Intégration avec Cisco SecureX et Cisco Threat Response

Cette rubrique contient les sections suivantes :

Intégration de votre appliance à Cisco SecureX ou Cisco Threat Response

Cisco SecureX est une plateforme de sécurité intégrée à tous les produits de sécurité Cisco. Cette solution est native dans le nuage, sans nouvelle technologie à déployer. Cisco SecureX simplifie les exigences de la protection contre les menaces en fournissant une plateforme qui unifie la visibilité, permet l'automatisation et améliore la sécurité sur le réseau, les terminaux, le nuage et les applications. En connectant la technologie dans une plateforme intégrée, Cisco SecureX fournit des informations mesurables, des résultats souhaitables et une collaboration entre les équipes inégalée. Cisco SecureX vous permet d'étendre vos capacités en connectant votre infrastructure de sécurité.

Le service d'intégration de l'appliance à Cisco SecureX ou Cisco Threat Response contient les sections suivantes :

- Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response, à la page 2
- Analyse des menaces à l'aide du ruban Cisco SecureX, à la page 6

Vous pouvez intégrer votre appliance à Cisco SecureX ou Cisco Threat Response et effectuer les actions suivantes dans Cisco SecureX ou Cisco Threat Response :

- Affichez et envoyez les données Web de plusieurs appliances de votre organisation.
- Identifiez, étudiez et corrigez les menaces observées dans les rapports Web et le suivi.
- Bloquez les URL ou le trafic Web compromis.

- Résoudre rapidement les menaces identifiées et fournir des recommandations de mesures à prendre contre les menaces identifiées.
- Documentez les menaces pour enregistrer l'enquête et permettre l'échange d'informations entre d'autres appliances.
- Bloquez les domaines malveillants, suivez les observations suspectes, lancez un flux de travail d'approbation ou créez un dossier informatique pour mettre à jour la politique Web.

Vous pouvez accéder à Cisco SecureX ou à Cisco Threat Response en utilisant l'URL suivante :

https://securex.us.security.cisco.com/login

Cisco Secure Web Appliance fournit des fonctionnalités avancées de protection contre les menaces qui détectent, bloquent et éliminent les attaques plus rapidement, qui empêchent la perte de données et qui sécurisent les informations importantes en transit avec un chiffrement de bout en bout. Pour en savoir plus sur les observables qui peuvent être enrichies par le module Secure Web Appliance, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX et cliquez sur **En savoir plus**.

Lorsque vous intégrez Cisco Secure Web Appliance à SecureX, les données de suivi Web de Secure Web Appliance sont validées. L'expiration du délai de transaction (60 secondes) se produit en raison du retard de traitement sur Secure Web Appliance, ce qui entraîne un échec de l'intégration. Réduisez la limite de temps d'intégration de 30 jours par défaut à 1 ou 2 jours pour une intégration réussie. Cependant, cette réduction aura une incidence sur l'efficacité de la supervision de Cisco Secure Web Appliance.

Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response

Tableau 1 : Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response

	Faire ceci	Plus d'informations
Étape 1	Passez en revue les conditions préalables.	Prérequis, à la page 3
Étape 2	Sur votre Secure Web Appliance, activez l'intégration Cisco SecureX ou Cisco Threat Response.	Activez l'intégration de Cisco SecureX ou Cisco Threat Response sur votre Secure Web Appliance Cisco, à la page 3
Étape 3	Sur Cisco SecureX, ajoutez votre appliance en tant que périphérique, enregistrez-la et générez un jeton d'enregistrement.	Pour en savoir plus, consultez https://securex.us.security.cisco.com/help/settings-devices
Étape 4	Sur votre Secure Web Appliance, terminez l'enregistrement de Cisco SecureX ou Cisco Threat Response.	Enregistrement de Cisco SecureX ou de Cisco Threat Response sur Cisco Secure Web Appliance, à la page 4
Étape 5	Confirmer si l'enregistrement a réussi.	Confirmer la réussite de l'enregistrement, à la page 5

	Faire ceci	Plus d'informations
Étape 6	Sur Cisco SecureX, ajoutez le module d'appliance Cisco pour la sécurité du Web.	Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module Secure Web Appliance requis pour l'intégration dans Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Prérequis

Remarque Si vous avez déjà un compte d'utilisateur Cisco Threat Response, vous n'avez pas besoin de créer un compte d'utilisateur Cisco SecureX. Vous pouvez vous connecter à Cisco SecureX à l'aide des informations d'authentification de votre compte d'utilisateur Cisco Threat Response.

- Assurez-vous de créer un compte d'utilisateur dans Cisco SecureX avec des droits d'accès administrateur. Pour créer un nouveau compte d'utilisateur, accédez à la page **Cisco SecureX login** (Connexion à Cisco SecureX) en utilisant l'URL https://securex.us.security.cisco.com/login et cliquez sur **Create a SecureX Sign-on Account** (Créer un compte de connexion SecureX) dans la page de connexion. Si vous ne parvenez pas à créer un nouveau compte d'utilisateur, communiquez avec le service d'assistance technique de Cisco pour obtenir de l'aide.
- [Uniquement si vous n'utilisez pas de serveur proxy.] Assurez-vous d'ouvrir le port HTTPS (entrée et sortie) 443 sur le pare-feu pour les noms de domaine complets suivants afin d'enregistrer votre appliance auprès de Cisco SecureX ou Cisco Threat Response :
  - api-sse.cisco.com (applicable pour les utilisateurs NAM uniquement)
  - api.eu.sse.itd.cisco.com (uniquement applicable aux utilisateurs dans l'Union européenne)
  - api.apj.sse.itd.cisco.com (uniquement applicable aux utilisateurs dans la région APJC)
  - est.sco.cisco.com (applicable aux utilisateurs APJC, UE et NAM)

Activez l'intégration de Cisco SecureX ou Cisco Threat Response sur votre Secure Web Appliance Cisco

Étape 1 Connectez-vous à votre appliance.

Étape 2 Sélectionnez **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 3 Cliquez sur **Edit Settings** (Modifier les paramètres).

Étape 4 Cochez la case **Enable** (Activer).

Étape 5 Choisissez le serveur Cisco SecureX ou Cisco Threat Response requis pour connecter votre appliance à Cisco SecureX ou Cisco Threat Response.

Étape 6 Envoyez et validez vos modifications.

Étape 7 Attendez quelques minutes et vérifiez si le bouton **Register** (Enregistrer) apparaît sur votre appliance.

Prochaine étape

Enregistrez votre appliance sur Cisco SecureX ou Cisco Threat Response. Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Enregistrement de Cisco SecureX ou de Cisco Threat Response sur Cisco Secure Web Appliance

Étape 1 Accédez à **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 2 Dans les **Cloud Services Settings** (Paramètres des services en nuage), saisissez le jeton d'enregistrement, puis cliquez sur **Register** (Enregistrer).

Remarque Pour enregistrer Cisco SecureX ou Cisco Threat Response à l'aide de l'interface de ligne de commande, utilisez la commande `cloudserviceconfig`.

Prochaine étape

Confirmer la réussite de l'enregistrement, à la page 5

Enregistrement de Cisco Secure Web Appliance sur le portail Security Service Exchange (SSE) à l'aide de la licence Smart

Lorsque vous effectuez une mise à niveau vers AsyncOS 14.x, les services Cisco Cloud sont automatiquement activés si l'appliance est déjà enregistrée dans Cisco Smart Software Manager. Suivez les étapes ci-dessous pour ajouter votre appliance au portail SSE.

Étape 1 Planifiez une fenêtre de maintenance.

Étape 2 Accédez à **System Administration** > **Smart Software Licensing** (Administration système > Licences logicielles Smart).

Étape 3 Dans la liste déroulante **Action**, sélectionnez **Deregister** (Annuler l'enregistrement) et cliquez sur **Go** (OK).

Étape 4 Supprimez toutes les entrées SWA du portail SSE.

Étape 5 Accédez à **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 6 Cochez la case **Enable Cisco Cloud Services** (Activer les services Cisco Cloud).

Étape 7 Cliquez sur **Enable** (Activer).

Étape 8 Envoyez et validez vos modifications.

Étape 9 Collez le jeton d'enregistrement.

Étape 10 Cliquez sur **Register** (Enregistrer).

Confirmer la réussite de l'enregistrement

- Sur la plateforme Security Services Exchange, confirmez la réussite de l'enregistrement en vérifiant l'état dans la plateforme Security Services Exchange.
- Sur Cisco SecureX, accédez à la page **Devices** (Périphériques) et affichez le Secure Web Appliance qui a été enregistré auprès de la plateforme Security Services Exchange.

Remarque Si vous souhaitez passer à un autre serveur Cisco SecureX ou Cisco Threat Response (par exemple, « Europe - api.eu.sse.itd.cisco.com »), vous devez d'abord annuler l'enregistrement de votre appliance auprès de Cisco SecureX ou de Cisco Threat Response, puis suivre les étapes mentionnées dans Comment intégrer votre appliance à Cisco SecureX ou Cisco Threat Response, à la page 2.

Après avoir intégré votre appliance à Cisco SecureX ou Cisco Threat Response, vous n'avez pas besoin d'intégrer votre appliance Cisco de gestion de la sécurité à Cisco SecureX ou Cisco Threat Response.

Après l'enregistrement réussi de votre appliance sur la plateforme Security Services Exchange, ajoutez le module Web Secure Web Appliance sur Cisco SecureX. Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Activation du portail de services infonuagiques Cisco Secure Web Appliance

Étape 1 Connectez-vous à votre Secure Web Appliance.

Étape 2 Sélectionnez **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 3 Cliquez sur **Enable** (Activer).

Étape 4 Cochez la case **Enable Cisco Cloud Services** (Activer les services Cisco Cloud).

Étape 5 Choisissez le serveur Cisco Secure requis pour connecter votre Secure Web Appliance au portail de services Cisco Cloud.

Étape 6 Envoyez et validez vos modifications.

Étape 7 Attendez quelques minutes et vérifiez si le bouton **Register** (Enregistrer) apparaît sur la page **Cloud Services Settings** (Paramètres des services Cisco Cloud).

Remarque Pour activer le portail de services Cisco Cloud à l'aide de l'interface de ligne de commande, utilisez la commande `cloudserviceconfig`.

Prochaine étape

Enregistrer votre Secure Web Appliance sur le portail des services Cisco Cloud. Pour en savoir plus, accédez à https://securex.us.security.cisco.com/settings/modules/available, accédez au module à intégrer à Cisco SecureX, cliquez sur **Add New Module** (Ajouter un nouveau module) et consultez les instructions sur la page.

Enregistrement de Secure Web Appliance sur le portail des services Cisco Cloud

Étape 1 Accédez à **Network** > **Cloud Service Settings** (Réseau > Paramètres des services en nuage).

Étape 2 Saisissez le jeton d'enregistrement dans les paramètres des services Cisco Cloud et cliquez sur **Register** (Enregistrer) .

Remarque Pour enregistrer votre Secure Web Appliance auprès du portail des services Cisco Cloud à l'aide de l'interface de ligne de commande, utilisez la commande `cloudserviceconfig`.

Vous ne pouvez pas désactiver ou annuler l'enregistrement des services Cisco Cloud si une licence Smart est enregistrée sur votre appliance.

Analyse des menaces à l'aide du ruban Cisco SecureX

Remarque Lorsque vous passez à AsyncOS 14.0 ou à des versions antérieures, **Casebook** fait partie du ruban Cisco SecureX.

Cisco SecureX prend en charge un ensemble distribué de fonctionnalités qui unifient la visibilité, permettent l'automatisation, accélèrent les flux de travail de réponse aux incidents et améliorent la recherche de menaces. Ces fonctionnalités distribuées sont présentées sous forme d'applications (applis) et d'outils dans le ruban Cisco SecureX.

Cette rubrique contient les sections suivantes :

- Accès au ruban Cisco SecureX, à la page 7
- Ajout d'observable à Casebook pour l'analyse des menaces à l'aide du menu du ruban et du tableau croisé dynamique de Cisco SecureX, à la page 8

Vous trouverez le ruban Cisco SecureX dans le volet inférieur de la page et il persiste lorsque vous vous déplacez entre le tableau de bord et les autres produits de sécurité de votre environnement. Le ruban Cisco SecureX se compose des icônes et des éléments suivants :

- Développer/Réduire le ruban
- Accueil

- Application Casebook
- Application Incidents
- Application Orbital
- Case de recherche d'enrichissement
- Recherche d'observables
- Paramètres

Pour en savoir plus sur le ruban Cisco SecureX, consultez la page https://securex.us.security.cisco.com/help/ribbon.

Accès au ruban Cisco SecureX

Avant de commencer

Assurez-vous de remplir tous les préalables mentionnés dans Prérequis, à la page 3.

Remarque Supposons que vous ayez déjà configuré les versions antérieures de **Casebook** pour AsyncOS. Vous devez créer un nouvel **ID client** et un nouveau **secret client** dans le client API Cisco SecureX avec des étendues supplémentaires, comme mentionné dans la procédure suivante.

Vous pouvez faire glisser le Cisco SecureX Ribbon, placé dans le volet inférieur de la page, depuis la droite en utilisant le bouton  .

Étape 1 Connectez-vous à la nouvelle interface Web de votre appliance. Pour en savoir plus, consultez Interprétation des pages de rapports Web sur la nouvelle interface Web.

Étape 2 Cliquez sur le ruban Cisco SecureX.

Étape 3 Créez un **ID client** et un **secret client** dans les **clients API SecureX**. Pour en savoir plus sur la génération d'informations d'authentification de client API, consultez Création d'un client API.

Lors de la création d'un ID client et d'un mot de passe client, veillez à choisir les étendues suivantes :

- recueil
- enrich:read
- global-intel:read
- inspect:read
- integration:read
- profil
- private-intel

- response
- registry/user/ribbon
- telemetry:write
- users:read
- orbital (si vous y avez accès)

Étape 4 Saisissez le nom d'utilisateur et le mot de passe client obtenus à l'étape 3 dans la boîte de dialogue **Login to use SecureX Ribbon** (Se connecter pour utiliser le ruban SecureX) dans votre appliance.

Étape 5 Sélectionnez le serveur Cisco SecureX requis dans la boîte de dialogue **Login to use SecureX Ribbon** (Se connecter pour utiliser le ruban SecureX).

Étape 6 Cliquez sur **Authenticate** (Authentifier).

Remarque Si vous souhaitez modifier l'ID du client, le mot de passe du client et le serveur Cisco SecureX, faites un clic droit sur le ruban Cisco SecureX et ajoutez les détails.

Prochaine étape

Ajout d'observable à Casebook pour l'analyse des menaces à l'aide du menu du ruban et du tableau croisé dynamique de Cisco SecureX, à la page 8

Ajout d'observable à Casebook pour l'analyse des menaces à l'aide du menu du ruban et du tableau croisé dynamique de Cisco SecureX

Avant de commencer

Assurez-vous d'obtenir l'ID client et le mot de passe client pour accéder aux widgets du ruban et du menu croisé dynamique de Cisco SecureX sur votre appliance. Pour en savoir plus, consultez Accès au ruban Cisco SecureX, à la page 7.

Étape 1 Connectez-vous à la nouvelle interface Web de votre appliance. Pour en savoir plus, consultez Interprétation des pages de rapports Web sur la nouvelle interface Web.

Étape 2 Accédez à la page **Web Reporting** (Rapports Web), cliquez sur le bouton de menu croisé dynamique  à côté de l'observable requis (par exemple, bit.ly).

Procédez comme suit:

- Cliquez sur le bouton  pour ajouter un observable au dossier actif.
- Cliquez sur le bouton  pour ajouter l'observable au nouveau dossier.

Remarque

Utilisez le bouton du menu croisé dynamique pour faire basculer un observable par rapport à d'autres périphériques enregistrés sur le portail (par exemple, Cisco Secure Endpoint) afin de mener une recherche pour l'analyse des menaces.

Étape 3 Passez le curseur sur l'icône et cliquez sur le bouton pour ouvrir **Casebook**. Vérifiez si l'observable est ajouté à un nouveau dossier ou à un dossier existant.

Étape 4 (Facultatif) Cliquez sur le bouton pour ajouter un titre, une description ou des remarques à **Casebook**.

Remarque Vous pouvez rechercher des observables pour l'analyse des menaces de deux manières différentes :

- Cliquez sur la zone de recherche **Enrichment** (Enrichissement) dans le ruban Cisco SecureX et recherchez les observables.
- Cliquez sur l'icône **Casebook** dans le ruban Cisco SecureX et recherchez les observables dans le champ de recherche 

.

Pour en savoir plus sur le ruban Cisco SecureX, consultez la page https://securex.us.security.cisco.com/help/ribbon.

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.