



Migrer le Cisco Secure Firewall Threat Defense géré par Centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

- [À propos de la migration de Défense contre les menaces vers Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\), à la page 1](#)
- [Versions logicielles prises en charge de Cisco Secure Firewall Management Center et Cisco Secure Firewall Threat Defense pour la migration, à la page 2](#)
- [Licence, à la page 3](#)
- [Fonctionnalités prises en charge, à la page 3](#)
- [Fonctionnalités non prises en charge, à la page 6](#)
- [Lignes directrices de la migration et limites pour la configuration du VPN, à la page 7](#)
- [Gestion des événements et de l'analyse Threat Defense \(de défense contre les menaces\), à la page 8](#)
- [Avant d'entreprendre la migration, à la page 9](#)
- [Migrer Défense contre les menaces vers Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\), à la page 11](#)
- [Afficher une tâche de migration Défense contre les menaces, à la page 14](#)
- [Activer les paramètres de notifications, à la page 20](#)
- [Dépannage de la migration de Défense contre les menaces vers le nuage, à la page 20](#)

À propos de la migration de Défense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Les administrateurs Cisco Defense Orchestrator peuvent migrer les périphériques défense contre les menaces vers les périphériques Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) de centre de gestion de pare-feu local exécutant la version 7.2 ou une version ultérieure. En outre, vous pouvez migrer des périphériques vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à partir d'un centre de gestion de pare-feu local 1000/2500/4500, nous prenons en charge une mise à niveau *temporaire* de la version 7.0 à la version 7.4.

Avant de lancer le processus de migration, il est important de mettre à niveau les modèles centre de gestion de pare-feu local vers une version prise en charge CDO et de les intégrer à CDO. Ce n'est qu'après cette étape que vous pouvez procéder à la migration des périphériques associés à centre de gestion de pare-feu local.

Vous disposez d'une période d'évaluation de 14 jours pour examiner et évaluer les modifications apportées à la migration sur les périphériques défense contre les menaces avant que CDO ne les valide automatiquement. Pendant cette période d'évaluation, si vous n'êtes pas satisfait des modifications, vous pouvez soit annuler les modifications et continuer à gérer le périphérique avec le centre de gestion de pare-feu local, soit valider les modifications de migration. Il est important de noter qu'après l'expiration de la période d'évaluation, CDO validera automatiquement les modifications et qu'il ne sera plus possible de les annuler.

Après la migration des périphériques, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) intègre les périphériques défense contre les menaces et importe toutes les politiques partagées et les objets associés, les politiques spécifiques aux périphériques et la configuration des périphériques de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). De plus, les périphériques se trouvent sur la page **Inventaire** de CDO.



Remarque

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) gère tous les noms de politiques et d'objets en double qui sont identifiés au cours du processus de migration centre de gestion de pare-feu local. Cette méthode est décrite ultérieurement dans ce document.

Rôles d'utilisateur

Les rôles d'utilisateur de centre de gestion de pare-feu local ne sont plus applicables dans CDO après la migration. Votre autorisation d'effectuer des tâches sur le périphérique migré est fonction de votre rôle d'utilisateur dans CDO. Consultez la rubrique [Utilisateurs](#) pour comprendre le mappage des rôles utilisateur de centre de gestion de pare-feu local et Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Versions logicielles prises en charge de Cisco Secure Firewall Management Center et Cisco Secure Firewall Threat Defense pour la migration

Cette section décrit la configuration logicielle minimale requise pour la migration des périphériques Cisco Secure Firewall Threat Defense à partir des versions sur site Cisco Secure Firewall Management Center :

- centre de gestion de pare-feu local minimal : 7.2e
- défense contre les menaces minimale : 7.0.3 ou 7.2 (non pris en charge pour la version 7.1)

Modèles gérés 1000/2500/4500 du Centre de gestion de pare-feu local Défense contre les menaces

Vous pouvez migrer des périphériques vers le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) à partir d'un modèle centre de gestion de pare-feu local 1000/2500/4500. Nous prenons en charge une mise à niveau *temporaire* de la version 7.0 à la version 7.4. Vous pouvez télécharger l'ensemble de mise à niveau [ici](#).



Remarque

Le centre de gestion de pare-feu local 1000/2500/4500, vous auriez fait migrer des périphériques à partir de la version 7.4, qui n'est pas prise en charge pour les opérations générales, mais sert de solution provisoire jusqu'à ce que la migration soit terminée. Pour rétablir une version prise en charge de centre de gestion de pare-feu local, vous devez supprimer les périphériques migrés de nouveau, rétablir l'image à la version 7.0.x, restaurer à partir de la sauvegarde et réenregistrer les périphériques.

Décompressez en mode zip (mais ne décompressez pas en mode tar) le paquet de mise à niveau avant de le téléverser dans centre de gestion de pare-feu local. Pour effectuer une mise à niveau à la version 7.4, consultez [le Guide de mise à niveau de Cisco Cisco Secure Firewall Management Center, version 6.0-7.0](#).

Nous vous recommandons de mettre à niveau les périphériques à la version 7.0.x avant de mettre à niveau centre de gestion de pare-feu local à la version 7.4.



Important

Une mise à niveau est requise, car les centres centre de gestion de pare-feu local de la version 7.0 ne prennent pas en charge la migration du périphérique vers le nuage. La version 7.4 est uniquement prise en charge pendant le processus de migration et d'évaluation du périphérique. Ces centre de gestion de pare-feu local n'exécuteront aucune version intermédiaire. Seuls les périphériques autonomes et à haute disponibilité défense contre les menaces exécutant les versions 7.0.3+ (7.0.5 recommandées) sont admissibles à la migration.

Licence

- Lors de la migration de défense contre les menaces vers le nuage, toutes les licences de fonctionnalités associées au périphérique sont transférées à CDO et transférées de centre de gestion au groupement de licences Smart. Le périphérique récupère les licences spécifiques au périphérique lors de son enregistrement auprès de CDO. Vous n'avez pas besoin d'appliquer à nouveau la licence sur le périphérique.
- Les licences spécifiques au périphérique ne sont pas nécessaires si vous souhaitez conserver les périphériques dans la liste centre de gestion pour l'analyse.
- Assurez-vous d'avoir enregistré Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avec une licence Smart.

Fonctionnalités prises en charge

Gestion des politiques et des objets partagés

Lorsque le processus de migration commence, les politiques partagées et les objets associés qui sont associés aux périphériques défense contre les menaces sont importés en premier, suivis de la configuration du périphérique.

Les politiques partagées suivantes sont importées dans CDO après la modification de gestionnaire sur les périphériques défense contre les menaces :

- Contrôle d'accès
- IPS

Fonctionnalités prises en charge

- SSL
- Préfiltre
- NAT
- Qualité de service
- Identité
- Paramètres de la plateforme
- Flex config
- Analyse du réseau
- DNS
- Programme malveillant et fichiers
- Santé
- VPN d'accès à distance
- VPN de site à site

Si une politique ou un objet de CDO porte le même nom que la politique ou l'objet importé de centre de gestion de pare-feu local, CDO effectue les actions suivantes après avoir modifié la gestion avec succès.

Objets politiques	Condition	Action
Contrôle d'accès, SSL, IPS, préfiltre, NAT, QoS, identité, paramètres de plateforme, analyse de réseau, DNS, politiques de programmes malveillants et de fichiers.	Le nom de la politique Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) correspond à celui de la politique centre de gestion de pare-feu local.	La politique Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) est utilisée à la place de la politique importée de centre de gestion de pare-feu local.
Politique de groupe par défaut du VPN d'accès distant (RA) DfltGrpPolicy	La politique de groupe par défaut DfltGrpPolicy de centre de gestion de pare-feu local est ignorée.	La politique de groupe Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) par défaut DfltGrpPolicy existante est utilisée à la place.
Objets de réseau, de port	Le nom et le contenu des objets réseau et port dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) correspondent à ceux de centre de gestion de pare-feu local.	Les objets Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) existants de réseau et de port du même nom et contenu sont utilisés à la place des objets importés de centre de gestion de pare-feu local. Si l'objet a le même nom mais un contenu différent, un remplacement d'objet est créé.

Objets politiques	Condition	Action
Tous les autres objets		L'objet Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) existant est utilisé à la place de l'objet importé de centre de gestion de pare-feu local.

Tout objet d'alerte Syslog associé à la politique de contrôle d'accès est importé dans CDO.

Prise en charge de la migration pour Défense contre les menaces dans une paire à haute disponibilité

Vous pouvez migrer un périphérique d'une paire à haute disponibilité vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). La gestion des périphériques actifs et de secours est transférée vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).



Important Nous vous recommandons fortement de valider les modifications du gestionnaire avant d'effectuer toute opération avancée, comme la création de configurations à haute disponibilité ou la rupture de configurations à haute disponibilité à partir de centre de gestion sur les périphériques migrés.

L'exécution de telles tâches pendant la période d'évaluation n'est pas prise en charge et peut entraîner l'échec de la validation de la migration.

Prise en charge de la migration pour Centre de gestion dans une paire à haute disponibilité

Vous pouvez migrer les périphériques défense contre les menaces dans une paire à haute disponibilité de centre de gestion de pare-feu local vers le nuage.

Le centre de gestion de pare-feu local peut être intégré à l'aide de SecureX ou des informations d'identification avec la méthode SDC. Toujours intégrer le centre de gestion active et non le centre de secours.



Remarque Si vous avez déjà intégré un centre de gestion autonome et que vous l'avez configuré ultérieurement en tant que centre de gestion de secours, supprimez le centre de gestion de secours et intégrez le centre actif.

Points à retenir :

• Méthode d'intégration SecureX

- La rupture de la haute disponibilité n'est pas prise en charge pendant la période d'évaluation de 14 jours. Vous pouvez interrompre la haute disponibilité après avoir validé les modifications manuellement ou automatiquement après la période d'évaluation.
- Le basculement vers la haute disponibilité est pris en charge pendant la période d'évaluation de 14 jours.

• Méthode d'intégration des informations d'authentification utilisant le SDC

- La rupture de la haute disponibilité ou le basculement vers la haute disponibilité ne sont pas pris en charge pendant la période d'évaluation de 14 jours. Vous pouvez effectuer ces opérations après avoir validé les modifications, manuellement ou automatiquement après la période d'évaluation.
- Après un basculement, intégrez la nouvelle unité active, qui était auparavant en mode veille, puis démarrez une tâche de migration sur les périphériques.

Fonctionnalités non prises en charge

Les fonctionnalités de migration suivantes ne sont **pas** prises en charge actuellement :

- Migrer un périphérique défense contre les menaces d'une grappe.



Remarque

Vous pouvez intégrer des périphériques **déjà en grappe** qui ont été configurés pour être gérés par Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Vous pouvez également mettre en grappe des périphériques autonomes **après** les avoir intégrés à Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

- Migrer un périphérique défense contre les menaces enregistré uniquement à des fins d'analyse avec centre de gestion.

Les configurations suivantes ne sont pas importées de centre de gestion vers CDO dans le cadre de la migration :

- Widgets personnalisés, détecteurs d'applications, corrélation, alertes SNMP et par courriel, analyseurs, groupes, politique d'accès dynamique, configuration AMP personnalisée, utilisateurs, domaines, tâches de déploiement planifiées, configuration ISE, mises à jour planifiées de GeoDB, configuration Threat Intelligence Director, Dynamic Analysis Connections.
- L'objet de certificat interne d'ISE n'est pas importé dans le cadre de la migration. Vous devez exporter un nouveau certificat système ou un certificat et la clé privée associée à partir d'ISE et l'importer dans CDO.

Règles recommandées par Cisco Secure Firewall Firepower

La migration de défense contre les menaces vers le nuage entraîne la migration des recommandations de règles déjà associées à l'une des politiques de prévention des intrusions. Cependant, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne permet pas la génération de nouvelles recommandations de règles ou la mise à jour automatique des recommandations déjà migrées après la migration. En effet, Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne prend pas en charge les recommandations de règles. Consultez [Règles recommandées par Cisco automatiquement](#).

Analyse de réseau personnalisée

Si le périphérique est associé à une politique d'analyse de réseau personnalisée, vous devez supprimer toutes les références à cette politique de l'instance sur site avant la migration.

1. Connectez-vous à centre de gestion sur site.

2. Choisissez **Policies > Access Control** (contrôle d'accès).
3. Cliquez sur l'icône de modification dans la politique de contrôle d'accès pour laquelle vous souhaitez dissocier la Politique d'analyse de réseau (NAP) personnalisée, puis cliquez sur l'onglet **Advanced** (Avancé).
4. Dans la zone **Network Analysis and Intrusion Policies** (politiques d'analyse de réseau et de prévention des intrusions), cliquez sur l'icône de modification.
5. Dans la liste **Politique d'analyse de réseau par défaut**, sélectionnez une politique fournie par le système.
6. Cliquez sur **OK**.
7. Cliquez sur **Save** (Enregistrer) pour enregistrer les modifications, puis sur **Deploy** (Déployer) pour télécharger les modifications sur le périphérique.

Après la migration, vous pouvez créer manuellement la politique d'analyse de réseau dans CDO.

Lignes directrices de la migration et limites pour la configuration du VPN

Gardez les éléments suivants à l'esprit lorsque vous migrez un périphérique avec une configuration VPN.

Prise en charge de la migration pour la politique VPN d'accès à distance

Dans le cadre du processus de migration, CDO importe tous les paramètres d'une politique VPN d'accès à distance, à l'exception de ce qui suit :

- Remplacements d'objets

Si des remplacements sont utilisés dans l'objet d'ensemble d'adresses, vous devez les ajouter manuellement à l'objet importé en utilisant CDO, après la migration.

- Utilisateurs locaux.

Si le serveur d'authentification est configuré avec une base de données locale pour l'authentification des utilisateurs, l'objet de domaine local associé est importé dans CDO. Cependant, vous devez ajouter manuellement les utilisateurs locaux à l'objet de domaine local importé à l'aide de CDO, après la migration. Voir [Créer un domaine et un répertoire de domaine](#).

- Configuration de l'équilibrage de la charge du VPN d'accès à distance.
- Inscription de certificat VPN d'accès à distance avec configuration de domaine.

Effectuez les opérations suivantes après la migration pour inscrire le certificat avec la configuration de domaine :

1. Dans CDO, choisissez **Inventaire > FTD**.
2. Sélectionnez le FTD migré et dans la **gestion des périphériques** à droite, cliquez sur **Vue d'ensemble des périphériques**.
3. Choisissez **Devices** (appareils) **Certificates** (certificats)

Effectuez une des tâches suivantes :

- Si les certificats sont importés avec un état d' **Erreur**, cliquez sur l'icône **Refresh certificate status** (actualiser l'état du certificat) pour synchroniser l'état du certificat avec celui du périphérique. L'état du certificat devient vert.
- Si les certificats ne sont pas importés, vous devez ajouter manuellement les certificats définis dans la politique VPN d'accès à distance configurée dans centre de gestion.

Prise en charge de la migration pour la politique VPN de site à site

Après avoir sélectionné un périphérique défense contre les menaces avec une configuration VPN de site à site, CDO sélectionnera automatiquement tous ses homologues provenant de différentes topologies. En effet, les périphériques de la topologie VPN de site à site doivent être migrés ensemble pour assurer le succès de la migration.



Remarque Bien que l'assistant de migration ne répertorie pas les périphériques extranet qui y sont associés, ils seront tout de même inclus automatiquement lors du processus de migration.

CDO importe tous les paramètres d'une politique VPN de site à site, à l'exception de ce qui suit :

- Si des remplacements d'objets sont utilisés dans l'objet réseau, vous devez les ajouter manuellement à l'objet importé à l'aide de CDO, après la migration.
- Si le type d'authentification est configuré dans « Clé automatique prépartagée » dans centre de gestion de pare-feu local, CDO définit une nouvelle clé prépartagée pour le déploiement VPN après la migration. La clé prépartagée mise à jour ne rompt pas les tunnels existants et les nouveaux tunnels commencent à utiliser la nouvelle clé prépartagée.
- Lorsque les périphériques sont déplacés vers CDO et que les modifications doivent encore être validées, la politique VPN de site à site associée à ces périphériques peut être modifiée à l'aide de centre de gestion de pare-feu local, mais ne met pas à jour la configuration du périphérique dans CDO.
- Si des périphériques sont configurés pour les tunnels SASE sur Cisco Umbrella, évitez de migrer ces périphériques.

Gestion des événements et de l'analyse Threat Defense (de défense contre les menaces)

La gestion des événements et des analyses peut être conservée dans le centre de gestion de pare-feu local ou transférée à CDO, où les périphériques doivent être configurés pour envoyer les événements à CDO. Lors du lancement du processus de migration, vous êtes autorisé à choisir le gestionnaire auquel les événements de périphérique doivent être envoyés à des fins d'analyse.



Attention Si vous migrez des périphériques de centre de gestion de pare-feu local 1000/2500/4500, il n'est pas possible d'utiliser le centre de gestion de pare-feu local pour la gestion des événements en raison de la disponibilité limitée. Par conséquent, vous devez utiliser Security Analytics and Logging (OnPrem) ou Security Analytics and Logging (logiciel-Service Saas) pour que les périphériques envoient des événements à des fins d'analyse. Consultez [Cisco Security Analytics and Logging](#).

Si vous sélectionnez centre de gestion de pare-feu local pour l'analyse, CDO devient le gestionnaire des périphériques sélectionnés mais conserve une copie de ces périphériques sur centre de gestion de pare-feu local dans le mode d'analyse uniquement. Les périphériques continuent d'envoyer des événements vers centre de gestion de pare-feu local, et CDO gère les modifications de configuration.

Si vous sélectionnez CDO pour l'analyse, CDO devient le gestionnaire pour les périphériques sélectionnés et supprime ces périphériques de centre de gestion de pare-feu local. CDO gère à la fois les modifications de configuration et la gestion des événements et des analyses. Vous devez configurer les périphériques de défense contre les menaces pour qu'ils envoient des événements au nuage Cisco. Vous pouvez utiliser Security Services Exchange ou Cisco Secure Event Connector (SEC) pour envoyer des événements des périphériques à Cisco Secure Analytics and Logging (SAL) dans le nuage.

Avant d'entreprendre la migration

Avant de commencer le processus, assurez-vous que les conditions préalables suivantes sont respectées :

- Un détenteur CDO provisionné est enregistré avec une licence Smart.
- Le centre de gestion de pare-feu local est intégré à CDO. L'intégration de centre de gestion de pare-feu local intègre également tous les périphériques défense contre les menaces enregistrés sur ce centre de gestion de pare-feu local. Voir [Intégrer un FMC](#).



Remarque Créez un nouvel utilisateur dans le centre de gestion de pare-feu local avec le rôle d'administrateur ou un rôle d'utilisateur personnalisé avec des autorisations « Périphériques » et « Système » à des fins d'intégration.



Mise en garde Si vous intégrez un centre de gestion de pare-feu local à CDO et que vous vous connectez simultanément à ce centre de gestion de pare-feu local avec le même nom d'utilisateur, l'intégration échoue.

- Pour la migration centre de gestion de pare-feu local 1000/2500/4500 :
 - Exécutez la version 7.4 (disponible pour ces modèles sur une base temporaire). Nous recommandons que les périphériques exécutent la version 7.0.5.
 - Nous vous recommandons de créer une sauvegarde de centre de gestion de pare-feu local.
- Pour les versions centre de gestion de pare-feu local 6.5 à 7.1, consultez la rubrique *Sauvegarde de FMC* dans le [Guide de configuration du centre de gestion Cisco Firepower Management Center](#).

Pour la version centre de gestion de pare-feu local 7.2 et versions ult rieures, consultez la rubrique *Sauvegarde de Management Center* dans le [Guide d'administration de Cisco Secure Firewall Management Center](#).

- Les p riph riques d fense contre les menaces ne doivent pas  tre synchronis s et avoir de modifications en attente. La migration  choue sur un p riph rique si CDO identifie des modifications en attente sur ce p riph rique.
- Tous les p riph riques homologues dans une topologie VPN de site   site doivent  tre en ligne et n'avoir aucun d ploiement en attente.
- Centre de gestion de pare-feu local doit permettre au protocole HTTP/HTTPS sortant de t l verser les configurations dans Amazon S3.
- CDO importe l'objet d'alerte Syslog utilis  dans la politique de contr le d'acc s du r pertoire centre de gestion de pare-feu local. Si CDO contient d j  un objet d'alerte du m me nom, mais d'un type diff rent (SNMP, courriel), il est r utilis  lors de l'importation de la configuration.

L'utilisateur doit v rifier si le nom de l'objet Syslog correspond   l'objet SNMP ou   l'objet d'alerte par courriel existant dans CDO. Si le nom correspond, vous devez renommer l'objet Syslog dans centre de gestion de pare-feu local avant de commencer le processus de migration.

- Si vous tentez de migrer des pare-feu avec des objets texte FlexConfig d finis par le syst me modifi s d'un centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), les valeurs des objets texte FlexConfig d finis par le syst me modifi s ne sont pas migr es vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) et le d ploiement  chouera.

Pour  viter cela, effectuez les t ches suivantes avant de commencer la migration :

- Copiez les valeurs de l'objet texte FlexConfig modifi es de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) avant la migration.
- Lancez la migration de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) apr s avoir v rifi  les objets texte FlexConfig pr d finis.

La liaison de basculement   haute disponibilit  doit  tre en service

La liaison de basculement   haute disponibilit  doit  tre active pour une migration r ussie. Avant de lancer le processus de migration sur CDO, d terminez l' tat d'int grit  de la liaison de basculement sur centre de gestion de pare-feu local.

1. D terminez les interfaces de basculement de toutes les paires   haute disponibilit  vers lesquelles vous souhaitez migrer Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).
 1. Choisissez **Devices** (p riph riques) > **Device Management** (gestion des p riph riques) .
 2.   c t  de la paire de p riph riques   haute disponibilit  que vous souhaitez modifier, cliquez sur **modifier**  .
 3. Cliquez sur l'onglet **High Availability** (haute disponibilit ).
 4. Dans la zone **Liaison   haute disponibilit **, le champ **Interface** (interface) affiche l'interface de basculement utilis e dans la paire.

5. D terminez les interfaces utilis es pour la communication de basculement s'il y a plusieurs paires   haute disponibilit  pour la migration.
2. V rifiez l' tat de fonctionnement des interfaces de basculement.
 1. Choisissez **Devices** (p riph riques) **Device Management** (gestion des p riph riques).
 2. Cliquez sur **Health Monitor** (Moniteur d'int grit )   c t  de la paire de p riph riques   haute disponibilit  souhait e.
 3. Dans le volet gauche, d veloppez la paire   haute disponibilit  pour voir les p riph riques d fense contre les menaces.
 4. Cliquez sur le p riph rique indiqu  par le point d'exclamation (!).
 5. Cliquez sur le bouton **Critical** (critique) en haut.
L'**interface Status** ( tat de l'interface) affiche les erreurs associ es aux interfaces.
 6. Si l'interface de basculement est en panne, le message **Interface « failover_interfacename » has no link** s'affiche.



Remarque

Cependant, vous pouvez migrer la paire   haute disponibilit  vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) si vous constatez d'autres probl mes d'interface de donn es,   l'exception de l'interface de basculement.

7. Corrigez le probl me et cliquez sur **Sync from onprem fmc now** pour obtenir les derni res modifications sur le p riph rique.

Migrer D fense contre les menaces vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Proc dure

-  tape 1** Dans la barre de navigation   gauche, choisissez **Outils et services > Migrations > Migrer FTD vers cdFMC**.
-  tape 2** Cliquez sur  et s lectionnez **On-Prem-managed FMC-managed FTD to cdFMC** (FTD g r  par la FMC sur site vers cdFMC).

Remarque Vous ne pouvez lancer qu'une seule t che de migration   la fois.
-  tape 3** Dans la zone **Select OnPrem FMC** (S lectionnez FMC OnPrem), proc dez comme suit :
 1. Vous pouvez cliquer sur le lien **Onboard an FMC** (Int grer un FMC) pour int grer le centre de gestion de pare-feu local si vous ne l'avez pas encore fait. Voir [Int grer un FMC](#).

2. Sélectionnez centre de gestion de pare-feu local dans la liste disponible et cliquez sur **Next**(suivant).

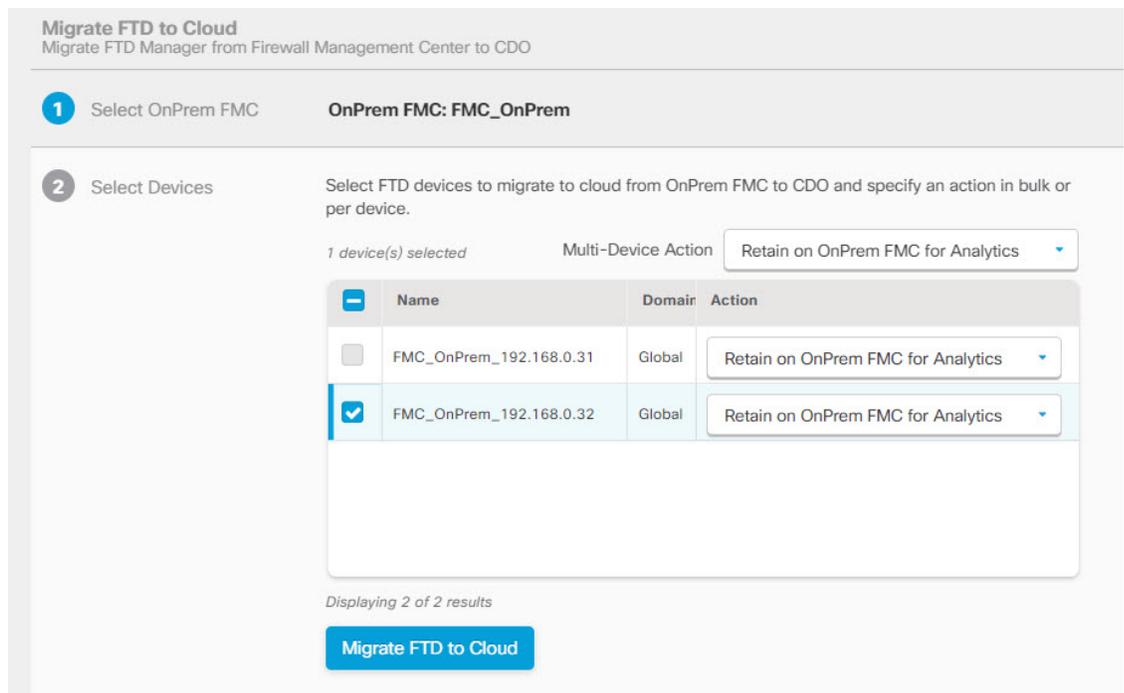
À l'étape de **sélection des périphériques**, vous verrez les périphériques défense contre les menaces gérés par le centre de gestion de pare-feu local sélectionné. Si une paire à haute disponibilité est configurée sur centre de gestion de pare-feu local, le nœud à haute disponibilité s'affichera à la place des périphériques actif et de secours.

Le champ **Last Synced time** (heure de la dernière synchronisation) indique le temps écoulé depuis la synchronisation de la configuration du périphérique dans centre de gestion de pare-feu local. Vous pouvez cliquer sur **Sync from OnPrem FMC Now** (Synchroniser à partir de FMC OnPrem Maintenant) pour récupérer les dernières modifications apportées au périphérique.

Étape 4

À l'étape de **sélection des périphériques**, procédez comme suit :

a) Sélectionnez les périphériques que vous souhaitez mettre à niveau.



Remarque • Les périphériques fonctionnant sur des versions non prises en charge ne sont pas disponibles pour la sélection.

• Les périphériques qui sont enregistrés pour l'analyse uniquement avec le centre de gestion de pare-feu local ou qui ont des modifications en attente à déployer ne sont pas admissibles à la migration.

• Lorsque vous sélectionnez un périphérique associé à une topologie VPN de site à site, CDO sélectionne automatiquement ses périphériques homologues appartenant à la même topologie ou à une topologie différente, car tous les périphériques de la topologie VPN de site à site doivent être migrés ensemble pour une migration réussie. L'assistant ne répertorie pas les périphériques extranet, le cas échéant. Cependant, CDO migre les périphériques extranet.

La colonne **S2S VPN Topology** (Topologie VPN S2S) indique le nombre de topologies VPN de site à site auxquelles participe un périphérique sélectionné. Vous cliquez sur le lien de topologie pour afficher les topologies et les périphériques qui sont migrés avec le périphérique sélectionné. Ce champ ne s'applique pas aux périphériques qui ne font pas partie de la topologie VPN de site à site.

• Une paire à haute disponibilité est présentée comme un nœud unique. Vous devez sélectionner ce nœud pour inclure les périphériques actifs et en veille dans la migration.

b) Dans la liste **Action multi-périphériques**, vous pouvez choisir une action commune à appliquer à tous les périphériques.

c) Dans la colonne **Commit Action** (valider l'action), vous pouvez choisir l'une des actions suivantes pour le périphérique sélectionné :

• **Retain on OnPrem FMC for Analytics** (Conserver sur OnPrem FMC pour l'analyse) : une fois le processus de migration terminé, la gestion des analyses pour les périphériques défense contre les menaces sélectionnés est conservée sur centre de gestion de pare-feu local.

• **Delete FTD from OnPrem FMC** (Supprimer FTD de OnPrem FMC : une fois le processus de migration terminé, les périphériques sélectionnés sont supprimés de centre de gestion de pare-feu local et sont disponibles pour CDO pour gérer les analyses. Vous devez configurer les périphériques pour qu'ils envoient des événements à CDO pour gérer les analyses. Lorsque les périphériques sont supprimés de centre de gestion de pare-feu local, ils ne peuvent pas être révoqués.

Important Pour les centre de gestion de pare-feu local 1000/2500/4500, lorsque vous sélectionnez les périphériques à migrer, assurez-vous de choisir **Delete FTD from OnPrem FMC** (Supprimer FTD de FMC OnPrem). Notez que le périphérique n'est pas entièrement supprimé, sauf si vous validez les modifications ou que 14 jours s'écoulent.

Remarque Les actions spécifiées ici sont validées automatiquement après la période d'évaluation de 14 jours ou après que les modifications aient été validées manuellement.

Étape 5

Par défaut, la case à cocher **Déploiement automatique sur FTD après réussite de la migration** est cochée pour déployer automatiquement la configuration migrée sur le périphérique après la réussite de la migration et de l'enregistrement du périphérique auprès de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Toutefois, si vous préférez examiner et déployer manuellement la configuration à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) après une migration réussie, vous pouvez décocher cette option et passer à l'étape suivante.

Étape 6 Cliquez sur **Migration de FTD vers cdFMC**

Étape 7 Cliquez sur **Afficher la progression de la migration vers le nuage** pour voir la progression.

Prochaine étape

Vous pouvez afficher l'état général et individuel des tâches de migration et générer un rapport lorsqu'une tâche est terminée avec succès. Consultez [Afficher une tâche de migration Défense contre les menaces, à la page 14](#).

Afficher une tâche de migration Défense contre les menaces

Le tableau de bord de la migration fournit l'état de toutes les tâches de migration lancées à partir de CDO. Vous pouvez développer une tâche spécifique pour voir l'état des périphériques associés à ce détenteur. Cela vous permet de suivre la progression de votre migration et de repérer les problèmes, le cas échéant, à résoudre.

Si vous avez configuré des alertes pour les flux de travail des périphériques, cliquez sur l'icône de notifications



pour voir les alertes qui ont été déclenchées pendant le processus de migration. En outre, si vous avez choisi de recevoir les notifications par courriel de CDO, vous recevrez également une notification par courriel concernant les alertes, le cas échéant.

À propos de la période d'évaluation de 14 jours

Lorsqu'une tâche de migration est réussie, vous avez 14 jours pour tester et évaluer les modifications apportées à la migration à l'aide de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Si vous êtes convaincu des modifications apportées à la migration, nous vous recommandons de valider les périphériques manuellement et de ne pas attendre que CDO valide automatiquement les modifications apportées à la migration. Voir [Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\)](#).

Notez que pour les centre de gestion de pare-feu local 1000/2500/4500, vous auriez dû migrer les périphériques à partir de la version 7.4, qui n'est pas prise en charge pour les opérations générales. Pour rétablir une version prise en charge de centre de gestion de pare-feu local, vous devez supprimer les périphériques migrés de nouveau, rétablir l'image à la version 7.0.x, restaurer à partir de la sauvegarde et réenregistrer les périphériques.



Remarque

- Vous ne pouvez pas révoquer les actions spécifiées dans la fenêtre de validation de la migration après avoir validé les modifications.
- Vous pouvez annuler la migration pendant la période d'évaluation et restaurer le périphérique à centre de gestion de pare-feu local.
- Vous ne pouvez pas supprimer de périphérique de centre de gestion de pare-feu local ou de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) pendant la période d'évaluation.

**Important**

Des modifications peuvent être apportées et déployées sur le périphérique en utilisant CDO pendant la période d'évaluation. Si vous remettez la gestion des périphériques sur centre de gestion de pare-feu local, les modifications spécifiques à CDO effectuées pendant la période d'évaluation ne sont pas enregistrées sur le périphérique une fois qu'il est revenu au détenteur source CDO. Vous devez déployer les modifications de centre de gestion de pare-feu local sur le périphérique après avoir rétabli le gestionnaire du périphérique.

- **Name** : représente le nom de la tâche qui comprend le nom centre de gestion de pare-feu local, ainsi que la date et l'heure de lancement de la tâche.
- **Number of FTD** : affiche le nombre total de périphériques qui sont migrés vers le nuage.
- **Status(état)** : affiche l'état de la tâche. Développez la tâche pour voir l'état des périphériques individuels.

Lorsqu'une tâche est terminée avec succès, le message **La tâche de migration FTD est réussie** s'affiche dans la colonne d'état. Vous pouvez cliquer sur l'info-bulle pour voir le nombre de jours restants pour l'évaluation du gestionnaire.

Vous pouvez cliquer sur [Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\)](#) pour valider les modifications manuellement avant la fin de la période d'évaluation de 14 jours.

- **Dernière mise à jour** : affiche la date et l'heure qui sont mises à jour uniquement lors d'une modification apportée au périphérique.



- **Actions** : cliquez sur  pour exécuter les actions suivantes :
 - **Flux de travail** : vous transfère aux **flux de travail** pour surveiller le travail.
 - **Télécharger le rapport** : vous permet de générer et de télécharger un rapport pour chaque tâche terminée avec succès. Consultez [Générer un rapport de migration Défense contre les menaces](#), à la page 19.
 - **Valider les changements du gestionnaire** : vous permet d'appliquer les modifications manuellement aux périphériques avant la fin de la période d'évaluation. Consultez [Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\)](#), à la page 16.
 - **Supprimer la tâche de migration** : vous permet de supprimer une tâche terminée. Le lien est disponible uniquement pour les tâches terminées. Consultez [Supprimer une tâche de migration](#), à la page 19.

Après une migration réussie, CDO déploie la configuration sur le périphérique. Si le système détecte des erreurs ou des avertissements dans les modifications à déployer, il les affiche dans la fenêtre **Validation Messages** (messages de validation). Pour afficher tous les détails, cliquez sur l'icône en forme de flèche avant les avertissements ou les erreurs. Si le déploiement échoue, consultez la section des *bonnes pratiques en matière de déploiement de modifications de configuration* du [Guide de configuration des périphériques du centre de gestion Cisco Firepower Management Center X.Y.](#)

Configurer la séquence Relam pour la politique d'identité

Si le périphérique contient une politique d'identité avec une configuration de domaine ou ISE, configurez votre appareil en tant que serveur mandataire pour que CDO communique avec la source d'identité. Les politiques d'identité ne fonctionnent pas si CDO ne parvient pas à se connecter aux domaines d'identité.

Une bulle d'aide s'affiche dans la colonne **Status** (état) pour un périphérique qui nécessite une configuration supplémentaire.



1. Cliquez sur l'icône d'info-bulle, puis sur **En savoir plus**.
2. Dans la fenêtre **Configure Proxy** (Configurer le serveur mandataire), cliquez sur **Configure my Realms** (configurer mes domaines).

Pour ajouter une séquence de serveur mandataire, consultez la section *Créer une séquence de serveur mandataire* du [Guide de configuration des périphériques du Firepower Management Center, version 7.2](#).

Valider manuellement les modifications de la migration dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Nous vous recommandons de valider manuellement les modifications apportées à la migration si vous êtes convaincu de vos modifications et que vous n'attendez pas que Cisco Defense Orchestrator valide automatiquement les modifications. La fenêtre **Valider les modifications de migration** affiche le nombre de jours restants pour valider la migration vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ou rétablir l'état du périphérique à centre de gestion de pare-feu local. Pendant la période d'évaluation, vous pouvez modifier les actions pour les périphériques de défense contre les menaces sélectionnés avant de valider les modifications. Une fois les modifications validées, vous ne pouvez plus révoquer les actions.



Remarque Les actions de modification du gestionnaire de validation sont désactivées dans les conditions suivantes :

- La période d'évaluation de 14 jours est écoulée.
- Les périphériques défense contre les menaces ont été remplacés par centre de gestion de pare-feu local ou supprimés de centre de gestion de pare-feu local, auquel cas aucune autre action ne peut être effectuée.

Procédure

- Étape 1** Dans la page des tâches de migration, cliquez sur le bouton  dans la colonne **Actions** d'une tâche terminée.
- Étape 2** Cliquez sur **Valider les modifications de migration**. (Ce lien est disponible uniquement lorsqu'une tâche est terminée avec succès.)
- Étape 3** Sélectionnez un périphérique et dans la liste **Commit Actions** (actions de validation), choisissez l'une des actions suivantes :

- **Conserver sur OnPrem FMC pour les analyses** : une fois les modifications validées, la gestion des analyses pour les périphériques défense contre les menaces sélectionnés est conservée sur le centre de gestion.
- **Supprimer Défense contre les menaces de OnPrem FMC** : après la validation des modifications, les périphériques sélectionnés sont supprimés de centre de gestion de pare-feu local et sont disponibles pour que Cisco Defense Orchestrator gère les analyses. Vous devez configurer défense contre les menaces pour envoyer des événements à Cisco Defense Orchestrator pour gérer les analyses. Une fois que les périphériques défense contre les menaces ont été supprimés du centre de gestion de pare-feu local, ils ne peuvent pas être révoqués.
- **rétablir le Manager à OnPrem FMC** : après la validation des modifications, la gestion des périphériques est rétablie à centre de gestion de pare-feu local à partir de Cisco Defense Orchestrator.

Remarque • Après avoir effectué cette action, vous ne pouvez plus modifier la gestion du périphérique sur Cisco Defense Orchestrator.

Solution de contournement : vous devez retirer le périphérique de centre de gestion de pare-feu local et l'intégrer. Ensuite, vous pourrez modifier la gestion du périphérique dans Cisco Defense Orchestrator.

- Après avoir effectué cette action, le périphérique n'affiche pas d'état « Out-of-date » dans centre de gestion de pare-feu local.

Solution de contournement : sur le site local centre de gestion de pare-feu local, déployez les modifications sur le périphérique.

Étape 4

Cliquez sur **Commit** (Valider) pour exécuter les actions que vous avez spécifiées immédiatement sans autre confirmation.

Dans l'écran des tâches de migration, vous pouvez développer la tâche pour vérifier la progression des actions spécifiées.

Les périphériques migrés apparaissent sur la page d'**inventaire** de CDO. Ces périphériques peuvent être gérés à l'aide du portail Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) qui est lié à CDO. Assurez-vous de déployer les modifications sur les périphériques à partir de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Afficher les périphériques migrés

Les périphériques migrés apparaissent sur la page **Inventaire** de CDO. Vous pouvez effectuer le lancement croisé et configurer la fonctionnalité requise sur Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).



Remarque

Les périphériques sur la page de liste des périphériques Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peuvent afficher `NO-IP` au lieu de l'adresse IP de gestion du périphérique. Comme l'enregistrement du périphérique utilise l'ID NAT, le périphérique lance le processus et, par conséquent, les adresses IP de gestion ne sont ni découvertes, ni utilisées pour la connexion. Notez que cela s'applique aux périphériques nouvellement intégrés et aux périphériques migrés à partir de centre de gestion de pare-feu local.

Exemple de périphérique Défense contre les menaces, analyse seulement

CDO crée deux instances du même périphérique qui est configuré pour rester sur centre de gestion pour analyse.

Name	Version	Location	Access Policy	Last Deploy	Configuration Status	Connectivity
10.10.16.13 FTD	7.2.0	-	test-policy-1855	-	Synced	Online
FMC_Beta2_OnPremFTD-141 FMC FTD	7.2.0	...		-	Synced	Online
FMC_Beta2_OnPremFTD-146 FMC FTD	7.2.0	...		-	Synced	Online
FMC_Beta2_OnPremFTD136 FMC FTD	7.2.0	...		-	Synced	Online
FMC_Beta2_eventsFtd-16-83 FMC FTD - Analytics Only	7.2.0	...		-	Synced	Online
eventsFtd-16-83 FTD	7.2.0	-	OnPremACPolicy	-	Synced	Online

L'instance de périphérique avec les étiquettes **FMC FTD** et **Analytics Only** indique que centre de gestion gère les analyses. L'instance de périphérique avec l'étiquette **FTD** indique que CDO gère sa configuration.

Vous pouvez gérer la configuration du périphérique à l'aide de CDO. Pour voir le périphérique dans Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), procédez comme suit :

Sélectionnez le périphérique ayant l'étiquette **FTD** et dans le volet **Management** (Gestion) à droite, cliquez sur **Device Summary** (Résumé du périphérique).

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
eventsFtd-16-83 N/A - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	OnPremACPolicy	

Vous pouvez afficher les événements du périphérique dans centre de gestion. Pour voir les événements, procédez comme suit :

1. Sélectionnez le périphérique ayant les étiquettes **FMC FTD** et **Analytics Only** (Analyse uniquement) et cliquez sur le lien **Manage Devices** (Gérer les périphériques) à droite.
2. Connectez-vous à centre de gestion sur site.
3. Cliquez sur **Devices** (périphériques) > **Device Management** (gestion des périphériques).

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
eventsFtd-16-83 10.10.16.83 - Routed	FTDv for VMware	7.2.0	N/A	CDO Managed	CDO Managed	
OnPremFTD-141 10.10.14.141 - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	OnPremACPolicy	

Vous ne pouvez pas sélectionner cet appareil, car CDO gère la configuration. Le centre de gestion affiche l'étiquette **Géré par CDO** pour ce périphérique.

Pour voir les événements en direct dans centre de gestion, cliquez sur **Analysis > Events** (Analyses > Événements).

Générer un rapport de migration Défense contre les menaces

Lorsqu'une tâche de migration est réussie, vous pouvez générer et télécharger un rapport en format PDF pour analyser chaque paramètre importé de centre de gestion de pare-feu local vers Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Le rapport fournit des détails sur chaque périphérique associé à la tâche. Les détails comprennent des informations sur les périphériques, les valeurs des politiques partagées, les objets, les détails de routage, les interfaces, les paramètres réseau, etc.

Dans la page des tâches de migration, cliquez sur le  dans la colonne **actions** d'une tâche terminée, puis cliquez sur **Télécharger le rapport**. Vous devez télécharger un rapport dans l'année suivant le déclenchement de la tâche.

Supprimer une tâche de migration

Le résultat de la suppression d'une tâche de migration dépend du moment où elle est supprimée.

- Pendant la période d'évaluation de 14 jours : cette action arrête la migration. La configuration des périphériques associés à la tâche de migration retrouve son état d'origine.
- Après avoir validé les modifications de migration : l'enregistrement est supprimé de la liste des travaux de migration.

Procédure

-
- Étape 1** Choisissez **Tools & Services** (Outils et services) > **Migrate FTD to cdFMC** (Migrer FTD vers cdFMC).
- Étape 2** Cliquez sur le  dans la colonne **Actions**, puis cliquez sur **Supprimer la tâche de migration**.
- Étape 3** Cliquez sur **Delete** (Supprimer) pour confirmer votre action.
-

Activer les paramètres de notifications

Vous pouvez vous abonner pour recevoir des notifications par courriel de CDO chaque fois qu'un périphérique associé à votre client effectue une action spécifique lors de la migration d'un périphérique défense contre les menaces vers CDO.

CDO envoie un courriel si vous activez la fonctionnalité pour recevoir une notification pour les états suivants pendant la migration :

- **Échec** : lorsqu'une tâche de migration échoue.
- **Démarrée** : lorsqu'une tâche de migration est lancée.
- **Réussie** : lorsqu'une tâche de migration est terminée avec succès.
- **Validation en attente** : lorsque les modifications de gestionnaire doivent être validées.

Pour activer les paramètres de notification, consultez [Paramètres de notification](#).

Dépannage de la migration de Défense contre les menaces vers le nuage

Cette section fournit des informations pour résoudre des erreurs spécifiques qui peuvent se produire lors de la migration de défense contre les menaces vers le nuage.

Code d'état HTTP 201 (Créé) trouvé dans la réponse de FMC

CDO affiche cette erreur au niveau du périphérique.

Problème :

La version du connecteur de périphérique sécurisé (SDC) n'est pas compatible.

Number of FTDs	Status
1 devices	✖ i Change FTD Manager job failed
IP ADDRESS	STATUS
10.10.90.32	✖ Device Connectivity with CDO failed. (HTTP status code 201 (Created) found in FMC response.)

Résolution :

Assurez-vous que le SDC est mis à niveau à la version « 202205191350 » ou une version ultérieure.

1. Naviguez jusqu'à **Admin > Secure Connectors**.
2. Cliquez sur le SDC pour voir la version existante du SDC dans le volet **Details** à droite.
3. [Mettre à jour votre connecteur de périphérique sécurisé \(Secure Device Connector\)](#)

Échec de la connectivité du périphérique à CDO

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-02-28-104213	2 devices	Change FTD Manager job failed	Feb 28, 2022, 4:14:12 PM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.84	10.10.16.84	Device Connectivity with CDO failed	Feb 28, 2022, 4:12:53 PM	

Le périphérique ne peut pas atteindre CDO pour l'une des raisons suivantes :

- Le périphérique n'est pas correctement câblé.
- Votre réseau peut nécessiter une adresse IP statique pour le périphérique.
- Votre réseau utilise un DNS personnalisé, ou un blocage DNS externe est en place sur le réseau du client.
- Une authentification PPPoE est nécessaire.
- Le périphérique se trouve derrière un serveur mandataire.

Résolution :

- Vérifiez la connectivité du réseau et réessayez.
- Assurez-vous que votre pare-feu ne bloque aucun trafic.
- [Vérifiez la connectivité de Défense contre les menaces avec Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\).](#)

Échec de la configuration de CDO en tant que gestionnaire de configuration

Lorsque CDO ne peut pas communiquer avec le périphérique en raison d'une perte de réseau, il ne parvient pas à exécuter la commande configure Manager avec Firewall Management Center en nuage.

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-03-04-055700	2 devices	Change FTD Manager job is in progress	Mar 4, 2022, 11:33:07 AM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.86	10.10.16.86	Syncing	Mar 4, 2022, 11:29:03 AM	
1771Fmc_10.10.16.84	10.10.16.84	Failed to configure CDO as Configuration Manager	Mar 4, 2022, 11:28:16 AM	

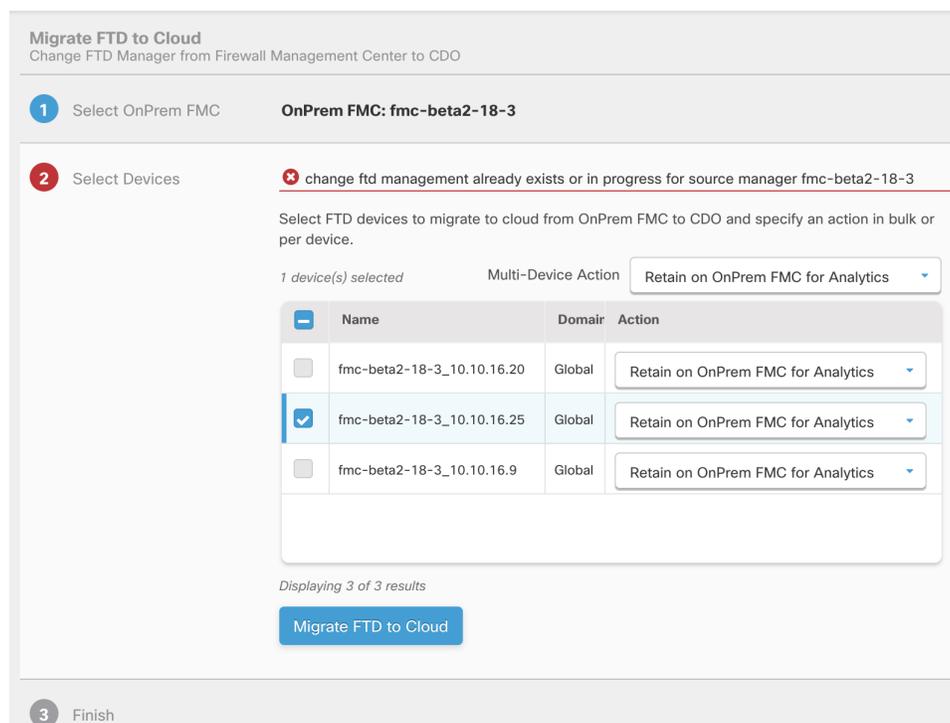
Résolution :

1. Vérifiez la connectivité du réseau et réessayez.
2. Assurez-vous que votre pare-feu ne bloque aucun trafic.
3. Assurez-vous que défense contre les menaces est doté d'une connectivité Internet et que l'adresse DNS est résolue en adresse IP. Consultez [Vérifiez la connectivité de Défense contre les menaces avec Cloud-Delivered Firewall Management Center \(centre de gestion de pare-feu en nuage\), à la page 22.](#)
4. Réessayez la migration pour ce défense contre les menaces à partir de CDO dans une nouvelle tâche de gestionnaire des changements.

Le gestionnaire des changements existe déjà ou est en cours pour le gestionnaire de source

Vous pouvez créer une tâche de migration défense contre les menaces pour une centre de gestion de pare-feu local uniquement lorsque la tâche précédente est terminée.

Cette erreur se produit lorsque vous créez une tâche alors que la tâche précédente est en cours.



Résolution :

1. Accédez au tableau de migration pour voir si une autre tâche est en cours pour une source particulière du centre de gestion sur site.
2. Attendez que la tâche de migration en cours soit terminée.
3. Lancez la prochaine tâche de migration.

Vérifiez la connectivité de Défense contre les menaces avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Cette section fournit les commandes pour déterminer la connectivité avec défense contre les menaces Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).

Vérification de la connectivité Internet sur le périphérique

Exécuter le **ping du système**<any OpenDNS server address> pour vérifier si le périphérique peut accéder à Internet.

1. Connectez-vous à l'interface de ligne de commande du périphérique, soit à partir du port de console ou à l'aide de SSH.

2. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur.
3. Saisissez **ping du système**<OpenDNS IPAddress>.

```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

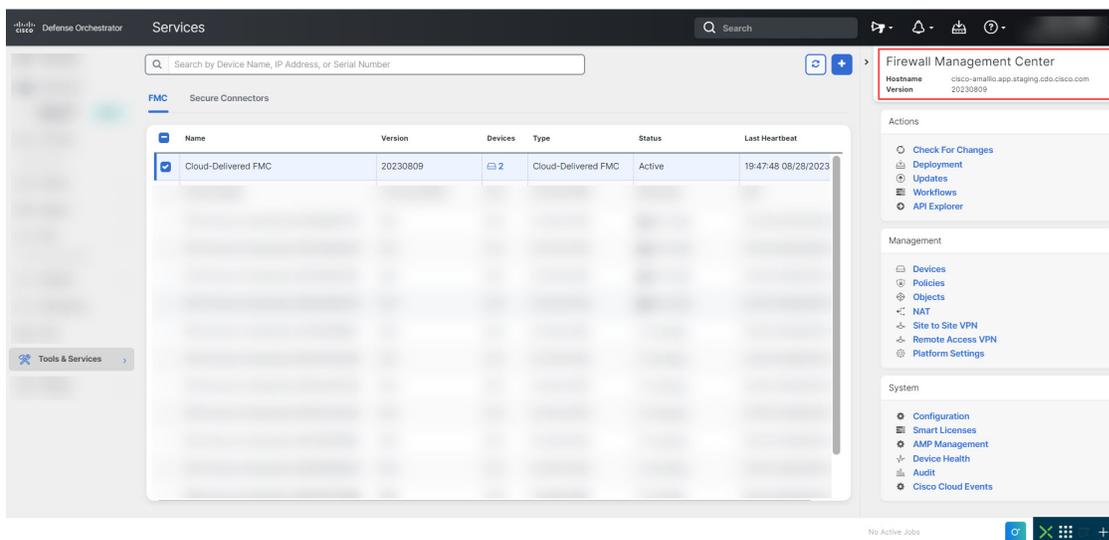
L'exemple ci-dessus montre que le périphérique peut se connecter à Internet en utilisant l'adresse IP du serveur OpenDNS. De plus, le nombre de paquets transmis est identique à celui reçu, ce qui indique que la connectivité Internet est disponible sur le périphérique. Cela montre que le périphérique peut accéder à Internet.



Remarque Si vos résultats ne correspondent pas, vérifiez la connexion Internet manuellement.

Vérifiez la connectivité du périphérique à l'aide de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

1. Obtenez le nom d'hôte de Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).
 1. Dans le volet de navigation CDO, cliquez sur **Tools and Services** (outils et services) > **Firewall Management Center** (centre de gestion Cisco Firewall Management Center).
 2. Choisissez **Cloud-Delivered FMC** (FMC en nuage) pour voir les détails Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans le volet droit.
 3. Dans le champ **Hostname** (nom d'hôte), copiez uniquement le nom d'hôte indiqué dans l'image d'exemple suivante.



Dans la figure ci-dessus, le texte en surbrillance est le nom d'h te (*cdo-acc10.app.us.cdo.cisco.com*) de FMC   copier.

2. Connectez-vous   l'interface de ligne de commande du p riph rique, soit   partir du port de console ou   l'aide de SSH.
3. Saisissez **le ping du syst me** *<hostname of the FMC>*.

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

Dans l'exemple ci-dessus, le nom d'h te est r solu avec l'adresse IP, ce qui indique que votre connexion a r ussi. Ignorez le message « 100 % de perte de paquets » affich  dans la r ponse.



Remarque

Si vous ne parvenez pas   vous connecter   l'h te, vous pouvez rectifier la configuration DNS dans la CLI   l'aide de la commande **configure network dns** *<address>*.

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.