



Domaine

Les rubriques suivantes décrivent les domaines et les politiques d'identité :

- [À propos des domaines et des séquences de domaine, à la page 1](#)
- [Exigences de licence pour les domaines, à la page 8](#)
- [Exigences et prérequis pour les domaines, à la page 8](#)
- [Créer une séquence de serveur mandataire, à la page 8](#)
- [Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 10](#)
- [Créer une séquence de domaine, à la page 24](#)
- [Configurer le Centre de gestion pour la confiance interdomaine : l'installation, à la page 25](#)
- [Gérer un domaine, à la page 33](#)
- [Comparer les domaines, à la page 34](#)
- [Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 35](#)
- [Historique des domaines, à la page 43](#)

À propos des domaines et des séquences de domaine

Les *domaines* sont des connexions entre les comptes Cisco Secure Firewall Management Center et les comptes d'utilisateurs sur les serveurs que vous surveillez. Ils précisent les paramètres de connexion et les paramètres de filtre d'authentification pour le serveur. Les domaines peuvent :

- Préciser les utilisateurs et les groupes d'utilisateurs dont vous souhaitez surveiller l'activité.
- Interroger le référentiel d'utilisateurs pour connaître les métadonnées utilisateur sur les utilisateurs faisant autorité, ainsi que certains utilisateurs ne faisant pas autorité : les utilisateurs POP3 et IMAP détectés par la détection basée sur le trafic et les utilisateurs détectés par la détection basée sur le trafic, un agent TS technique ou ISE/ISE-PIC.

Vous pouvez ajouter plusieurs contrôleurs de domaine en tant que répertoires dans un domaine, mais ils doivent partager les mêmes informations de domaine de base. Les répertoires d'un domaine doivent être exclusivement des serveurs LDAP ou Active Directory (AD). Après avoir activé un domaine, vos modifications enregistrées prendront effet la prochaine fois que centre de gestion interrogera le serveur.

Pour effectuer la sensibilisation des utilisateurs, vous devez configurer un domaine pour tout [Serveurs pris en charge pour les domaines](#). Le système utilise ces connexions pour interroger les serveurs sur les données associées aux utilisateurs POP3 et IMAP et pour recueillir des données sur les utilisateurs LDAP découverts grâce à la détection basée sur le trafic.

Le système utilise les adresses de courriel dans les connexions POP3 et IMAP pour établir la corrélation avec les utilisateurs LDAP sur un répertoire Active Directory ou OpenLDAP. Par exemple, si un périphérique géré détecte une connexion POP3 pour un utilisateur ayant la même adresse courriel qu'un utilisateur LDAP, le système associe les métadonnées de l'utilisateur LDAP à cet utilisateur.

Pour effectuer le contrôle de l'utilisateur, vous pouvez configurer l'un des éléments suivants :

- Un domaine ou une séquence de domaine pour un serveur Active Directory ou ISE/ISE-PIC



Remarque La configuration d'un domaine Microsoft AD ou d'une séquence de domaine est facultative si vous prévoyez configurer des conditions d'attribut SGT ISE, mais pas les conditions d'utilisateur, de groupe, de domaine, d'emplacement de point terminal ou de profil de point terminal; ou si vous utilisez votre politique d'identité uniquement pour filtrer le trafic réseau.

- Un domaine ou une séquence de domaine pour un serveur Microsoft AD pour l'agent des services TS.
- Pour les portails captifs, un domaine LDAP.

Les séquences de domaine ne sont pas prises en charge pour LDAP.

Vous pouvez imbriquer groupes AD Microsoft et Cisco Secure Firewall Management Center télécharge ces groupes et les utilisateurs qu'ils contiennent. Vous pouvez éventuellement restreindre les groupes et les utilisateurs téléchargés, comme indiqué dans [Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine](#), à la page 10.

À propos de la synchronisation des utilisateurs

Vous pouvez configurer un domaine ou une séquence de domaine pour établir une connexion entre centre de gestion et un serveur LDAP ou Microsoft AD afin de récupérer les métadonnées d'utilisateur et de groupes d'utilisateurs pour certains utilisateurs détectés :

- Utilisateurs LDAP et Microsoft AD authentifiés par le portail captif ou signalés par ISE/ISE-PIC. Ces métadonnées peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.
- Connexions d'utilisateurs POP3 et IMAP détectées par la détection basée sur le trafic, si ces utilisateurs ont la même adresse courriel qu'un utilisateur LDAP ou AD. Ces métadonnées peuvent être utilisées pour sensibiliser l'utilisateur.

centre de gestion obtient les informations et métadonnées suivantes sur chaque utilisateur :

- Nom d'utilisateur LDAP
- Prénoms et noms de famille
- Adresse de courriel
- Service
- Numéro de téléphone



Important Pour réduire la latence entre Cisco Secure Firewall Management Center et votre contrôleur de domaine Active Directory, nous vous recommandons fortement de configurer un répertoire de domaine (c'est-à-dire le contrôleur de domaine) qui est aussi proche que possible géographiquement de Cisco Secure Firewall Management Center.

Par exemple, si votre Cisco Secure Firewall Management Center est en Amérique du Nord, configurez un répertoire de domaine qui se trouve également en Amérique du Nord. Ne pas le faire peut entraîner des problèmes tels que l'expiration du délai de téléchargement des utilisateurs et des groupes.

À propos des données d'activité des utilisateurs

Les données d'activités des utilisateurs sont stockées dans la base de données d'activités des utilisateurs et les données d'identité des utilisateurs sont stockées dans la base de données des utilisateurs. Si vos paramètres de contrôle d'accès sont trop généraux, le centre de gestion obtient des informations sur autant d'utilisateurs que possible et signale le nombre d'utilisateurs qu'il n'a pas réussi à récupérer dans l'onglet Tâches du Centre de messages.

Pour limiter les sous-réseaux sur lesquels un périphérique géré surveille les données de sensibilisation des utilisateurs, vous pouvez utiliser la commande **configure identity-subnet-filter**, comme indiqué dans [Référence des commandes de défense contre les menaces de Cisco Secure Firewall](#).



Remarque Si vous supprimez un utilisateur qui a été détecté par le système de votre référentiel d'utilisateurs, le centre de gestion ne supprime *pas* cet utilisateur de sa base de données des utilisateurs; vous devez le supprimer manuellement. Cependant, vos modifications LDAP *sont* reflétées dans les règles de contrôle d'accès lors de la prochaine mise à jour de la liste d'utilisateurs de centre de gestion.

Domaines et domaines de confiance

Lorsque vous configurez un *domaine* Microsoft Active Directory (AD) dans le centre de gestion, il est associé à un *domaine* Microsoft Active Directory ou LDAP.

Un groupe de domaines Microsoft Active Directory (AD) qui se font confiance est communément appelé une « forêt ». Cette relation d'approbation peut permettre aux domaines d'accéder aux ressources des uns et des autres de différentes manières. Par exemple, un compte d'utilisateur défini dans le domaine A peut être marqué comme membre d'un groupe défini dans le domaine B.

Le système et les domaines de confiance

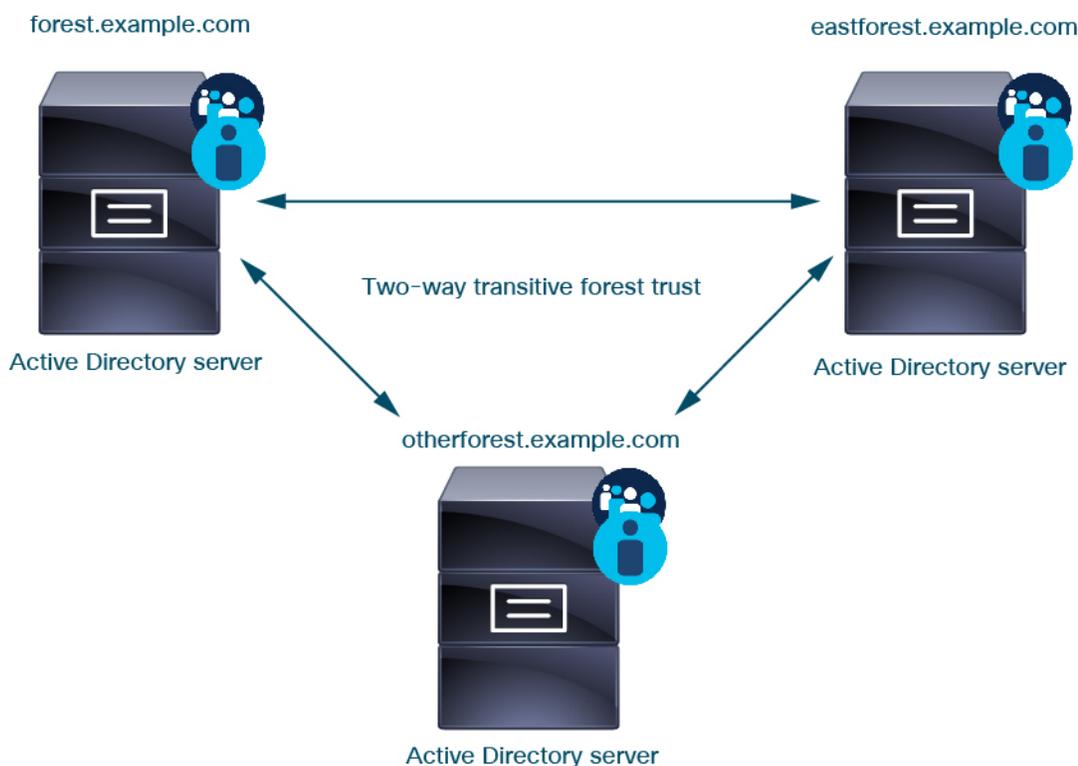
Le système prend en charge les forêts AD configurées dans une relation d'approbation. Il existe plusieurs types de relations de confiance. Ce guide traite des relations d'approbation de forêt transitives bidirectionnelles. L'exemple simple suivant montre deux forêts : **forest.example.com** et **eastforest.example.com**. Les utilisateurs et les groupes de chaque forêt peuvent être authentifiés par AD dans l'autre forêt, à condition que vous configurez les forêts de cette façon.

Si vous configurez le système avec un domaine pour chaque domaine et un répertoire pour chaque contrôleur de domaine, le système peut détecter jusqu'à 100 000 [principaux de sécurité étrangers](#) (utilisateurs et groupes). Si ces principaux de sécurité étrangers correspondent à un utilisateur téléchargé dans un autre domaine, ils peuvent être utilisés dans la politique de contrôle d'accès.

Vous n'avez pas besoin de configurer de domaine pour un domaine qui n'a aucun utilisateur que vous souhaitez utiliser dans les politiques de contrôle d'accès.



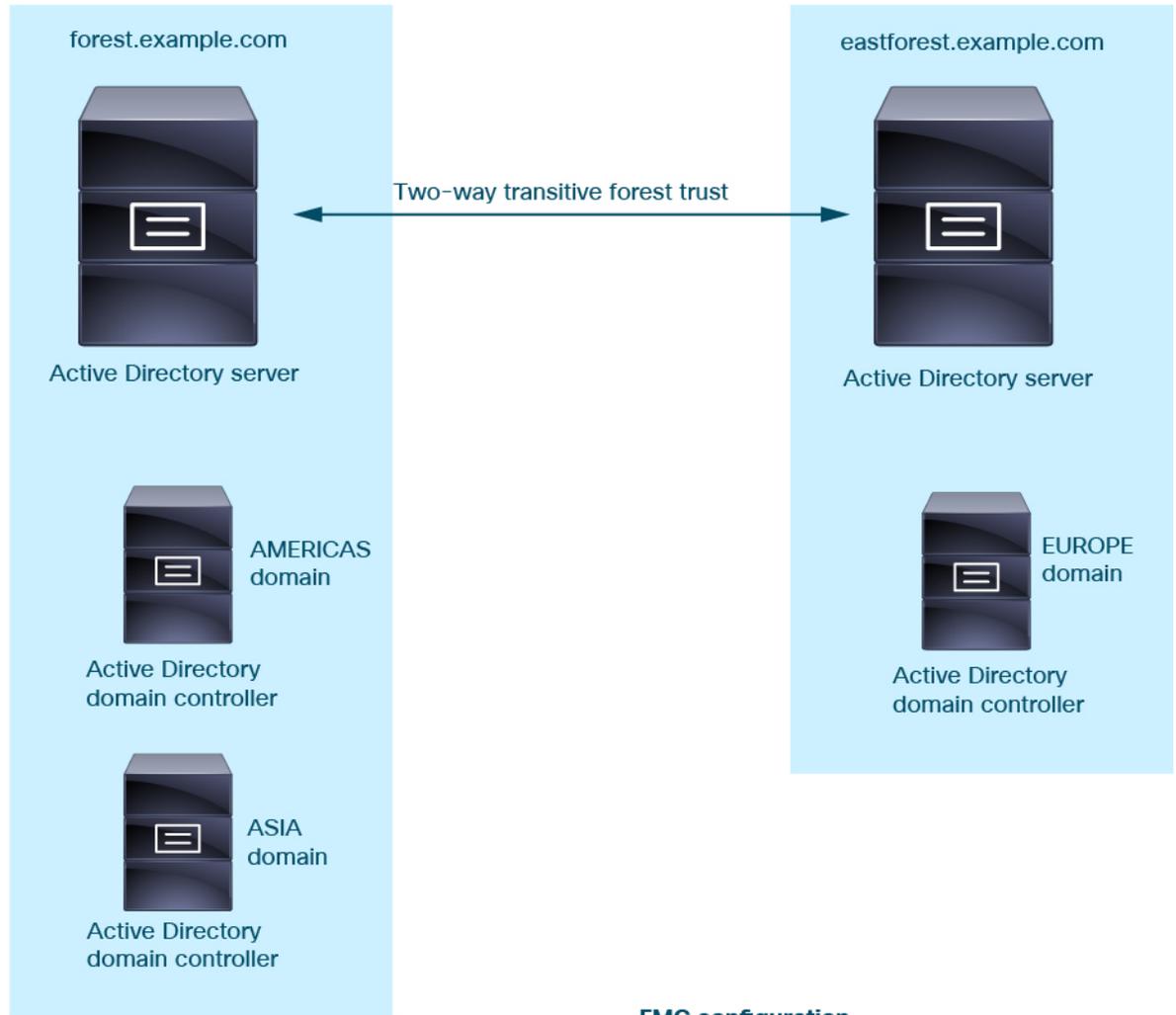
Pour continuer avec l'exemple, supposons que vous ayez trois forêts AD (dont l'une pourrait être un sous-domaine ou une forêt indépendante), toutes configurées comme des relations de forêt transitive bidirectionnelles, tous les utilisateurs et groupes sont disponibles dans les trois forêts ainsi que dans le système. (Comme dans l'exemple précédent, les trois domaines AD doivent être configurés en tant que domaines et tous les contrôleurs de domaine doivent être configurés comme des répertoires dans ces domaines.)



Enfin, vous pouvez configurer centre de gestion pour pouvoir appliquer les politiques d'identité aux utilisateurs et aux groupes dans un système à deux forêts avec une approbation de forêt transitive bidirectionnelle. Supposons que chaque forêt ait au moins un contrôleur de domaine, dont chacun authentifie différents utilisateurs et groupes. Pour que centre de gestion puisse appliquer les politiques d'identité à ces utilisateurs et groupes, vous devez configurer chaque domaine contenant les utilisateurs concernés en tant que domaine

centre de gestion et chaque contrôleur de domaine en tant que répertoire centre de gestion dans le domaine respectif.

Ne pas configurer correctement centre de gestion empêche certains utilisateurs et groupes d'être utilisés dans les politiques. Vous verrez des avertissements lorsque vous tenterez de synchroniser les utilisateurs et les groupes.



FMC configuration



Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

En utilisant l'exemple précédent, configurez centre de gestion comme suit :

- Domaine pour tout domaine de **forest.example.com** qui contient des utilisateurs que vous souhaitez contrôler avec des politiques de contrôle d'accès

- Répertoire dans le domaine pour **AMERICAS.forest.example.com**
- Répertoire dans le domaine pour **ASIA.forest.example.com**
- Domaine pour tout domaine de **eastforest.example.com** qui contient des utilisateurs que vous souhaitez contrôler avec des politiques de contrôle d'accès
 - Répertoire dans le domaine pour **EUROPE.eastforest.example.com**



Remarque

centre de gestion utilise le champ AD **msDS-PrincipalName** pour résoudre les références afin de trouver les noms d'utilisateur et de groupe dans chaque contrôleur de domaine. **msDS-PrincipalName** renvoie un nom NetBIOS.

Serveurs pris en charge pour les domaines

Vous pouvez configurer des domaines pour qu'ils se connectent aux types de serveurs suivants, à condition qu'ils disposent d'un accès TCP/IP à partir de centre de gestion :

Type de serveur	Prise en charge pour la récupération de données ISE/ISE-PIC?	Prise en charge pour la récupération des données de l'agent des services?	Prise en charge pour la récupération des données du portail captif?
Microsoft Active Directory sur Windows Server 2012, 2016 et 2019	Oui	Oui	Oui
OpenLDAP sur Linux	Non	Non	Oui

Les serveurs de catalogue global Active Directory ne sont *pas pris en charge* en tant que répertoire de domaine. Pour en savoir plus sur le serveur de catalogue global, consultez [le catalogue global](#) sur le site learning.microsoft.com.



Remarque

Si l'agent TS est installé sur un serveur Windows Microsoft Active Directory partagé avec une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion donne la priorité aux données de l'agent TS. Si l'agent TS et une source d'identité passive signalent une activité par la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.

Tenez compte des éléments suivants concernant les configurations de vos groupes de serveurs :

- Pour effectuer le contrôle d'utilisateur sur des groupes d'utilisateurs ou des utilisateurs dans des groupes, vous devez configurer les groupes d'utilisateurs sur le serveur LDAP ou Active Directory.
- Les noms de groupe ne peuvent pas commencer par **S-**, car il est utilisé en interne par LDAP.

Ni les noms de groupes ni les noms d'unités organisationnelles ne peuvent contenir de caractères spéciaux comme l'astérisque (*), le signe égal (=) ou la barre oblique inverse (\). Sinon, les utilisateurs de ces

groupes ou unités organisationnelles ne sont pas téléchargés et ne sont pas disponibles pour les politiques d'identité.

- Pour configurer un domaine Active Directory qui inclut ou exclut les utilisateurs membres d'un sous-groupe sur votre serveur, notez que Microsoft recommande qu'Active Directory n'ait pas plus de 5 000 utilisateurs par groupe dans Windows Server 2012. Pour en savoir plus, consultez [Limites maximales d'Active Directory - Évolutivité sur MSDN](#).

Au besoin, vous pouvez modifier la configuration de votre serveur Active Directory pour augmenter cette limite par défaut et ainsi permettre un plus grand nombre d'utilisateurs.

- Pour identifier de façon unique les utilisateurs signalés par un serveur dans votre environnement de services bureau à distance, vous devez configurer l'agent des services de terminaux Cisco (TS). Une fois installé et configuré, l'agent des services de terminaux (TS) affecte des ports uniques aux utilisateurs afin que le système puisse identifier ces utilisateurs de façon unique. (Microsoft a changé le nom des *Services de terminaux* en *Services de bureau à distance*.)

Pour en savoir plus sur l'agent TS, consultez le *Guide de l'agent Cisco Terminal Services (TS)*.

Noms d'attribut et de classe d'objet serveur pris en charge

Les serveurs de vos domaines *doivent* utiliser les noms d'attributs répertoriés dans le tableau suivant pour que centre de gestion récupère les métadonnées des utilisateurs sur les serveurs. Si les noms d'attribut sont incorrects sur votre serveur, centre de gestion ne peut pas remplir sa base de données avec les informations de cet attribut.

Tableau 1 : Mise en correspondance des noms d'attributs avec les champs Cisco Secure Firewall Management Center

Métadonnées	Attribut Centre de gestion	Classe d'objet LDAP	Attribut Active Directory	Attribut OpenLDAP
Nom d'utilisateur LDAP	Nom d'utilisateur	<ul style="list-style-type: none"> • utilisateur • in Open 	samaccountname	cn uid
prénom	Prénom		prénom	prénom
nom	Nom		sn	sn
adresse courriel	Courriel		mail userprincipalname (si courriel n'a aucune valeur)	mail
department	Service		department distinguishedname (si le service n'a aucune valeur)	ou
nom distinctif	Téléphone		telephonenumber	telephonenumber



Remarque La classe d'objets LDAP pour les groupes est `group`, `groupOfNames`, (`group-of-names` pour Active Directory) ou `groupOfUniqueNames`.

Pour plus d'informations sur les classes d'objets et les attributs, consultez les références suivantes :

- Microsoft Active Directory :
 - ObjectClasses : toutes les classes sur [MSDN](#)
 - Attributs : tous les attributs sur [MSDN](#)
- OpenLDAP : [RFC 4512](#)

Exigences de licence pour les domaines

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et prérequis pour les domaines

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Créer une séquence de serveur mandataire

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

ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

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

Historique de la fonctionnalité Défense contre les menaces

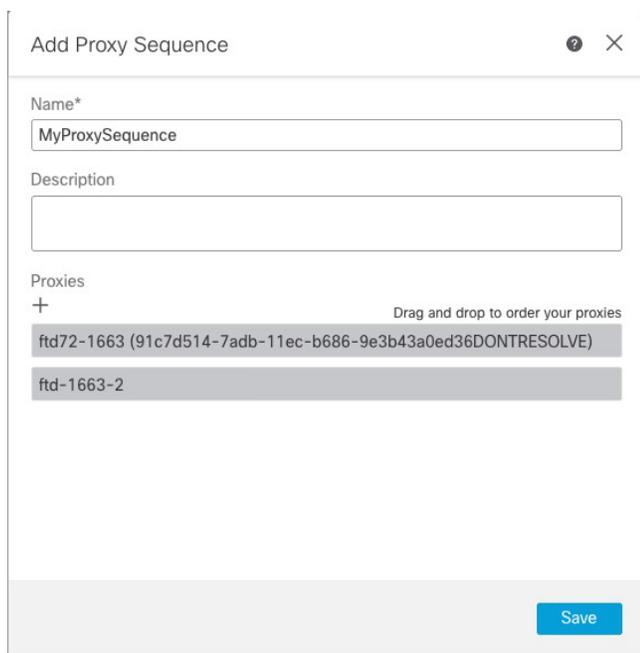
7.2 : cette fonctionnalité a été ajoutée.

Avant de commencer

Vous devez ajouter au moins deux périphériques gérés à CDO, qui doivent tous pouvoir communiquer avec Active Directory ou ISE/ISE-PIC.

Procédure

- Étape 1** Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.
- Étape 2** Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines) > Proxy Sequence (séquences de proxy)**.
- Étape 3** Cliquez sur **Add Sequence** (Ajouter une séquence).
- Étape 4** Dans le champ **Name**, saisissez un nom pour identifier la séquence de serveur mandataire
- Étape 5** (Facultatif) Dans le champ **Description**, saisissez une description pour la séquence de serveur mandataire.
- Étape 6** Sous Mandataires, cliquez sur **Ajouter (+)**.
- Étape 7** Cliquez sur le nom de chaque périphérique géré à ajouter à la séquence.
Pour affiner votre recherche, saisissez tout ou une partie du nom de domaine dans le champ **Filter** (filtre).
- Étape 8** Cliquez sur **OK**.
- Étape 9** Dans la boîte de dialogue Add Proxy Sequence (ajouter une séquence de serveur mandataire), faites glisser et déposez les serveurs mandataires dans l'ordre dans lequel vous souhaitez que CDO les recherchent. La figure suivante montre un exemple de séquence de serveurs mandataires composée de deux serveurs mandataires. Les utilisateurs du serveur mandataire supérieur seront recherchés avant ceux du serveur mandataire inférieur. Les deux serveurs mandataires doivent pouvoir communiquer avec Active Directory ou ISE/ISE-PIC.



Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

Consultez [Créer une politique d'identité](#).

Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine

Si vous configurez ISE/ISE-PIC sans domaine, sachez qu'il y a un délai d'expiration de session utilisateur qui affecte la façon dont les utilisateurs sont vus par Cisco Secure Firewall Management Center. Pour obtenir plus de renseignements, consultez [Champs de domaine, à la page 13](#).

La procédure suivante vous permet de créer un *domaine* (une connexion entre centre de gestion et un domaine Active Directory) et un *répertoire* (une connexion entre centre de gestion et un serveur LDAP ou un contrôleur de domaine Active Directory).

(Recommandé.) Pour vous connecter de manière sécurisée de centre de gestion à votre serveur Active Directory, effectuez d'abord les tâches suivantes :

- [Exporter le certificat racine du serveur Active Directory, à la page 21](#)
- [Trouver le nom du serveur Active Directory, à la page 21](#)

Microsoft a annoncé que les serveurs Active Directory commenceront à appliquer la liaison et la signature LDAP en 2020. Microsoft en fait des exigences obligatoires, car lors de l'utilisation des paramètres par défaut, il existe une vulnérabilité d'élection de privilèges dans Microsoft Windows qui pourrait permettre à un attaquant de l'intermédiaire de réussir une demande d'authentification à un serveur LDAP Windows. Pour en savoir

plus, consultez [Déclaration 2020 relative à la liaison de canal LDAP et à la signature LDAP pour Windows](#) sur le site d'assistance de Microsoft.

Pour en savoir plus sur les champs de configuration de domaine et de répertoire, consultez [Champs de domaine, à la page 13](#) et [Champs Répertoire de domaine et Synchroniser, à la page 18](#).

Un exemple étape par étape de la configuration d'un domaine avec approbation interdomaine est présenté dans [Configurer le Centre de gestion pour la confiance interdomaine : l'installation, à la page 25](#).

Les serveurs de catalogue global Active Directory ne sont *pas pris en charge* en tant que répertoire de domaine. Pour en savoir plus sur le serveur de catalogue global, consultez [le catalogue global](#) sur le site learning.microsoft.com.

**Remarque**

Vous devez spécifier un **domaine principal AD** unique pour chaque domaine Microsoft Active Directory (AD). Bien que le système vous permette de spécifier le même **domaine AD principal** pour différents domaines Microsoft AD, le système ne fonctionnera pas correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier. Le système empêche de spécifier plus d'un domaine avec le même **domaine AD principal**, car les utilisateurs et les groupes ne seront pas identifiés correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier.

Si vous configurez ISE/ISE-PIC sans domaine, sachez qu'il y a un délai d'expiration de session utilisateur qui affecte la façon dont les utilisateurs sont vus par Cisco Secure Firewall Management Center. Pour obtenir plus de renseignements, consultez [Champs de domaine, à la page 13](#).

Avant de commencer

Si vous utilisez l'authentification Kerberos pour le portail captif, consultez la section suivante avant de commencer : [Conditions préalables à l'authentification Kerberos, à la page 13](#).

Si vous gérez des périphériques avec Cisco Defense Orchestrator (CDO), créez d'abord une séquence de mandataire comme décrit dans [Créer une séquence de serveur mandataire, à la page 8](#)

**Important**

Pour réduire la latence entre Cisco Secure Firewall Management Center et votre contrôleur de domaine Active Directory, nous vous recommandons fortement de configurer un répertoire de domaine (c'est-à-dire le contrôleur de domaine) qui est aussi proche que possible géographiquement de Cisco Secure Firewall Management Center.

Par exemple, si votre Cisco Secure Firewall Management Center est en Amérique du Nord, configurez un répertoire de domaine qui se trouve également en Amérique du Nord. Ne pas le faire peut entraîner des problèmes tels que l'expiration du délai de téléchargement des utilisateurs et des groupes.

Procédure**Étape 1**

Connectez-vous au Cisco Secure Firewall Management Center.

Étape 2

Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.

Étape 3

Pour créer un domaine, choisissez dans la liste déroulante **Add Realm** (ajouter un domaine).

- Étape 4** Pour effectuer d'autres tâches (comme activer, désactiver ou supprimer un domaine), consultez [Gérer un domaine, à la page 33](#).
- Étape 5** Saisissez les informations de domaine comme indiqué dans [Champs de domaine, à la page 13](#).
- Étape 6** (Facultatif) Dans la liste **Proxy** (Mandataire), cliquez sur un périphérique géré ou une séquence de mandataire pour communiquer avec ISE/ISE-PIC si CDO n'est pas en mesure de le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.
- Étape 7** Dans la section de configuration du serveur de répertoire, saisissez les informations sur le répertoire comme indiqué dans [Champs Répertoire de domaine et Synchroniser, à la page 18](#).
- Étape 8** (Facultatif) Pour configurer un autre domaine pour ce domaine, cliquez sur **Add another directory** (ajouter un autre répertoire).
- Étape 9** Cliquez sur **Configure Groups and Users** (Configurer les groupes et les utilisateurs). Saisissez l'information suivante :

Information	Description
Domaine AD principal	Domaine du serveur Active Directory où les utilisateurs doivent être authentifiés. Pour de l'information supplémentaire, reportez-vous à la section Champs de domaine, à la page 13 .
Nom unique de base	L'arborescence de répertoires sur le serveur où le Cisco Secure Firewall Management Center doit commencer à rechercher les données de l'utilisateur.
Nom unique du groupe	L'arborescence de répertoires sur le serveur où le Cisco Secure Firewall Management Center doit commencer à rechercher les données de groupe.
Serveur mandataire	Dans la liste, cliquez sur un ou plusieurs périphériques gérés ou sur une séquence de mandataire. Ces périphériques doivent pouvoir communiquer avec Active Directory ou ISE/ISE-PIC pour récupérer les données des utilisateurs pour les politiques d'identité.
Charger les groupes	Cliquez pour télécharger des groupes à partir du serveur Active Directory. Si aucun groupe ne s'affiche, saisissez ou modifiez les renseignements dans les champs AD Primary Domain , (Domaine principal AD) Base DN (Numéro de répertoire de base) et Group DN (Numéro de répertoire de groupe) , puis cliquez sur Load Groups (Téléverser les groupes). Pour plus d'informations sur ces champs, consultez Champs de domaine, à la page 13 .
Section Groupes disponibles	Limitez les groupes à utiliser dans la politique en les déplaçant dans la liste Groupes et utilisateurs inclus ou Groupes et utilisateurs exclus . Par exemple, le fait de déplacer un groupe dans la liste Groupes et utilisateurs inclus permet d'utiliser uniquement ce groupe dans la politique, mais exclut tous les autres groupes. Les groupes dans la liste Groupes et utilisateurs exclus et les utilisateurs qu'ils contiennent sont exclus de la sensibilisation et du contrôle des utilisateurs. Tous les autres groupes et utilisateurs <i>sont</i> disponibles. Pour en savoir plus, consultez Champs Répertoire de domaine et Synchroniser, à la page 18 .

- Étape 10** Cliquez sur l'onglet **Configuration du domaine**.
- Étape 11** Saisissez l'attribut de groupe **Group Attribute** et (si vous utilisez l'authentification Kerberos pour le portail captif), le **nom d'utilisateur AD Join** et le **mot de passe AD Join**. Pour en savoir plus, consultez [Champs Répertoire de domaine et Synchroniser](#), à la page 18.
- Étape 12** Si vous utilisez l'authentification Kerberos, cliquez sur **Tester**. Si le test échoue, attendez un court instant et réessayez.
- Étape 13** Saisir des valeurs de délai d'expiration de session utilisateur, en minutes, pour **les utilisateurs ISE/ISE-PIC**, les **utilisateurs d'agents de serveur Terminal Server**, les **utilisateurs du portail captif**, les **utilisateurs ayant échoué à accéder au portail captif**, et les **utilisateurs du portail captif invités**.
- Étape 14** Lorsque vous avez terminé de configurer le domaine, cliquez sur **Save** (Enregistrer).

Prochaine étape

- [Configurer le Centre de gestion pour la confiance interdomaine : l'installation](#), à la page 25
- [Synchroniser les utilisateurs et les groupes](#), à la page 23
- Modifier, supprimer, activer ou désactiver un domaine; voir [Gérer un domaine](#), à la page 33.
- [Comparer les domaines](#), à la page 34.
- Si vous le souhaitez, vous pouvez suivre l'état de la tâche; voir *Affichage des messages de la tâche* dans la section [Guide d'administration Cisco Secure Firewall Management Center](#).

Conditions préalables à l'authentification Kerberos

Si vous utilisez Kerberos pour authentifier les utilisateurs du portail captif, tenez compte des éléments suivants.

Limite de nombre de caractères pour le nom d'hôte

Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : [Conventions de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles](#).

Limite de nombre de caractères de la réponse DNS

Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans [la section 6.2.5 de la RFC 6891](#).

Champs de domaine

Les champs suivants sont utilisés pour configurer un domaine.

Champs de configuration de domaine

Ces paramètres s'appliquent à tous les serveurs ou contrôleurs de domaine Active Directory (également appelés *répertoires*) d'un domaine.

Nom

Un nom unique pour le domaine.

- Pour utiliser le domaine dans les politiques d'identité, le système prend en charge les caractères alphanumériques et spéciaux.
- Pour utiliser le domaine dans les configurations de VPN d'accès à distance, le système prend en charge les caractères alphanumériques, les tirets (-), les traits de soulignement (_) et les plus (+).

Description

(Facultatif) Saisissez une description du domaine.

Type

Le type de domaine, **AD** pour Microsoft Active Directory, **LDAP** pour les autres référentiels LDAP pris en charge ou **Local**. Pour obtenir la liste des référentiels LDAP pris en charge, consultez [Serveurs pris en charge pour les domaines, à la page 6](#). Vous pouvez authentifier les utilisateurs du portail captif à l'aide d'un référentiel LDAP; tous les autres nécessitent Active Directory.

**Remarque**

Seul le portail captif prend en charge un domaine LDAP.

Le type de domaine **LOCAL** est utilisé pour configurer les paramètres de l'utilisateur local. Le domaine LOCAL est utilisé pour l'authentification des utilisateurs d'accès distant.

Ajoutez les informations sur l'utilisateur local suivantes pour le domaine LOCAL :

- **Username** : Nom de l'utilisateur local.
- **Password** : Mot de passe de l'utilisateur local.
- **Confirm Password** : confirmer le mot de passe de l'utilisateur local.

**Remarque**

Cliquez sur Ajouter un autre utilisateur local pour ajouter d'autres utilisateurs au domaine LOCAL.

Vous pouvez ajouter d'autres utilisateurs après avoir créé le domaine et mettre à jour le mot de passe pour les utilisateurs locaux. Vous pouvez également créer plusieurs domaines de type LOCAL, mais pas les désactiver.

Domaine AD principal

Pour les domaines Microsoft Active Directory uniquement. Domaine du serveur Active Directory où les utilisateurs doivent être authentifiés.

**Remarque**

Vous devez spécifier un **domaine principal AD** unique pour chaque domaine Microsoft Active Directory (AD). Bien que le système vous permette de spécifier le même **domaine AD principal** pour différents domaines Microsoft AD, le système ne fonctionnera pas correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier. Le système empêche de spécifier plus d'un domaine avec le même **domaine AD principal**, car les utilisateurs et les groupes ne seront pas identifiés correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier.

Nom d'utilisateur et mot de passe AD Join

(Disponible dans l'onglet **Realm Configuration** (Configuration du domaine) lorsque vous modifiez un domaine.)

Pour les domaines Microsoft Active Directory destinés à l'authentification active du portail captif Kerberos, le nom d'utilisateur et le mot de passe distincts de tout utilisateur Active Directory disposant des droits appropriés pour créer un compte d'ordinateur de domaine dans le domaine Active Directory.

Gardez les éléments suivants à l'esprit :

- Le DNS doit être en mesure de résoudre le nom de domaine en adresse IP d'un contrôleur de domaine Active Directory.
- L'utilisateur que vous spécifiez doit être en mesure de joindre des ordinateurs au domaine Active Directory.
- Le nom d'utilisateur doit être complet; par exemple, **administrateur@mondomaine.com**, *non administrateur*).

Si vous choisissez **Kerberos** (ou **HTTP Negotiate**, si vous souhaitez que Kerberos soit offert en option) comme **protocole d'authentification** dans une règle d'identité, le **domaine** que vous sélectionnez doit être configuré avec un nom d'**utilisateur AD Join** et un **mot de passe AD Join** pour effectuer l'authentification active du portail captif Kerberos.

**Remarque**

L'algorithme de hachage SHA-1 n'est pas sécurisé pour le stockage des mots de passe sur votre serveur Active Directory et ne doit pas être utilisé. Pour en savoir plus, consultez des documents de référence comme [Migration de votre algorithme de hachage d'autorité de certification de SHA1 à SHA2 sur Microsoft TechNet](#) ou [l'aide-mémoire sur le stockage des mots de passe](#) sur le site Web d'Open Web Application Security Project.

Nous recommandons SHA-256 pour communiquer avec Active Directory.

Nom d'utilisateur et mot de passe du répertoire

Le nom d'utilisateur et le mot de passe d'un utilisateur uniques disposant d'un accès approprié aux informations sur l'utilisateur que vous souhaitez récupérer.

Tenez compte des points suivants :

- Pour certaines versions de Microsoft Active Directory, des autorisations spécifiques peuvent être nécessaires pour lire des utilisateurs et des groupes. Consultez la documentation fournie avec Microsoft Active Directory pour en savoir plus.
- Pour OpenLDAP, les privilèges d'accès de l'utilisateur sont déterminés par le paramètre `<level>` décrit dans la section 8 de la [spécification OpenLDAP](#). Le paramètre `<level>` de l'utilisateur doit être `auth` ou supérieur.
- Le nom d'utilisateur doit être complet; par exemple, `administrateur@mondomaine.com`, *non* `administrateur`).



Remarque

L'algorithme de hachage SHA-1 n'est pas sécurisé pour le stockage des mots de passe sur votre serveur Active Directory et ne doit pas être utilisé. Pour en savoir plus, consultez des documents de référence comme [Migration de votre algorithme de hachage d'autorité de certification de SHA1 à SHA2 sur Microsoft TechNet](#) ou [l'aide-mémoire sur le stockage des mots de passe](#) sur le site Web d'Open Web Application Security Project.

Nous recommandons SHA-256 pour communiquer avec Active Directory.

Nom unique de base

(Facultatif) L'arborescence de répertoires sur le serveur où le Cisco Secure Firewall Management Center doit commencer à rechercher les données de l'utilisateur. Si vous ne spécifiez pas de **DN de base**, le système récupère le DN de niveau supérieur, à condition que vous puissiez vous connecter au serveur.

En règle générale, le nom distinctif (DN) de base a une structure de base indiquant le nom de domaine et l'unité opérationnelle de l'entreprise. Par exemple, l'organisation de la sécurité de l'entreprise Exemple pourrait avoir un DN de base de `ou=security,dc=example,dc=com`.

Nom unique du groupe

(Facultatif) L'arborescence du répertoire sur le serveur où le Cisco Secure Firewall Management Center doit rechercher les utilisateurs ayant l'attribut de groupe. Une liste des attributs de groupe pris en charge figure dans la section [Noms d'attribut et de classe d'objet serveur pris en charge](#), à la page 7. Si vous ne spécifiez pas de **DN de groupe**, le système récupère le DN de niveau supérieur, à condition que vous puissiez vous connecter au serveur.



Remarque

Voici la liste des caractères que le système *prend en charge* en ce qui concerne les utilisateurs, les groupes et les noms de domaine de votre serveur d'annuaire. L'utilisation de caractères autres que les suivants peut empêcher le système de télécharger les utilisateurs et les groupes.

Entité	Caractères pris en charge
Nom d'utilisateur	<code>a-z A-Z 0-9 ! # \$ % ^ & () _ - { } ' . ~ `</code>
Nom du groupe	<code>a-z A-Z 0-9 ! # \$ % ^ & () _ - { } ' . ~ `</code>
DN de base et DN de groupe	<code>a-z A-Z 0-9 ! @ \$ % ^ & * () _ - . ~ `</code>

Les espaces ne sont pas pris en charge dans un nom d'utilisateur, y compris à la fin.

Serveur mandataire

Dans la liste, cliquez sur un ou plusieurs périphériques gérés ou sur une séquence de mandataire. Ces périphériques doivent pouvoir communiquer avec Active Directory ou ISE/ISE-PIC pour récupérer les données des utilisateurs pour les politiques d'identité.

Les champs suivants sont disponibles lorsque vous modifiez un domaine existant.

Session utilisateur expirée

(Disponible dans l'onglet **Realm Configuration** (Configuration du domaine) lorsque vous modifiez un domaine.)

Saisissez le nombre de minutes avant l'expiration des sessions utilisateur. La valeur par défaut est 24 heures (1440 minutes) après l'événement de connexion de l'utilisateur. Une fois le délai dépassé, la session de l'utilisateur se termine; si l'utilisateur continue d'accéder au réseau sans se reconnecter, l'utilisateur est vu par centre de gestion comme Inconnu (sauf pour les **utilisateurs du portail captif ayant échoué**).

En outre, si vous configurez ISE/ISE-PIC sans domaine et que le délai d'expiration est dépassé, une solution de contournement est requise. Pour en savoir plus, communiquez avec le [TAC de Cisco](#).

Vous pouvez définir des valeurs de délai d'expiration pour les éléments suivants :

- **Utilisateurs de l'agent utilisateur et d'ISE/ISE-PIC** : Délai d'expiration pour les utilisateurs suivis par l'agent utilisateur ou par ISE/ISE-PIC, qui sont des types d'authentification passive.

La valeur du délai d'expiration que vous spécifiez ne s'applique *pas* aux abonnements aux rubriques de session SXP pxGrid (par exemple, les mappages SGT de destination). Au lieu de cela, les mappages de rubriques de session sont conservés tant qu'il n'y a pas de message de suppression ou de mise à jour pour un mappage donné d'ISE.

Pour plus d'informations sur ISE/ISE-PIC, consultez [Source d'identité ISE/ISE-PIC](#).

- **Utilisateurs des agents des services de terminaux** : délai d'expiration pour les utilisateurs suivis par l'agent TS, qui est un type d'authentification passive. Pour en savoir plus, consultez [La source d'identité de l'agent des services de terminaux \(TS\)](#).
- **Utilisateurs du portail captif** : délai d'expiration pour les utilisateurs qui ont réussi à se connecter à l'aide du portail captif, qui est un type d'authentification active. Pour en savoir plus, consultez [Source d'identité du portail captif](#).
- **Utilisateurs du portail captif ayant échoué** : délai d'expiration pour les utilisateurs qui ne parviennent pas à se connecter à l'aide du portail captif. Vous pouvez configurer le **nombre maximal de tentatives de connexion** avant que l'utilisateur ne soit vu par centre de gestion comme ayant échoué à l'authentification. Un utilisateur ayant échoué à l'authentification peut éventuellement se voir accorder l'accès au réseau à l'aide de la politique de contrôle d'accès et, si tel est le cas, cette valeur de délai d'expiration s'applique à ces utilisateurs.

Pour en savoir plus sur les échecs de connexion au portail captif, consultez [Champs du portail captif](#).

- **Utilisateurs invités du portail captif** : délai d'expiration pour les utilisateurs qui se connectent au portail captif en tant qu'utilisateur invité. Pour en savoir plus, consultez [Source d'identité du portail captif](#).

Champs Répertoire de domaine et Synchroniser

Champs de répertoire de domaine

Ces paramètres s'appliquent aux serveurs individuels (comme les contrôleurs de domaine Active Directory) dans un domaine.

Nom d'hôte/adresse IP

Nom d'hôte complet du contrôleur de domaine Active Directory. Pour trouver le nom qualifié complet, consultez [Trouver le nom du serveur Active Directory, à la page 21](#).

Si vous utilisez Kerberos pour l'authentification du portail captif, assurez-vous également de comprendre les éléments suivants :

Si vous utilisez l'authentification Kerberos, le nom d'hôte du périphérique géré doit comporter moins de 15 caractères (il s'agit d'une limitation NetBIOS définie par Windows). Sinon, l'authentification du portail captif échoue. Vous définissez le nom d'hôte du périphérique géré lors de la configuration du périphérique. Pour en savoir plus, consultez un article comme celui-ci sur le site de documentation de Microsoft : [Conventions de dénomination dans Active Directory pour les ordinateurs, les domaines, les sites et les unités organisationnelles](#).

Le DNS doit renvoyer une réponse de 64 Ko ou moins au nom d'hôte; sinon, le test de connexion AD échoue. Cette limite s'applique dans les deux sens et est évoquée dans [la section 6.2.5 de la RFC 6891](#).

Port

Le port du serveur .

Encryption (Chiffrement)

(Fortement recommandé.) La méthode de chiffrement à utiliser :

- **STARTTLS** : connexion LDAP chiffrée
- **LDAPS** : connexion LDAP chiffrée
- **Aucun** : connexion LDAP non chiffrée (trafic non sécurisé)

Pour communiquer en toute sécurité avec un serveur Active Directory, consultez [Se connecter de manière sécurisée à Active Directory, à la page 20](#).

Certificat de l'autorité de certification

Le certificat TLS/SSL à utiliser pour l'authentification sur le serveur. Vous devez configurer **STARTTLS** ou **LDAPS** comme type de **chiffrement** pour utiliser un certificat TLS/SSL.

Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au **nom d'hôte ou à l'adresse IP** du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais **computer1.example.com** dans le certificat, la connexion échouera.

Interface utilisée pour la connexion au serveur d'annuaire

Requis uniquement pour l'authentification de VPN d'accès à distance afin que Cisco Secure Firewall Threat Defense puisse se connecter de manière sécurisée à votre serveur Active Directory. Cependant, cette interface n'est pas utilisée pour le téléchargement d'utilisateurs et de groupes.

Vous pouvez choisir uniquement un groupe d'interfaces routées. Pour en savoir plus, consultez [Interface](#).

Cliquez sur l'un des éléments suivants :

- **Résolution par recherche de routage** : utilisez le routage pour vous connecter au serveur Active Directory.
- **Choisissez une interface** : choisissez un groupe d'interfaces de périphérique géré spécifique pour vous connecter au serveur Active Directory.

Champs de synchronisation de l'utilisateur

Domaine AD principal

Pour les domaines Microsoft Active Directory uniquement. Domaine du serveur Active Directory où les utilisateurs doivent être authentifiés.



Remarque

Vous devez spécifier un **domaine principal AD** unique pour chaque domaine Microsoft Active Directory (AD). Bien que le système vous permette de spécifier le même **domaine AD principal** pour différents domaines Microsoft AD, le système ne fonctionnera pas correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier. Le système empêche de spécifier plus d'un domaine avec le même **domaine AD principal**, car les utilisateurs et les groupes ne seront pas identifiés correctement. Cela se produit parce que le système attribue un ID unique à chaque utilisateur et groupe de chaque *domaine*. par conséquent, le système ne peut pas identifier définitivement un utilisateur ou un groupe en particulier.

Saisir une requête pour rechercher des utilisateurs et des groupes

Nom unique de base

(Facultatif) L'arborescence de répertoires sur le serveur où le centre de gestion doit commencer à rechercher les données de l'utilisateur.

En règle générale, le nom distinctif (DN) de base a une structure de base indiquant le nom de domaine et l'unité opérationnelle de l'entreprise. Par exemple, l'organisation de la sécurité de l'entreprise Exemple pourrait avoir un DN de base de **ou=security,dc=example,dc=com**.

Nom unique du groupe

(Facultatif) L'arborescence du répertoire sur le serveur où le centre de gestion doit rechercher les utilisateurs ayant l'attribut de groupe. Une liste des attributs de groupe pris en charge figure dans la section [Noms d'attribut et de classe d'objet serveur pris en charge, à la page 7](#).



Remarque

Ni le nom du groupe ni le nom de l'unité organisationnelle ne peuvent contenir de caractères spéciaux comme l'astérisque (*), le égal (=), la barre oblique inverse (\), car les utilisateurs de ces groupes ne sont pas téléchargés et ne peuvent pas être utilisés dans les politiques d'identité.

Charger les groupes

Vous permet de télécharger des utilisateurs et des groupes pour la sensibilisation et le contrôle des utilisateurs.

Groupes disponibles, Ajouter à inclure, Ajouter à exclure

Limite les groupes qui peuvent être utilisés dans la politique.

- Les groupes affichés dans le champ **Groupes disponibles** le sont pour la politique, sauf si vous déplacez les groupes vers le champ **Groupes et utilisateurs inclus** ou **Groupes et utilisateurs exclus**.
- Si vous déplacez des groupes vers le champ **Groupes et utilisateurs inclus**, seuls les groupes et les utilisateurs qu'ils contiennent sont téléchargés, et les données des utilisateurs sont disponibles pour la sensibilisation et le contrôle de l'utilisateur.
- Si vous déplacez des groupes vers le champ **Groupes et utilisateurs exclus**, tous les groupes et utilisateurs qu'ils contiennent, à l'exception de ceux-ci, sont téléchargés et disponibles pour la sensibilisation et le contrôle de l'utilisateur.
- Pour inclure des utilisateurs de groupes qui ne sont pas inclus, saisissez le nom d'utilisateur dans le champ sous **User Inclusion** (Inclusion d'utilisateurs) et cliquez sur **Add** (Ajouter).
- Pour exclure des utilisateurs de groupes qui ne sont pas exclus, saisissez le nom d'utilisateur dans le champ sous **User Exclusion** (exclusion d'utilisateurs) et cliquez sur **Add** (Ajouter).

**Remarque**

Le nombre d'utilisateurs téléchargés dans centre de gestion est calculé à l'aide de la formule $R = I - (E+e) + i$, où

- R est la liste des utilisateurs téléchargés
- I sont les groupes inclus
- E sont les groupes exclus
- e sont les utilisateurs exclus
- i sont les utilisateurs inclus

Synchroniser maintenant

Cliquez pour synchroniser les groupes et les utilisateurs avec AD.

Commencez la synchronisation automatique à

Saisissez l'heure et l'intervalle de temps pour le téléchargement des utilisateurs et des groupes à partir d'AD.

Se connecter de manière sécurisée à Active Directory

Pour créer une connexion sécurisée entre un serveur Active Directory et centre de gestion (ce que nous recommandons fortement), vous devez effectuer toutes les tâches suivantes :

- Exportez le certificat racine du serveur Active Directory.
- Importez le certificat racine dans centre de gestion en tant que certificat d'autorité de certification de confiance.
- Recherchez le nom complet du serveur Active Directory.
- Créez le répertoire de domaine.

Consultez l'une des tâches suivantes pour en savoir plus.

Sujets connexes

[Exporter le certificat racine du serveur Active Directory](#), à la page 21

[Trouver le nom du serveur Active Directory](#), à la page 21

[Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine](#), à la page 10

Trouver le nom du serveur Active Directory

Pour configurer un répertoire de domaine dans centre de gestion, vous devez connaître le nom complet du serveur, que vous pouvez trouver comme indiqué dans la procédure qui suit.

Avant de commencer

Vous devez vous connecter au serveur Active Directory en tant qu'utilisateur disposant de privilèges suffisants pour afficher le nom de l'ordinateur.

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Connectez-vous au serveur Active Directory. |
| Étape 2 | Cliquez sur Start (Démarrer) . |
| Étape 3 | Cliquez avec le bouton droit sur Ce PC . |
| Étape 4 | Cliquez sur Propriétés (Propriétés). |
| Étape 5 | Cliquez sur Advanced System Settings (paramètres système avancés) . |
| Étape 6 | Cliquez sur l'onglet Nom de l'ordinateur . |
| Étape 7 | Notez la valeur de Full computer name (Nom complet de l'ordinateur).
Vous devez saisir ce nom exact lorsque vous configurez le répertoire de domaine dans FMC. |
-

Prochaine étape

[Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine](#), à la page 10.

Sujets connexes

[Exporter le certificat racine du serveur Active Directory](#), à la page 21

Exporter le certificat racine du serveur Active Directory

La tâche qui suit explique comment exporter le certificat racine du serveur Active Directory, qui est nécessaire pour se connecter de manière sécurisée à centre de gestion afin d'obtenir des informations d'identité de l'utilisateur.

Avant de commencer

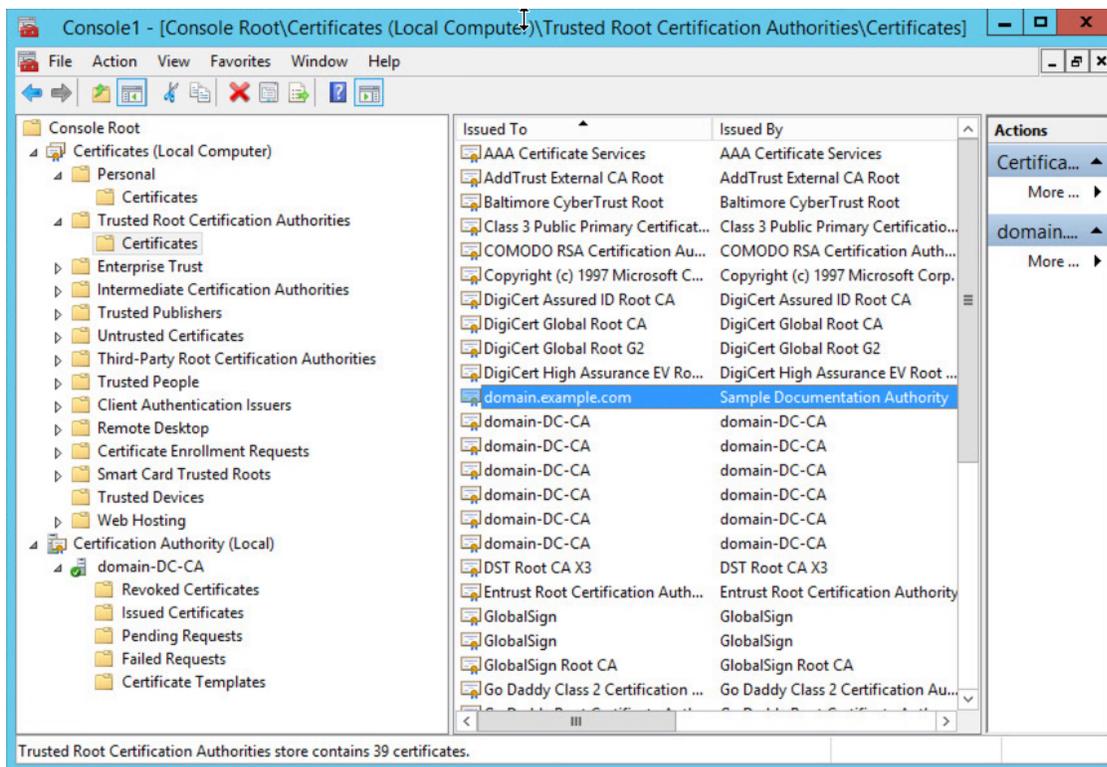
Vous devez connaître le nom du certificat racine de votre serveur Active Directory. Le certificat racine peut avoir le même nom que le domaine ou le certificat peut avoir un nom différent. La procédure qui suit montre une façon de déterminer le nom; il pourrait y avoir d'autres moyens, cependant.

Procédure

Étape 1

Voici une façon de trouver le nom du certificat racine du serveur Active Directory; consultez la documentation de Microsoft pour plus d'informations :

- a) Connectez-vous au serveur Active Directory en tant qu'utilisateur doté de privilèges pour exécuter des commandes sur la console de gestion Microsoft.
- b) Cliquez sur **Démarrer** et saisissez **mmc**.
- c) Cliquez sur **Fichier > Ajouter/supprimer un composant logiciel enfichable**.
- d) Dans la liste des composants logiciels enfichables disponibles dans le volet gauche, cliquez sur **Certificats (locaux)**.
- e) Cliquez sur **Add** (ajouter).
- f) Dans la boîte de dialogue du composant logiciel enfichable Certificats, cliquez sur **Compte de l'ordinateur** puis sur **Suivant**.
- g) Dans la boîte de dialogue de sélection d'ordinateurs, cliquez sur **Ordinateur local**, puis sur **Terminer**.
- h) *Windows Server 2012 uniquement*. Répétez les étapes précédentes pour ajouter le composant logiciel enfichable Autorité de certification.
- i) Cliquez sur **Console racine > Autorités de certification de confiance > Certificats**.
Les certificats de confiance du serveur s'affichent dans le volet droit. La figure suivante n'est qu'un exemple pour Windows Server2012; le vôtre sera probablement différent.



Étape 2

Exportez le certificat à l'aide de la commande **certutil**.

Il ne s'agit que d'une façon d'exporter le certificat. C'est un moyen pratique d'exporter le certificat, en particulier si vous pouvez faire fonctionner un navigateur Web et vous connecter à centre de gestion à partir du serveur Active Directory.

- a) Cliquez sur **Démarrer** et saisissez **cmd**.
- b) Saisissez la commande **certutil -ca.cert certificate-name**.
Le certificat du serveur s'affiche à l'écran.
- c) Copiez l'ensemble du certificat dans le presse-papier, en commençant par **-----BEGIN CERTIFICATE-----** et en terminant par **-----END CERTIFICATE-----** (y compris ces chaînes).

Prochaine étape

Importez le certificat du serveur Active Directory dans centre de gestion en tant que certificat d'autorité de certification de confiance, comme décrit dans la section [Ajout d'un objet autorité de certification de confiance](#).

Sujets connexes

[Trouver le nom du serveur Active Directory](#), à la page 21

Synchroniser les utilisateurs et les groupes

En cours de *synchronisation* des utilisateurs et des groupes, le centre de gestion interroge les domaines et les répertoires que vous avez configurés pour les groupes et les utilisateurs de ces groupes. Tous les utilisateurs que centre de gestion trouve, peuvent être utilisés dans les politiques d'identité.

Si des problèmes sont détectés, vous devrez probablement ajouter un domaine qui contient des utilisateurs et des groupes que centre de gestion ne peut pas téléverser. Pour de plus amples renseignements, consultez la section [Domaines et domaines de confiance](#), à la page 3.

Avant de commencer

Créez un centre de gestion *domaine* pour chaque domaine Active Directory et un centre de gestion *répertoire* pour chaque contrôleur de domaine Active Directory dans chaque forêt. Consultez [Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine](#), à la page 10.

Vous devez créer un domaine uniquement pour les domaines qui ont des utilisateurs que vous souhaitez utiliser dans le contrôle utilisateur.

Vous pouvez imbriquer groupes AD Microsoft et Cisco Secure Firewall Management Center télécharge ces groupes et les utilisateurs qu'ils contiennent. Vous pouvez éventuellement restreindre les groupes et les utilisateurs téléchargés, comme indiqué dans [Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine](#), à la page 10.

Procédure

- Étape 1** Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.
- Étape 2** Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
- Étape 3** À côté de chaque domaine, cliquez sur **Télécharger** (↓).
- Étape 4** Pour voir les résultats, cliquez sur l'onglet **Résultats de la synchronisation**.
La colonne Realms indique s'il y a eu ou non des problèmes de synchronisation des utilisateurs et des groupes dans les forêts Active Directory. Recherchez les indicateurs suivants à côté de chaque domaine.

Indicateur dans la colonne Realms (Domaines)	Signification
(Rien)	Tous les utilisateurs et groupes ont été synchronisés sans erreur. Aucune action n'est nécessaire.
Triangle jaune (⚠)	Des problèmes sont survenus lors de la synchronisation des utilisateurs et des groupes. Assurez-vous d'avoir ajouté un domaine pour chaque domaine Active Directory et un répertoire pour chaque contrôleur de domaine Active Directory. Pour en savoir plus, consultez Dépannage de la confiance interdomaine , à la page 39.

Créer une séquence de domaine

La procédure suivante vous permet de créer une séquence de domaine, qui est une liste ordonnée de domaines recherchés par le système lorsqu'il applique une politique d'identité. Vous ajoutez une séquence de domaine à une règle d'identité exactement de la même manière que vous ajoutez un domaine; la différence est que le système recherche tous les domaines dans l'ordre spécifié dans la séquence de domaine lors de l'application d'une politique d'identité.

Avant de commencer

Vous devez créer et activer au moins deux domaines, chacun correspondant à une connexion avec un serveur Active Directory. Vous ne pouvez pas créer de séquences de domaine pour les domaines LDAP.

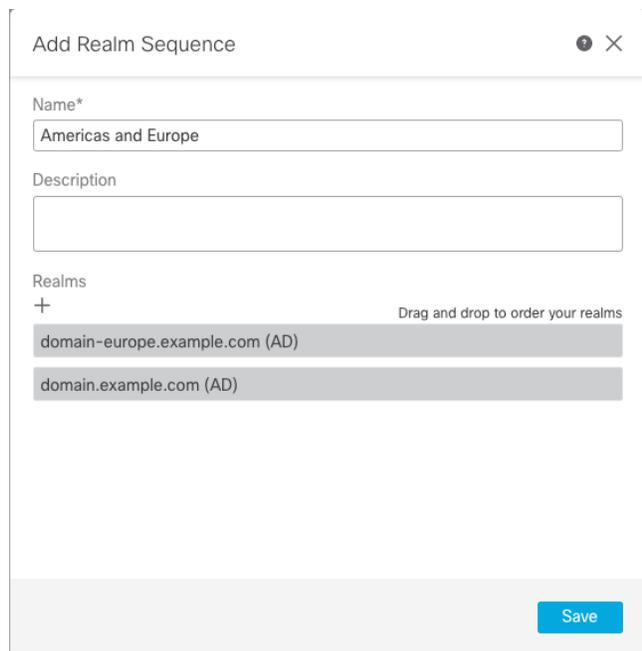
Créez un domaine comme décrit dans [Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine](#), à la page 10.

Procédure

- Étape 1** Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.
- Étape 2** Cliquez sur **Intégration (intégration) > Other Integrations (autres intégrations) > Realms (domaines) > Realm Sequences (séquences de domaines)**.
- Étape 3** Cliquez sur **Add Sequence** (Ajouter une séquence).
- Étape 4** Dans le champ **Name**, saisissez un nom pour identifier la séquence de domaine.
- Étape 5** (Facultatif) Dans le champ **Description**, saisissez une description pour la séquence de domaine.
- Étape 6** Sous Domaines, cliquez sur **Ajouter** (+).
- Étape 7** Cliquez sur le nom de chaque domaine à ajouter à la séquence.

Pour affiner votre recherche, saisissez tout ou une partie du nom de domaine dans le champ **Filter** (filtre).
- Étape 8** Cliquez sur **OK**.
- Étape 9** Dans la boîte de dialogue Add Realm Sequence (ajouter une séquence de domaine), faites glisser et déposez les domaines dans l'ordre dans lequel vous souhaitez que le système les recherche.

La figure suivante montre un exemple de séquence de domaine composée de deux domaines. Le domaine **domain-europe.example.com** fera l'objet de la recherche d'utilisateurs avant le domaine **domain.example.com**



Add Realm Sequence

Name*

Americas and Europe

Description

Realms

+ Drag and drop to order your realms

domain-europe.example.com (AD)

domain.example.com (AD)

Save

Étape 10 Cliquez sur **Save** (enregistrer).

Prochaine étape

Consultez [Créer une politique d'identité](#).

Configurer le Centre de gestion pour la confiance interdomaine : l'installation

Il s'agit d'une présentation de plusieurs rubriques qui vous guident dans la configuration du centre de gestion à deux domaines avec approbation interdomaine.

Cet exemple étape par étape implique deux forêts : **forest.example.com** et **eastforest.example.com**. Les forêts sont configurées de sorte que certains utilisateurs et groupes de chaque forêt puissent être authentifiés par Microsoft AD dans l'autre forêt.

Voici l'exemple de configuration utilisé dans cet exemple.



En utilisant l'exemple précédent, vous configurez le centre de gestion comme suit :

- Domaine et annuaire de n'importe quel domaine dans **forest.example.com** qui contient les utilisateurs que vous souhaitez contrôler avec la politique de contrôle d'accès
- Domaine et annuaire de n'importe quel domaine dans **eastforest.example.com** qui contient les utilisateurs que vous souhaitez contrôler avec la politique de contrôle d'accès

Chaque domaine de l'exemple possède un contrôleur de domaine, qui est configuré dans le centre de gestion comme répertoire. Les répertoires dans cet exemple sont configurés comme suit :

- **forest.example.com**
 - Nom distinctif (DN) de base pour les utilisateurs : **ou=UsersWest,dc=forest,dc=example,dc=com**
 - DN de base pour les groupes : **ou=EngineeringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
 - DN de base pour les utilisateurs : **ou=EastUsers,dc=eastforest,dc=example,dc=com**
 - DN de base pour les groupes : **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

Sujets connexes

[Configurer le Cisco Secure Firewall Management Center pour la confiance interdomaine Étape 1 : configuration des domaines et des répertoires](#), à la page 26

Configurer le Cisco Secure Firewall Management Center pour la confiance interdomaine Étape 1 : configuration des domaines et des répertoires

Il s'agit de la première tâche d'une procédure étape par étape qui explique comment configurer le centre de gestion pour reconnaître les serveurs Active Directory configurés dans une relation d'approbation interdomaine, qui est une configuration de plus en plus courante pour les entreprises. Pour une présentation de cet exemple de configuration, consultez [Configurer le Centre de gestion pour la confiance interdomaine : l'installation, à la page 25](#).

Si vous configurez le système avec un domaine pour chaque domaine et un répertoire pour chaque contrôleur de domaine, le système peut détecter jusqu'à 100 000 [principaux de sécurité étrangers](#) (utilisateurs et groupes). Si ces principaux de sécurité étrangers correspondent à un utilisateur téléchargé dans un autre domaine, ils peuvent être utilisés dans la politique de contrôle d'accès.

Avant de commencer

Vous devez configurer les serveurs Microsoft Active Directory dans une relation d'approbation entre domaines; Consultez [Domaines et domaines de confiance](#), à la page 3 pour plus d'informations.

Si vous authentifiez les utilisateurs avec LDAP, vous *ne pouvez pas* utiliser cette procédure.

Procédure

- Étape 1** Connectez-vous au centre de gestion.
- Étape 2** Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
- Étape 3** Choisissez dans la liste déroulante **Add Realm** (ajouter un domaine) .
- Étape 4** Saisissez l'information suivante pour configurer **forest.example.com**.

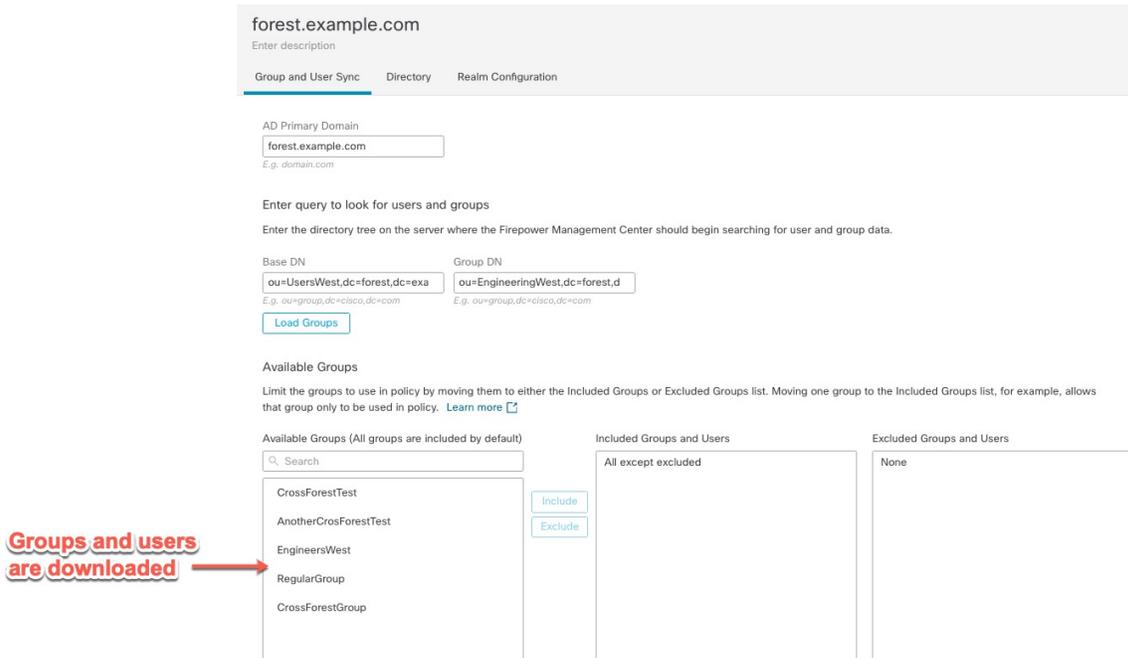
The screenshot shows the 'Add New Realm' configuration window. It includes the following fields and sections:

- Name***: forest.example.com
- Description**: (empty)
- Type**: AD
- AD Primary Domain**: forest.example.com (with example: E.g. domain.com)
- Directory Username***: limited.user@forest.example.com (with example: E.g. user@domain.com)
- Directory Password***: (masked with dots)
- Base DN**: ou=Users,dc=forest,dc=example,dc=com (with example: E.g. ou=group,dc=cisco,dc=com)
- Group DN**: :ringWest,dc=forest,dc=example,dc=com (with example: E.g. ou=group,dc=cisco,dc=com)
- Proxy**: MyProxySequence (highlighted with a red circle and number 5)
- Directory Server Configuration**:
 - Hostname/IP Address*: 192.168.0.200
 - Port*: 389
 - Encryption: None
 - CA Certificate: Select certificate
 - Interface used to connect to Directory server:
 - Resolve via route lookup
 - Choose an interface (Default: Management/Diagnostic Interface)
 - Test** button (highlighted with a red circle and number 6) with a green checkmark and the text 'Test connection succeeded'.
- Buttons**: Cancel and **Configure Groups and Users** (highlighted with a red circle and number 7).

Remarque Le nom d'utilisateur de l'annuaire peut être n'importe quel utilisateur du domaine Active Directory; aucune autorisation spéciale n'est requise.

L'interface utilisée pour la connexion au serveur d'annuaire peut être n'importe quelle interface pouvant se connecter au serveur Active Directory.

- Étape 5 Un **proxy** est un périphérique géré facultatif ou une séquence proxy permettant de communiquer avec ISE ou ISE-PIC si CDO n'est pas en mesure de le faire. Par exemple, votre CDO peut être dans un nuage public, mais le serveur ISE/ISE-PIC peut se trouver sur un intranet interne.
- Étape 6 cliquez sur **Tester** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.
- Étape 7 Cliquez sur **Configure Groups and Users** (Configurer les groupes et les utilisateurs).
- Étape 8 Si votre configuration a réussi, la page suivante s'affiche semblable à ce qui suit.



Remarque Si les groupes et les utilisateurs n'ont pas été téléchargés, vérifiez les valeurs des champs **DN de base** et **Groups DN**, puis cliquez sur **Load Groups** (téléverser les groupes).

D'autres configurations facultatives sont disponibles sur cette page; pour plus d'informations à leur sujet, consultez [Champs de domaine, à la page 13](#) et [Champs Répertoire de domaine et Synchroniser, à la page 18](#).

- Étape 9 Si vous avez apporté des modifications à cette page ou à des pages à onglet, cliquez sur **Save** (Enregistrer).
- Étape 10 Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
- Étape 11 Cliquez sur **Add Realm** (ajouter un domaine).
- Étape 12 Saisissez l'information suivante pour configurer **eastforest.example.com**.

Add New Realm
?
✕

<p>Name*</p> <input type="text" value="eastforest.example.com"/>	<p>Description</p> <input type="text"/>
<p>Type</p> <input type="text" value="AD"/>	<p>AD Primary Domain</p> <input type="text" value="eastforest.example.com"/> <p><small>E.g. domain.com</small></p>
<p>Directory Username*</p> <input type="text" value="limited.eastuser@eastforest.example.com"/> <p><small>E.g. user@domain.com</small></p>	<p>Directory Password*</p> <input type="password" value="....."/>
<p>Base DN</p> <input type="text" value="jUsers,dc=eastforest,dc=example,dc=com"/> <p><small>E.g. ou=group,dc=cisco,dc=com</small></p>	<p>Group DN</p> <input type="text" value="eering,dc=eastforest,dc=example,dc=com"/> <p><small>E.g. ou=group,dc=cisco,dc=com</small></p>

Directory Server Configuration

▲ eastforest.example.com:636

<p>Hostname/IP Address*</p> <input type="text" value="eastforest.example.com"/>	<p>Port*</p> <input type="text" value="636"/>
<p>Encryption</p> <input type="text" value="LDAPS"/>	<p>CA Certificate*</p> <input type="text" value="EastForest"/>

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface ▾

Test

✔ Test connection succeeded

Add another directory

Cancel

Configure Groups and Users

Étape 13

cliquez sur **Tester** et assurez-vous que l'essai réussit avant de sauvegarder le connecteur.

Étape 14

Cliquez sur **Configure Groups and Users** (Configurer les groupes et les utilisateurs).

Étape 15

Si votre configuration a réussi, la page suivante s'affiche semblable à ce qui suit.

eastforest.example.com
Cancel Save

Enter description

Group and User Sync
Directory
Realm Configuration

AD Primary Domain

E.g. domain.com

Enter query to look for users and groups

Enter the directory tree on the server where the Firewall Management Center should begin searching for user and group data.

Base DN

E.g. ou=group,dc=cisco,dc=com

Group DN

E.g. ou=group,dc=cisco,dc=com

[Load Groups](#)

Available Groups

Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

No groups were found

Included Groups and Users

All except excluded

Excluded Groups and Users

None

[Include](#)

[Exclude](#)

Sujets connexes

[Configurer le centre de gestion pour l'approbation interdomaine - Étape 2 : Synchroniser les utilisateurs et les groupes](#), à la page 31

Configurer le centre de gestion pour l'approbation interdomaine - Étape 2 : Synchroniser les utilisateurs et les groupes

Après avoir configuré au moins deux serveurs Active Directory qui ont une relation d'approbation entre domaines, vous devez télécharger les utilisateurs et les groupes. Ce processus met en évidence des problèmes possibles de configuration Active Directory (par exemple, les groupes ou les utilisateurs téléchargés pour un domaine Active Directory mais pas pour l'autre).

Avant de commencer

Assurez-vous d'avoir effectué les tâches décrites dans [Configurer le Cisco Secure Firewall Management Center pour la confiance interdomaine Étape 1 : configuration des domaines et des répertoires](#), à la page 26.

Procédure

- Étape 1** Connectez-vous au centre de gestion.
- Étape 2** Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
- Étape 3** À la fin de la ligne de n'importe quel domaine de l'approbation interdomaine, cliquez sur (Télécharger maintenant), puis sur **Yes (Oui)**.

Étape 4 Cliquez sur **Coche** (✔) (Notifications) > **Tâches** .

Si les groupes et les utilisateurs ne parviennent pas à télécharger , réessayez. Si les tentatives suivantes échouent, passez en revue la configuration de votre domaine et de votre répertoire comme indiqué dans [Champs de domaine, à la page 13](#) et [Champs Répertoire de domaine et Synchroniser, à la page 18](#).

Si vous utilisez un serveur mandataire ou une séquence mandataire , assurez-vous que tous les périphériques gérés peuvent communiquer avec Active Directory ou ISE/ISE-PIC. Si plusieurs périphériques gérés peuvent communiquer avec ISE/ISE-PIC, nous vous recommandons de configurer une séquence proxy pour le domaine, comme indiqué dans la section [Créer une séquence de serveur mandataire, à la page 8](#) de serveur mandataire

Étape 5 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Sync Results (synchronisation des résultats)**.

Sujets connexes

[Configurer le centre de gestion pour la confiance interdomaine - Étape 3 : Résoudre les problèmes](#), à la page 32

Configurer le centre de gestion pour la confiance interdomaine - Étape 3 : Résoudre les problèmes

La dernière étape de la configuration de l'approbation interdomaine dans centre de gestion consiste à s'assurer que les utilisateurs et les groupes sont téléchargés sans erreur. Une raison typique pour laquelle les utilisateurs et les groupes ne téléchargent pas correctement est que les domaines auxquels ils appartiennent n'ont pas été téléchargés sur centre de gestion.

Cette rubrique explique comment diagnostiquer qu'un groupe référencé dans un ensemble ne peut pas être téléchargé, car le domaine n'est pas configuré pour trouver le groupe dans la hiérarchie des contrôleurs de domaine.

Avant de commencer

Procédure

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

Étape 2 Cliquez sur **Integration (intégration)** > **Other Integrations (autres intégrations)** > **Realms (domaines)** > **Sync Results (synchronisation des résultats)**.

Dans la colonne Realms (Domaines), si **Triangle jaune** (▲) s'affiche à côté du nom d'un domaine, des problèmes doivent être résolus. Sinon, vos résultats sont configurés correctement et vous pouvez quitter l'écran.

Étape 3 Téléchargez de nouveau les utilisateurs et les groupes à partir des domaines qui affichent des problèmes.

a) Cliquez sur l'onglet **Realms** (Domaines).

b) Cliquez sur  (Télécharger maintenant), puis sur **Yes**(oui).

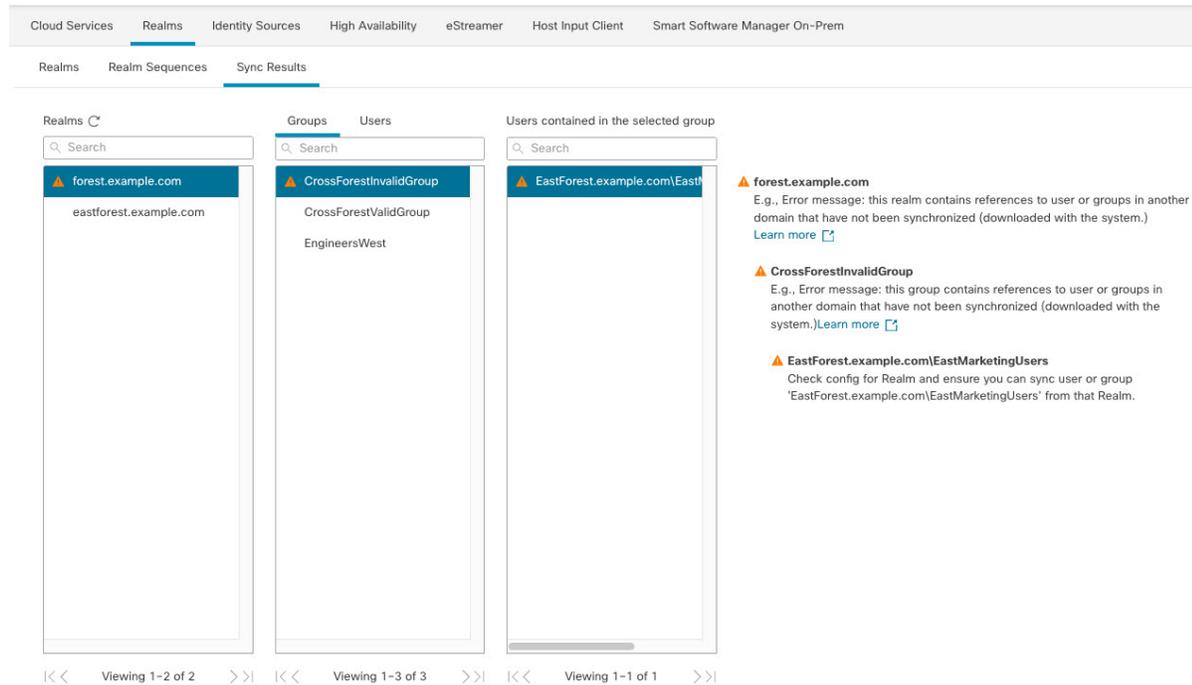
Étape 4 Cliquez sur la page à onglet des **résultats de la synchronisation**.

Si un **Triangle jaune** (▲) s'affiche dans la colonne Domaines, cliquez sur **Triangle jaune** (▲) à côté du domaine qui présente des problèmes.

Étape 5 Dans la colonne du milieu, cliquez sur **Groups** (Groupes) ou **Users** (Utilisateurs) pour trouver plus d'informations.

Étape 6 Dans la page à onglet Groupes ou Utilisateurs, cliquez sur **Triangle jaune** (▲) pour afficher plus d'informations.

La colonne de droite doit contenir suffisamment de renseignements pour vous permettre de déterminer la source du problème.



Dans l'exemple précédent, **forest.example.com** comprend un groupe interdomaine **CrossForestInvalidGroup** qui contient un autre groupe **EastMarketingUsers** qui n'a pas été téléchargé par centre de gestion. Si, après la nouvelle synchronisation du domaine **eastforest.example.com**, l'erreur ne se résout pas, cela signifie probablement que le contrôleur de domaine Active Directory n'inclut pas **EastMarketingUsers**.

Pour résoudre ce problème, vous pouvez :

- Supprimer **EastMarketingUsers** de **CrossForestInvalidGroup**, synchroniser à nouveau le domaine **forest.example.com** et vérifier à nouveau.
- Supprimez la valeur **ou=EastEngineering** du **DN de groupe** du domaine **eastforest.example.com**, ce qui permet à centre de gestion de récupérer les groupes du niveau le plus élevé dans la hiérarchie Active Directory, de synchroniser **eastforest.example.com** et de vérifier de nouveau.

Gérer un domaine

Cette section explique comment effectuer diverses tâches de maintenance pour un domaine à l'aide des contrôles de la page Domaines. Tenez compte des points suivants :

- Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.
- Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Procédure

- Étape 1** Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.
- Étape 2** Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
- Étape 3** Pour supprimer un domaine, cliquez sur **Supprimer** (🗑).
- Étape 4** Pour modifier un domaine, cliquez sur **Edit** (✎) à côté du domaine et apportez les modifications comme décrit dans [Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 10](#).
- Étape 5** Pour activer un domaine, faites glisser **l'état** vers la droite; pour désactiver un domaine, faites-le glisser vers la gauche.
- Étape 6** Pour télécharger des utilisateurs et des groupes d'utilisateurs, cliquez sur **Télécharger** (↓).
- Étape 7** Pour copier un domaine, cliquez sur **Copier** (📄).
- Étape 8** Pour comparer les domaines, consultez [Comparer les domaines, à la page 34](#).
-

Comparer les domaines

Vous devez être un Admin, Administrateur d'accès, Administrateur de réseau ou Approbateur de sécurité pour effectuer cette tâche.

Procédure

- Étape 1** Connectez-vous au centre de gestion.
- Étape 2** Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
- Étape 3** Cliquez sur **Compare Realms** (Comparer les domaines).
- Étape 4** Choisissez **Compare Realm** (Comparer le domaine) dans la liste **Compare Against** (Comparer par rapport à).
- Étape 5** Choisissez les domaines que vous souhaitez comparer dans les listes des domaines **A** et **B**.
- Étape 6** Cliquez sur **OK**.
- Étape 7** Pour naviguer individuellement dans les modifications, cliquez sur **Précédent** ou **Suivant** au-dessus de la barre de titre.
- Étape 8** (Facultatif) Cliquez sur **Comparison Report** pour générer le rapport de comparaison de domaine.
- Étape 9** (Facultatif) Cliquez sur **New Comparison** pour générer une nouvelle vue de comparaison de domaine.
-

Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs

Si vous remarquez un comportement inattendu de la connexion du serveur, envisagez d'ajuster votre configuration de domaine, les paramètres de périphérique ou les paramètres de serveur. Pour d'autres renseignements de dépannage, consultez :

- [Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec](#)
- [Dépannage de la source d'identité de l'agent TS](#)
- [Dépannage de la source d'identité du portail captif](#)
- [Dépanner la source d'identité du VPN d'accès à distance](#)
- [Dépannage du contrôle d'utilisateur](#)

Symptôme : domaines et groupes signalés, mais non téléchargés

Le moniteur d'intégrité de centre de gestion vous informe des non-concordances d'utilisateurs ou de domaine, qui sont définies comme suit :

- Incompatibilité de l'utilisateur : un utilisateur est signalé à centre de gestion sans être téléchargé.
Une raison typique d'une incompatibilité d'utilisateur est que l'utilisateur appartient à un groupe que vous avez exclu du téléchargement sur centre de gestion. Passez en revue les renseignements décrits dans la section [Guide de configuration Cisco Secure Firewall Management Center Device](#).
- Incompatibilité de domaine : un utilisateur se connecte à un domaine qui correspond à un domaine inconnu de centre de gestion.

Par exemple, si vous avez défini un domaine qui correspond à un domaine nommé **domain.example.com** dans centre de gestion, mais qu'une connexion est signalée à partir d'un domaine nommé **another-domain.example.com**, il y a une *incompatibilité de domaine*. Les utilisateurs de ce domaine sont identifiés par centre de gestion comme Inconnus.

Vous définissez le seuil d'incompatibilité sous forme de pourcentage, au-dessus duquel un avertissement d'intégrité est déclenché. Exemples :

- Si vous utilisez le seuil d'incompatibilité par défaut de 50 % et qu'il y a deux domaines non concordants dans huit sessions entrantes, le pourcentage d'incompatibilité est de 25 % et aucun avertissement n'est déclenché.
- Si vous définissez le seuil d'incompatibilité à 30 % et qu'il y a trois domaines non concordants dans cinq sessions entrantes, le pourcentage d'incompatibilité est de 60 % et un avertissement est déclenché.

Aucune politique n'est appliquée aux utilisateurs inconnus qui ne correspondent pas aux règles d'identité. (Bien que vous puissiez configurer des règles d'identité pour les utilisateurs inconnus, nous vous recommandons de réduire le nombre de règles au minimum en identifiant correctement les utilisateurs et les domaines.)

Pour en savoir plus, consultez [Détection des non-concordances de domaines ou d'utilisateurs](#), à la page 38.

Symptôme : Les utilisateurs ne sont pas téléchargés

Les causes possibles sont les suivantes :

- Si le **type** de domaine est mal configuré, les utilisateurs et les groupes ne peuvent pas être téléchargés en raison d'une incompatibilité entre l'attribut attendu par le système et ce que le référentiel fournit. Par exemple, si vous configurez le **type** sur **LDAP** pour un domaine Microsoft Active Directory, le système attend l'attribut `uid`, qui est défini comme `none` sur Active Directory. (Les référentiels Active Directory utilisent `sAMAccountName` comme ID utilisateur.)

Solution : Définissez le champ **Type** de domaine de manière appropriée : **AD** pour Microsoft Active Directory ou **LDAP** pour un autre référentiel LDAP pris en charge.

- Les utilisateurs des groupes Active Directory qui ont des caractères spéciaux dans le nom de l'unité d'organisation peuvent ne pas être disponibles pour les règles de politique d'identité. Par exemple, si le nom d'un groupe ou d'une unité organisationnelle contient les caractères astérisque (*), égal (=) ou barre oblique inverse (\), les utilisateurs de ces groupes ne sont pas téléchargés et ne peuvent pas être utilisés pour les politiques d'identité.

Solution : Supprimer les caractères spéciaux du nom du groupe ou de l'unité organisationnelle.

**Important**

Pour réduire la latence entre Cisco Secure Firewall Management Center et votre contrôleur de domaine Active Directory, nous vous recommandons fortement de configurer un répertoire de domaine (c'est-à-dire le contrôleur de domaine) qui est aussi proche que possible géographiquement de Cisco Secure Firewall Management Center.

Par exemple, si votre Cisco Secure Firewall Management Center est en Amérique du Nord, configurez un répertoire de domaine qui se trouve également en Amérique du Nord. Ne pas le faire peut entraîner des problèmes tels que l'expiration du délai de téléchargement des utilisateurs et des groupes.

Symptôme : tous les utilisateurs d'un domaine ne sont pas téléchargés

Les causes possibles sont les suivantes :

- Si vous tentez de télécharger plus que le nombre maximal d'utilisateurs dans un domaine, le téléchargement s'arrête au nombre maximal d'utilisateurs et une alerte d'intégrité s'affiche. Les limites de téléchargement d'utilisateur sont définies par le modèle Cisco Secure Firewall Management Center.
- Chaque utilisateur doit être membre d'un groupe. Les utilisateurs qui ne sont membres d'aucun groupe ne sont pas téléchargés.

Symptôme : la politique de contrôle d'accès ne correspond pas à l'appartenance à un groupe

Cette solution s'applique à un domaine AD qui est dans une relation d'approbation avec d'autres domaines AD. Dans la discussion qui suit, *domaine externe* désigne un domaine autre que celui auquel l'utilisateur se connecte.

Si un utilisateur appartient à un groupe défini dans un domaine externe de confiance, centre de gestion n'effectue pas le suivi de l'appartenance dans le domaine externe. Par exemple, examinez les scénarios suivants :

- Les contrôleurs de domaine 1 et 2 se font mutuellement confiance
- Le groupe A est défini sur le contrôleur de domaine 2

- L'utilisateur `mparvinder` dans le contrôleur 1 est membre du groupe A

Même si l'utilisateur `mparvinder` figure dans le groupe A, les règles de politique de contrôle d'accès centre de gestion des règles d'appartenance au groupe A ne correspondent pas.

Solution : créez un groupe similaire dans le contrôleur de domaine 1 qui contient tous les comptes du domaine 1 qui appartiennent au groupe A. Modifiez la règle de politique de contrôle d'accès pour qu'elle corresponde à n'importe quel membre du groupe A ou du groupe B.

Symptôme : la politique de contrôle d'accès ne correspond pas à l'appartenance au domaine enfant

Si un utilisateur appartient à un domaine qui est enfant du domaine parent, Firepower ne suit pas les relations parent/enfant entre les domaines. Par exemple, examinez les scénarios suivants :

- Le domaine enfant `.parent.com` est un enfant du domaine `parent.com`
- L'utilisateur `mparvinder` est défini dans `enfant.parent.com`

Même si l'utilisateur `mparvinder` se trouve dans un domaine enfant, la politique de contrôle d'accès Firepower correspondant à `parent.com` ne correspond pas à `mparvinder` dans le domaine `enfant.parent.com`.

Solution : modifiez la règle de politique de contrôle d'accès pour qu'elle corresponde à l'appartenance à `parent.com` ou à `enfant.parent.com`.

Symptôme : échec du domaine ou du répertoire de domaine

Le bouton **Tester** sur la page du répertoire envoie une requête LDAP au nom d'hôte ou à l'adresse IP que vous avez saisi. En cas d'échec, vérifiez les éléments suivants :

- Le **nom d'hôte** que vous avez saisi correspond à l'adresse IP d'un serveur LDAP ou d'un contrôleur de domaine Active Directory.
- L'**adresse IP** que vous avez saisie est valide.

Le bouton **Test AD Join** (Tester la jonction AD) de la page de configuration de domaine vérifie les éléments suivants :

- Le DNS résout le **domaine principal AD** en une adresse IP de serveur LDAP ou d'un contrôleur de domaine Active Directory.
- Le **nom d'utilisateur** et le **mot de passe AD Join** sont corrects.

Le **nom d'utilisateur de jointure AD** doit être complet; (par exemple, `administrateur@mondomaine.com`, *non administrateur*).

- L'utilisateur dispose de privilèges suffisants pour créer un ordinateur dans le domaine et joindre centre de gestion au domaine en tant qu'ordinateur de domaine.

Symptôme : des délais d'expiration d'utilisateur se produisent à des moments inattendus

Si vous remarquez que le système effectue des délais d'utilisateur à des intervalles inattendus, confirmez que l'heure de votre serveur ISE/ISE-PIC est synchronisée avec l'heure de Cisco Secure Firewall Management Center. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.

Si vous remarquez que le système expire à des intervalles inattendus, vérifiez que l'heure de votre serveur ISE/ISE-PIC ou de votre serveur d'agent TS est synchronisée avec l'heure de Cisco Secure Firewall Management Center. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.

Symptôme : les données utilisateur pour des utilisateurs ISE/ISE-PIC inconnus ne s'affichent pas dans l'interface Web

Une fois que le système a détecté une activité d'un utilisateur d'agent ISE/ISE-PIC ou TS dont les données ne sont pas encore dans la base de données, il récupère les informations à ce sujet sur le serveur. Dans certains cas, le système a besoin de plus de temps pour récupérer avec succès cette information des serveurs Microsoft Windows. Tant que la récupération des données n'est pas réussie, l'activité vue par l'ISE/ISE-PIC ou l'utilisateur de l'agent TS ne s'affiche *pas* dans l'interface Web.

Notez que cela peut également empêcher le système de gérer le trafic de l'utilisateur à l'aide des règles de contrôle d'accès.

Symptôme : les données utilisateur dans les événements sont inattendues

Si vous remarquez que des événements d'activités d'utilisateurs ou d'utilisateurs contiennent des adresses IP inattendues, vérifiez vos domaines. Le système ne prend pas en charge la configuration de plusieurs domaines avec la même valeur **de domaine AD principal**.

Symptôme : les utilisateurs provenant des connexions au serveur de terminaux ne sont pas identifiés de manière unique par le système

Si votre déploiement comprend un serveur de terminal et que vous avez un domaine configuré pour un ou plusieurs serveurs connectés au serveur de terminal, vous devez déployer l'agent Cisco Terminal Services (TS) pour signaler avec précision les connexions d'utilisateurs dans les environnements de serveur de terminal. Une fois installé et configuré, l'agent TS attribue des ports uniques aux utilisateurs afin que le système puisse identifier de manière unique ces utilisateurs dans l'interface Web.

Pour en savoir plus sur l'agent TS, consultez le *Guide de l'agent Cisco Terminal Services (TS)*.

Détecter les non-concordances de domaines ou d'utilisateurs

Cette section explique comment détecter les *incompatibilités* de domaine ou d'utilisateur, qui sont définies comme suit :

- Incompatibilité de l'utilisateur : un utilisateur est signalé à centre de gestion sans être téléchargé.
Une raison typique d'une incompatibilité d'utilisateur est que l'utilisateur appartient à un groupe que vous avez exclu du téléchargement sur centre de gestion. Passez en revue les renseignements décrits dans la section [Guide de configuration Cisco Secure Firewall Management Center Device](#).
- Incompatibilité de domaine : un utilisateur se connecte à un domaine qui correspond à un domaine inconnu de centre de gestion.

Pour en savoir plus, consultez [Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs, à la page 35](#).

Aucune politique n'est appliquée aux utilisateurs inconnus qui ne correspondent pas aux règles d'identité. (Bien que vous puissiez configurer des règles d'identité pour les utilisateurs inconnus, nous vous recommandons de réduire le nombre de règles au minimum en identifiant correctement les utilisateurs et les domaines.)

Procédure

Étape 1

Activer la détection des incompatibilités de domaine ou d'utilisateur :

- a) Connectez-vous au centre de gestion si vous ne l'avez pas déjà fait.
- b) Cliquez sur **System (Système) > Health (Intégrité) > Policy (Politique)**.
- c) Créez une nouvelle politique de contrôle d'intégrité ou modifiez une politique existante.
- d) Dans la page de modification de la politique, définissez un **intervalle d'exécution des politiques**. Il s'agit de la fréquence à laquelle toutes les tâches de surveillance de l'intégrité sont exécutées.
- e) Dans le volet de gauche, cliquez sur **Realm (Domaine)**.
- f) Saisissez l'information suivante :
 - **Activé** : Cliquez sur.
 - **Warning Users match threshold % (% d'atteinte du seuil d'avertissement des utilisateurs)** : pourcentage de non-concordances de domaines ou d'utilisateurs qui déclenche un avertissement dans le moniteur d'intégrité. Pour en savoir plus, consultez [Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs](#), à la page 35.
- g) Au bas de la page, cliquez sur **Save Policy and Exit** (Sauvegarder la politique et quitter).
- h) Appliquez la politique d'intégrité aux périphériques gérés, comme indiqué dans *Application des politiques d'intégrité* dans [Guide d'administration Cisco Secure Firewall Management Center](#).

Étape 2

Affichez les non-concordances entre les utilisateurs et les domaines de l'une des manières suivantes :

- Si le seuil d'avertissement est dépassé, cliquez sur **Avertissement > Intégrité** dans la partie supérieure de centre de gestion. Cela ouvre le moniteur d'intégrité.
- Cliquez sur **System (Système) > Health (Intégrité) > Monitor (Moniteur)**.

Étape 3

Dans la page Health Monitor (Moniteur d'intégrité), dans la colonne Display (Afficher), développez **Realm: Domain** ou **Realm: User** (Domaine : Domaine ou Utilisateur) pour afficher les détails de la non-concordance.

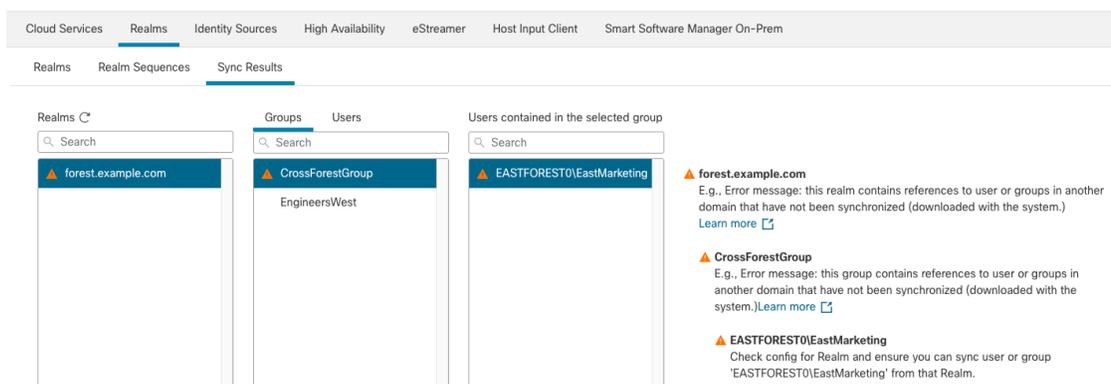
Dépannage de la confiance interdomaine

Les problèmes typiques de dépannage de la configuration centre de gestion pour l'approbation interdomaine sont les suivants :

- N'ajoutez pas de domaine ou de répertoire pour toutes les forêts qui ont des groupes partagés;
- Configurez un domaine pour exclure les utilisateurs du téléchargement. Ces utilisateurs sont référencés dans un groupe dans un domaine différent.
- Certains problèmes temporaires

Comprendre les problèmes

Si la synchronisation par centre de gestion des utilisateurs et des groupes avec vos forêts Active Directory pose problème, la page de l'onglet Résultats de la synchronisation s'affiche comme suit.



Le tableau suivant explique comment interpréter ces informations.

Colonne	Signification
Domaine	Affiche tous les domaines configurés dans le système. Cliquez sur Actualisation (🔄) pour mettre à jour la liste des domaines. Triangle jaune (⚠️) s'affiche pour indiquer des problèmes dans le domaine. Rien ne s'affiche à côté d'un domaine si tous les utilisateurs et groupes ont été synchronisés.
Groupes	Cliquez sur Groups (groupes) pour afficher tous les groupes du domaine. Comme pour les domaines, Triangle jaune (⚠️) s'affiche pour indiquer des problèmes. Cliquez sur Triangle jaune (⚠️) pour afficher davantage de renseignements sur le problème.
Utilisateurs	Cliquez sur Users (utilisateurs) pour afficher tous les utilisateurs, triés par groupe.
Utilisateurs compris dans le groupe sélectionné	Affiche tous les utilisateurs du groupe que vous avez sélectionné dans la colonne Groups (groupes). Cliquez sur Triangle jaune (⚠️) pour afficher plus d'informations à droite du tableau.
Groupes contenant l'utilisateur sélectionné	Affiche tous les groupes auxquels l'utilisateur sélectionné appartient. Cliquez sur Triangle jaune (⚠️) pour afficher plus d'informations à droite du tableau.

Colonne	Signification
Informations détaillées sur l'erreur (affichées à droite du tableau)	<p>Le système affiche le nom de la forêt NetBIOS et le nom du groupe qu'il n'a pas pu synchroniser. Les raisons typiques pour lesquelles le système ne peut pas synchroniser ces utilisateurs et groupes sont les suivantes :</p> <ul style="list-style-type: none"> • Problème : la forêt contenant les groupes et les utilisateurs n'ont pas de domaine correspondant configurés dans centre de gestion. • Solution : ajoutez un domaine pour la forêt qui contient le groupe , comme indiqué dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine, à la page 10. • Problème : vous avez exclu des groupes du téléchargement vers centre de gestion. • Solution : cliquez sur la page à onglets Domaines, cliquez sur Edit (✎), puis déplacez le groupe ou l'utilisateur indiqué de la liste Groupes et utilisateurs exclus.

Essayez de télécharger à nouveau les utilisateurs et les groupes.

S'il est possible que les problèmes soient temporaires, téléchargez les utilisateurs et les groupes pour tous les domaines.

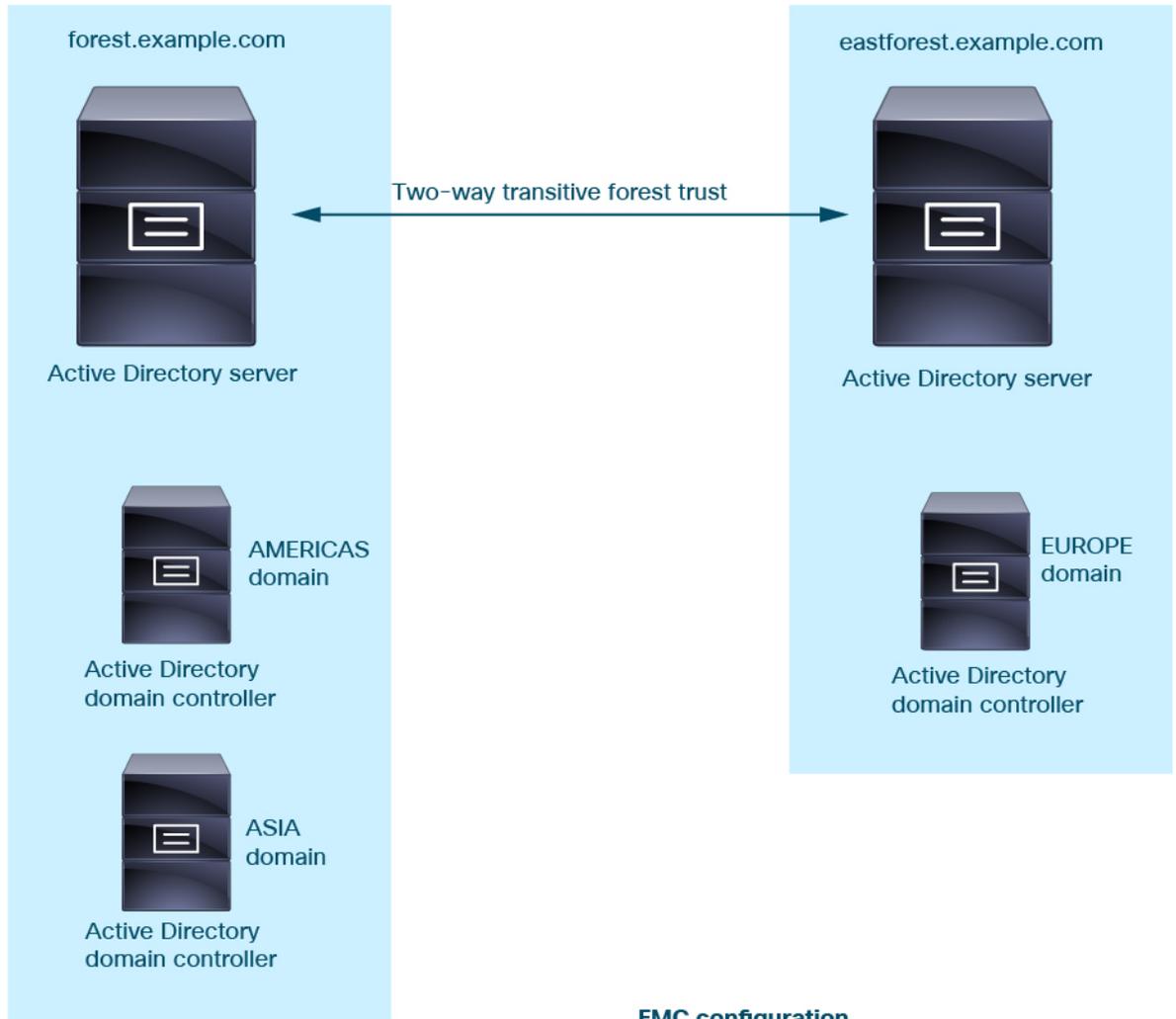
1. Connectez-vous au centre de gestion si vous ne l'avez pas encore fait.
2. Cliquez sur **Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines)**.
3. Cliquez sur **Télécharger** (↓).
4. Cliquez sur la page à onglet des **résultats de la synchronisation**.
5. Si aucun indicateur ne s'affiche pour les entrées de la colonne Realms (Domaines), les problèmes sont résolus.

Ajouter un domaine pour toutes les forêts

Assurez-vous d'avoir configuré un :

- Domaine centre de gestion pour chaque forêt qui a des utilisateurs que vous souhaitez utiliser dans les politiques d'identité.
- Répertoire centre de gestion pour chaque contrôleur de domaine de cette forêt avec les utilisateurs que vous souhaitez utiliser dans les politiques d'identité.

La figure suivante présente un exemple.



FMC configuration



- Realm:** forest.example.com
- Directory:** AMERICAS.forest.example.com
- Directory:** ASIA.forest.example.com

- Realm:** eastforest.example.com
- Directory:** EUROPE.eastforest.example.com

Historique des domaines

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Séquences du serveur mandataire	N°importe lequel	7.2.0	<p>Similaire à une séquence de domaine, une séquence de mandataire est un ou plusieurs périphériques gérés qui peuvent communiquer avec Cisco Defense Orchestrator si Cisco Defense Orchestrator ne peut pas communiquer avec le serveur LDAP ou Active Directory.</p> <p>Écrans nouveaux ou modifiés : Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines) > Proxy Sequence (séquences de proxy)</p>
Approbation interdomaine pour les domaines Active Directory.	N°importe lequel	7.0.0	<p>Un groupe de domaines Microsoft Active Directory (AD) qui se font confiance est communément appelé une « forêt ». Cette relation d'approbation peut permettre aux domaines d'accéder aux ressources des uns et des autres de différentes manières. Par exemple, un compte d'utilisateur défini dans le domaine A peut être marqué comme membre d'un groupe défini dans le domaine B.</p> <p>Les centre de gestion peuvent obtenir des utilisateurs des forêts Active Directory pour les règles d'identité.</p>
Séquences de domaines.	N°importe lequel	6.7.0	<p>Une <i>séquence de domaine</i> est une liste ordonnée de deux domaines ou plus auxquelles appliquer des règles d'identité. Lorsque vous associez une séquence de domaine à une politique d'identité, le système Firepower recherche dans les domaines Active Directory dans l'ordre, du premier au dernier, comme spécifié dans la séquence de domaine.</p> <p>Écrans nouveaux ou modifiés : Integration (intégration) > Other Integrations (autres intégrations) > Realms (domaines) > Realm Sequences (séquences de domaines)</p>
Domaines pour le contrôle de l'utilisateur.	N°importe lequel	N°importe lequel	Un domaine est une connexion entre centre de gestion un référentiel d'utilisateurs Active Directory ou LDAP.

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.