes suivants :

- Téléchargement en bloc : après le redémarrage d'un processus géré, Secure Web Appliance envoie la demande de téléchargement en bloc au nœud de l'agrégateur ISE afin d'obtenir des informations sur toutes les entrées ISE-SXP disponibles sur le nœud de l'agrégateur. Vous pouvez planifier l'horodatage du redémarrage à l'aide de l'interface de ligne de commande AsyncOS.

- Mise à jour incrémentielle Secure Web Appliance : s'abonne sur un connecteur Web pour recevoir des messages de mise à jour incrémentielle. Il existe deux types de messages :
  - Create (Créer) : pour toutes les entrées nouvellement créées
  - Delete (Supprimer) : pour toutes les entrées SXP mises à jour

Remarque Secure Web Appliance reçoit deux messages (Delete suivi de Create) pour chaque entrée mise à jour.

Vous êtes autorisé à planifier le redémarrage.

Étape 1 Accédez à **Network** > **Identification Service Engine** (Réseau > Network Identification Service Engine).

Étape 2 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 3 Cochez la case **Enable ISE service** (Activer le service ISE).

Étape 4 Cochez la case **Enable** (Activer) pour permettre à Secure Web Appliance de récupérer les rubriques de liaison SXP des services ISE.

Par défaut, le service ISE SGT eXchange Protocol (SXP) est désactivé.

Étape 5 Cliquez sur **Start Test** (Démarrer le test) pour tester la connexion.

Remarque Les informations SXP ne s'affichent que si le service ISE-SGT eXchange Protocol (SXP) a été activé.

Étape 6 Cliquez sur **Submit** (Soumettre).

Vérification de la configuration du protocole ISE-SXP

Vous pouvez vérifier la configuration du protocole ISE-SXP en utilisant l'une des méthodes suivantes :

- Cliquez sur **Start Test** (Démarrer le test) dans le champ Activation du protocole ISE-SXP pour le mappage des adresses SGT vers les adresses IP, à la page 14 et vérifiez les informations affichées.
- Utilisez la commande **STATISTICS** sous la commande **ISEDATA** dans l'interface de ligne de commande AsyncOS (CLI).

Lorsque vous utilisez la commande **STATISTICS**, les informations suivantes s'affichent :

- Nom d'hôte ERS
- Heure de connexion ERS
- Téléchargement en bloc de session
- Téléchargement en bloc de groupe
- Téléchargement en bloc de SGT
- Téléchargement en bloc de SXP

- Mise à jour de la session
- Mise à jour de groupe
- Mise à jour SXP
- attribution de mémoire
- Désaffectation de mémoire
- Nombre total de sessions

Le nom d'utilisateur est généré dans le format suivant :

```
isesxp_<ISE-node-ip>_sgt<SGT number>_<Client IP address>
```

Par exemple : isesxp_10.10.2.68_sgt18_10.10.10.10

Authentification des utilisateurs VDI (Virtual Desktop Infrastructure) dans les intégrations ISE/ISE-PIC

Vous pouvez configurer une identification transparente avec ISE/ISE-PIC pour les utilisateurs dans des environnements VDI en fonction des ports source utilisés.

Vous devez installer l'agent Cisco Terminal Services (TS Agent) sur les serveurs VDI. L'agent Cisco TS fournit les renseignements d'identité à ISE/ISE-PIC. Les informations d'identité comprennent le domaine, le nom d'utilisateur et les plages de ports utilisées par chaque utilisateur.

- Téléchargez Cisco TS agent à partir du site d'assistance https://www.cisco.com/c/en/us/support/index.html.
- Consultez le Guide de l'agent pour les services Cisco Terminal Services (TS) https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html pour en savoir plus.
- Configurez le fournisseur d'API ISE/ISE-PIC pour qu'il fonctionne avec un agent Cisco TS. Consultez la documentation sur les agents Cisco TS pour en savoir plus sur l'envoi d'appels d'API.

Remarque

- L'authentification de secours pour les utilisateurs de l'environnement VDI n'est pas prise en charge.
- Assurez-vous que le nombre maximal de sessions de bureau à distance est le même dans les paramètres d'agent de Cisco Terminal Services et du serveur Microsoft. Cela empêche l'envoi d'informations de session incorrectes à Secure Web Appliance par ISE et permet d'éviter les fausses authentifications pour les nouvelles sessions.

Résolution des problèmes du service Cisco de vérification des identités

- Problèmes liés au service Cisco de vérification des identités

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.