Effectuer les configurations de système dans Cisco Secure Workload

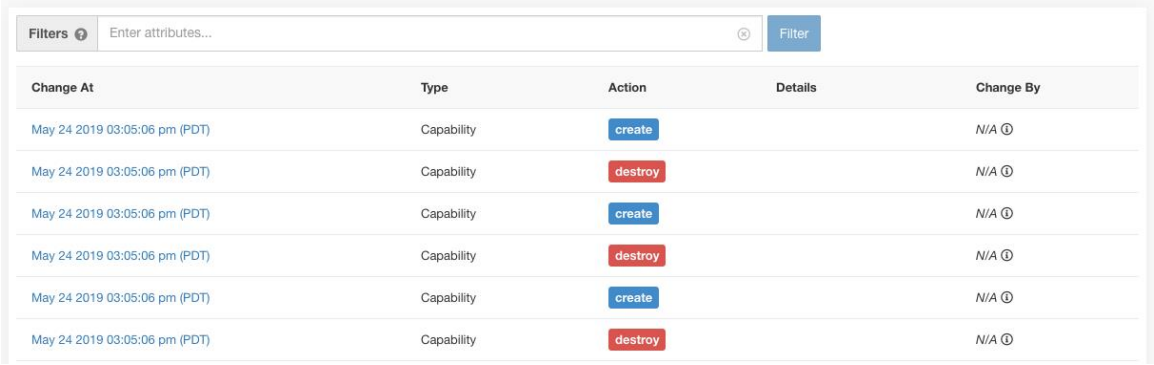
Les paramètres au niveau du système sont à votre disposition en fonction de votre rôle. Par exemple, seuls les utilisateurs ayant le rôle d' **administrateur de site** et de **service d'assistance à la clientèle** peuvent afficher l'option **Users** (Utilisateurs).

Journal des modifications

Les **administrateurs du site** peuvent accéder à la page **Change Log**(Journal des modifications) dans le menu **Manage** (Gérer) dans la barre de navigation à gauche de la fenêtre. Cette page affiche les modifications les plus récentes effectuées dans Cisco Cisco Secure Workload.

Note **Période de rétention des journaux des modifications** : Cisco Secure Workload gère les journaux des modifications pour une durée maximale d'un an sur les grappes de logiciels-services et sur site. Une tâche horaire supprime les journaux des modifications qui dépassent une période d'un an.

Figure 1: Page du journal des modifications

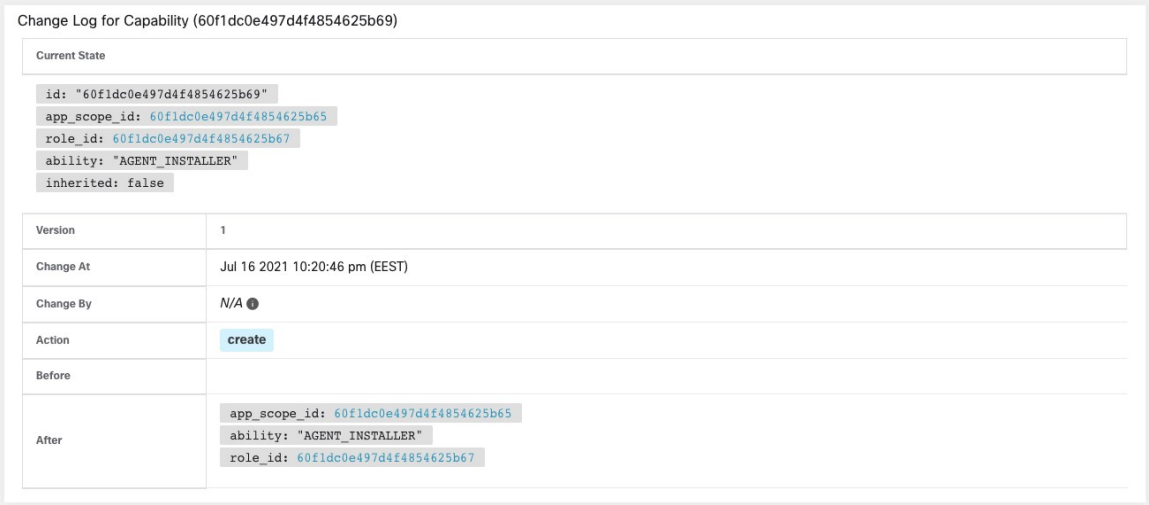


Pour consulter les détails de chaque entrée du journal des modifications, cliquez sur le lien dans la colonne **Change at** (Modifier à). Cette page comprend un instantané **avant** et **après** des champs modifiés. Les champs peuvent inclure des noms techniques qui nécessitent une certaine interprétation pour comprendre comment ils sont présentés ailleurs dans Cisco Secure Workload.

Figure 2: Page des détails du journal des modifications

La liste complète des modifications pour une entité peut être consultée en cliquant sur le bouton dans le coin supérieur droit, intitulé **Full log for this <entity type>** (Journal complet pour ce <type d'entité>). Cette page affiche les détails de chaque modification. Elle comprend également l' **état actuel** de l'entité, lorsqu'il est disponible.

Figure 3: Journal complet des modifications pour l'entité



Règles de collecte

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Collection Rules** (règles de collecte) dans le menu **Manage (Gestion) > Services Settings (Paramètres de service)** dans la barre de navigation à gauche de la fenêtre. Cette page affiche les règles de collecte matérielles par VRF qui sont utilisées par les commutateurs exécutant l'agent Cisco Cisco Secure Workload. Il y a une ligne dans le tableau pour chaque VRF.

Règles

Cliquez sur le bouton **Edit** (modifier) d'un VRF pour modifier ses règles de collecte. Par défaut, chaque VRF est configuré avec deux règles collecteurs par défaut, une pour IPv4 `(0.0.0.0/0 INCLUDE)` et une pour IPv6 `(::/0 INCLUDE)`. *Ces règles par défaut peuvent être supprimées, mais procédez avec prudence.*

Des règles d'inclusion et d'exclusion supplémentaires peuvent être ajoutées. Saisissez un sous-réseau valide, sélectionnez inclure ou exclure, puis cliquez sur **Add Rule** (Ajouter une règle). La priorité de ces règles peut être ajustée par glisser-déposer. Cliquez et maintenez une règle dans la liste et faites-la glisser pour ajuster l'ordre.

Plusieurs minutes peuvent être nécessaires pour que les modifications se propagent à vos commutateurs. Cliquez sur le bouton **Back** (Précédent) dans le coin supérieur droit pour revenir à la liste des fichiers VRF.

Priorité

Les règles de collecte sont classées par ordre de priorité décroissant. Aucune correspondance du préfixe le plus long n'est effectuée pour déterminer la priorité. La règle apparaissant en premier a une priorité plus élevée sur toutes les règles suivantes. Exemple :

1. 1.1.0.0/16 INCLUDE
2. 1.0.0.0/8 EXCLUDE

3. 0.0.0.0/0 INCLUDE

Dans l'exemple précédent, toutes les adresses appartenant au sous-réseau 1.0.0.0/8 sont exclues, sauf le sous-réseau 1.1.0.0/16 qui est inclus.

Autre exemple avec ordre modifié :

1. 1.0.0.0/8 EXCLUDE
2. 1.1.0.0/16 INCLUDE
3. 0.0.0.0/0 INCLUDE

Dans l'exemple ci-dessus, toutes les adresses appartenant au sous-réseau 1.0.0.0/8 sont exclues. La règle numéro 2 n'est pas appliquée ici, en raison d'une règle d'ordre supérieur déjà définie pour son sous-réseau.

Collecteurs

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Collectors** (Collecteurs) dans le menu **Platform** (Plateforme) dans la barre de navigation à gauche de la fenêtre. Cette page affiche les collecteurs actuellement configurés. Les agents Cisco Secure Workload envoient des données de flux aux collecteurs mis en service. Il est donc important que tous les collecteurs mis en service soient disponibles. Par défaut, l'intégrité de tous les collecteurs fait l'objet d'une vérification périodique et ils sont mis en service ou désactivés en fonction de leur intégrité. Vous pouvez vous désinscrire de ce processus automatisé en utilisant le bouton **Auto Commission Opt Out** (pour la désactivation automatique de la commission). Lorsque cette bascule est activée, les icônes **Play** (Lecture) et **Stop** (Arrêt) sous la colonne la plus à droite peuvent être utilisées pour la mise en service et la désactivation respectivement.

Figure 4: Page Collectors (Collecteurs)

Configuration de session

Le délai d'expiration de la session d'inactivité de l'authentification de l'utilisateur de l'interface utilisateur peut être configuré ici. Cette configuration s'applique à tous les utilisateurs de l'appareil. La durée par défaut d'une session inactive est de 1 heure. La durée d'une session d'inactivité peut être définie entre 5 minutes et 24 heures. Le délai d'expiration de session prend effet sur la session authentifiée d'un utilisateur lorsque cette valeur est enregistrée.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à ce paramètre. Dans le volet de navigation de gauche, cliquez sur **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Session Configuration (Configuration de la session)**.

Société

Vous pouvez définir les configurations suivantes à l'échelle de l'entreprise (par grappe Cisco Secure Workload.

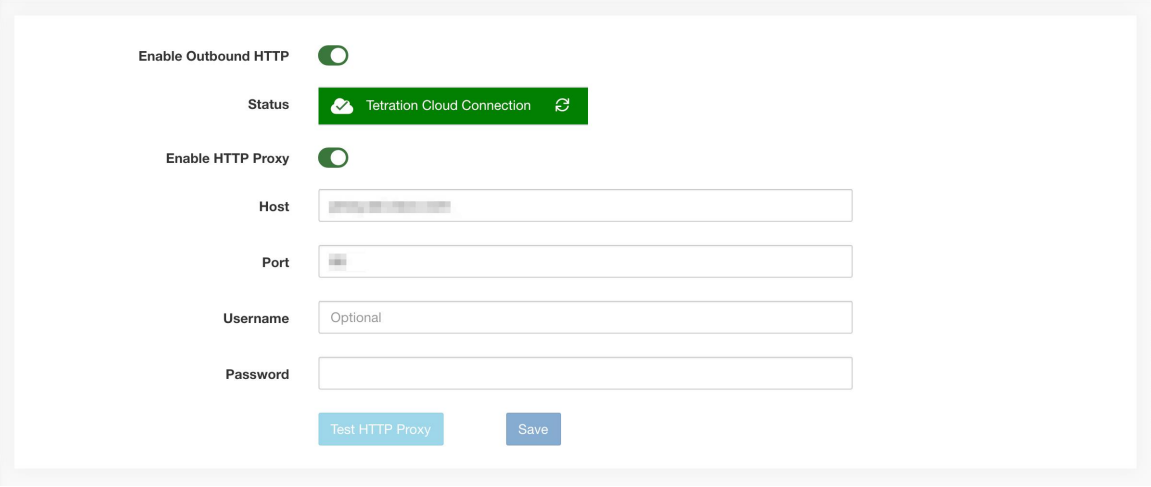
Connexion HTTP sortante

Pour vous assurer que les derniers ensembles de données d'informations sur les menaces sont récupérés à partir de Cisco Cloud, nous vous recommandons fortement de configurer une connexion HTTP sortante.

Warning Votre demande HTTP sortante d'entreprise peut nécessiter d'autoriser le trafic vers **periscope.tetrationcloud.com** et **uas.tetrationcloud.com** dans les règles de sortie du pare-feu d'entreprise en plus de configurer le serveur mandataire HTTP comme indiqué ci-dessous.

La connexion TLS à **periscope.tetrationcloud.com** est utilisée pour transporter des données d'informations sur les menaces afin d'identifier les vulnérabilités connues. Par conséquent, il est essentiel que Cisco Cisco Secure Workload vérifie l'authenticité du nom de domaine en comparant le certificat de l'autorité de certification x.509 du domaine par rapport aux certificats d'autorité de certification racine réputés inclus avec Cisco Secure Workload. L'altération de la chaîne de confiance X.509 empêche la fonctionnalité de fonctionner correctement.

Figure 5: Connexion HTTP sortante



Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder aux paramètres HTTP sortants. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **Outbound HTTP (HTTP sortant)**.

Champ	Description
État	Indique si l'appareil Cisco Secure Workload peut accéder à Cisco Secure Workload infonuagique pour récupérer les mises à jour de l'ensemble de données des menaces. La vérification de l'état peut être redéclenchée en cliquant sur le bouton d'actualisation. Les paramètres de serveur mandataire HTTP suivants peuvent être utilisés pour configurer les paramètres de serveur mandataire HTTP en fonction de votre déploiement Cisco Secure Workload.

Champ	Description
Activer le serveur mandataire HTTP	Toutes les connexions HTTP externes utilisent un serveur mandataire HTTP si cette option est activée
Hébergement	Adresse de l'hôte du serveur mandataire HTTP
Port	Numéro de port du serveur mandataire HTTP
Nom d'utilisateur	Nécessaire uniquement si votre serveur mandataire HTTP utilise l'authentification de base
mot de passe	Nécessaire uniquement si votre serveur mandataire HTTP utilise l'authentification de base

Message de page de connexion

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent saisir un message de 1 600 caractères maximum que les utilisateurs peuvent voir sur la page de connexion.

Pour créer ou modifier le message de la page de connexion :

1. Dans la page de navigation de gauche, cliquez sur **Platform (Plateforme)** > **Login Page Message (Message de la page de connexion).**
2. Saisissez ou modifiez le message. La limite de caractères est inférieure ou égale à 1 600 caractères.
3. Cliquez sur **Save** (enregistrer).

Configurer l'authentification externe

Si cette option est activée, l'authentification peut être transférée à un système externe. Les options actuelles d'authentification sont le protocole LDAP (Lightweight Directory Access Protocol) et la connexion unique (Single Sign-On ou SSO). Cela signifie qu'une fois activé, tous les utilisateurs qui se connectent utiliseront le mécanisme choisi pour s'authentifier. Il est important d'établir que la connexion LDAP est configurée correctement, en particulier si aucun utilisateur ne recourt à l'Option « Use Local Authentication » (Utiliser l'authentification locale). L'approche recommandée est d'avoir au moins un utilisateur authentifié localement avec des informations d'authentification **Site Admin** (administrateur de site) en activant l'Option « Use Local Authentication » (Utiliser l'authentification locale). Cet utilisateur peut s'assurer que la configuration LDAP est configurée correctement. Une fois la connexion configurée, cet utilisateur peut également être transféré vers l'authentification externe en décochant l'option « Use Local Authentication » (Utiliser l'authentification locale) dans le flux de modification de l'utilisateur.

L'administrateur du site peut activer davantage de messages de débogage, ce qui est utile pour déboguer les problèmes de connexion externe, les échecs de connexion de l'utilisateur, etc. Ils peuvent être activés en cochant l'option « External Auth Debug » (Débogage de l'authentification externe). Une fois cette option activée, des messages de journalisation plus descriptifs sont écrits dans un fichier journal distinct intitulé « external_auth_debug.log » (journal_auth_debog_externe). Il est recommandé de désactiver le « débogage d'authentification externe » une fois le débogage terminé pour éviter que des journaux supplémentaires ne soient écrits dans le fichier journal.

Note Une fois l'authentification externe activée, les utilisateurs peuvent la contourner pour un utilisateur spécifique, comme indiqué dans l'Option « Use Local Authentication » (Utiliser l'authentification locale). Cette option peut également être activée en accédant au flux de modification de l'utilisateur à partir du lien grâce au message d'avertissement lorsque l'authentification externe est également activée.

L'authentification externe à l'aide de SSO est l'approche d'authentification recommandée si la Fédération est activée.

Note À partir de la version 3.7. et ultérieures, la durée d'éviction d'une session d'authentification externe passe de six à neuf heures. Ce paramètre est applicable pour l'authentification externe ou sur site uniquement.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent configurer l'authentification externe. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **External Authentication (Authentification externe)**.

Figure 6: Configuration de l'authentification externe

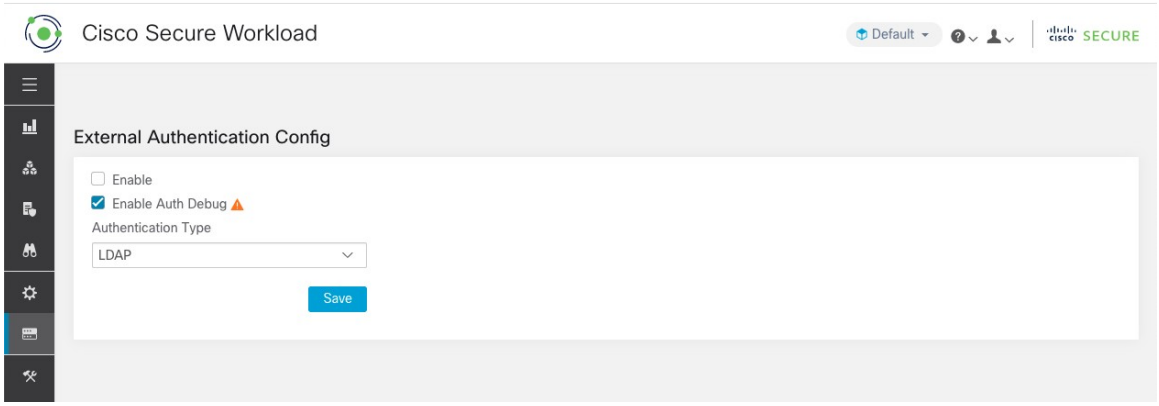


Figure 7: Configuration de l'authentification externe (Suite)

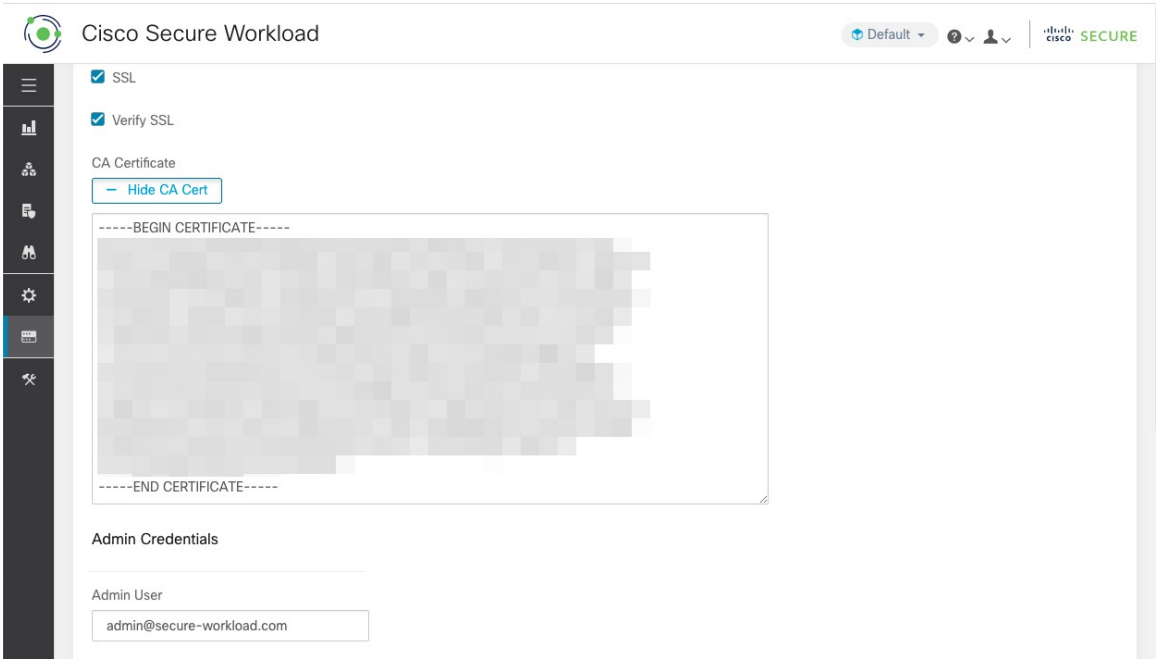


Figure 8: Configuration de l'authentification externe (Suite)

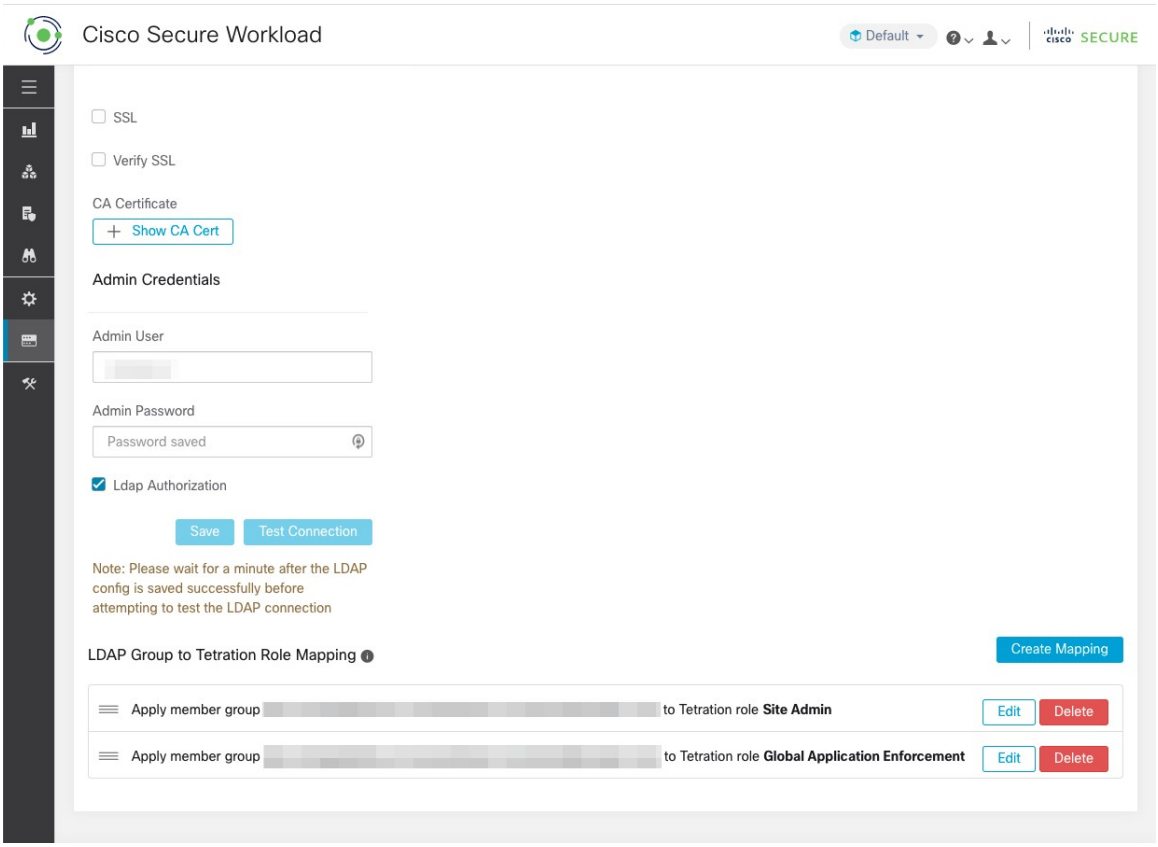
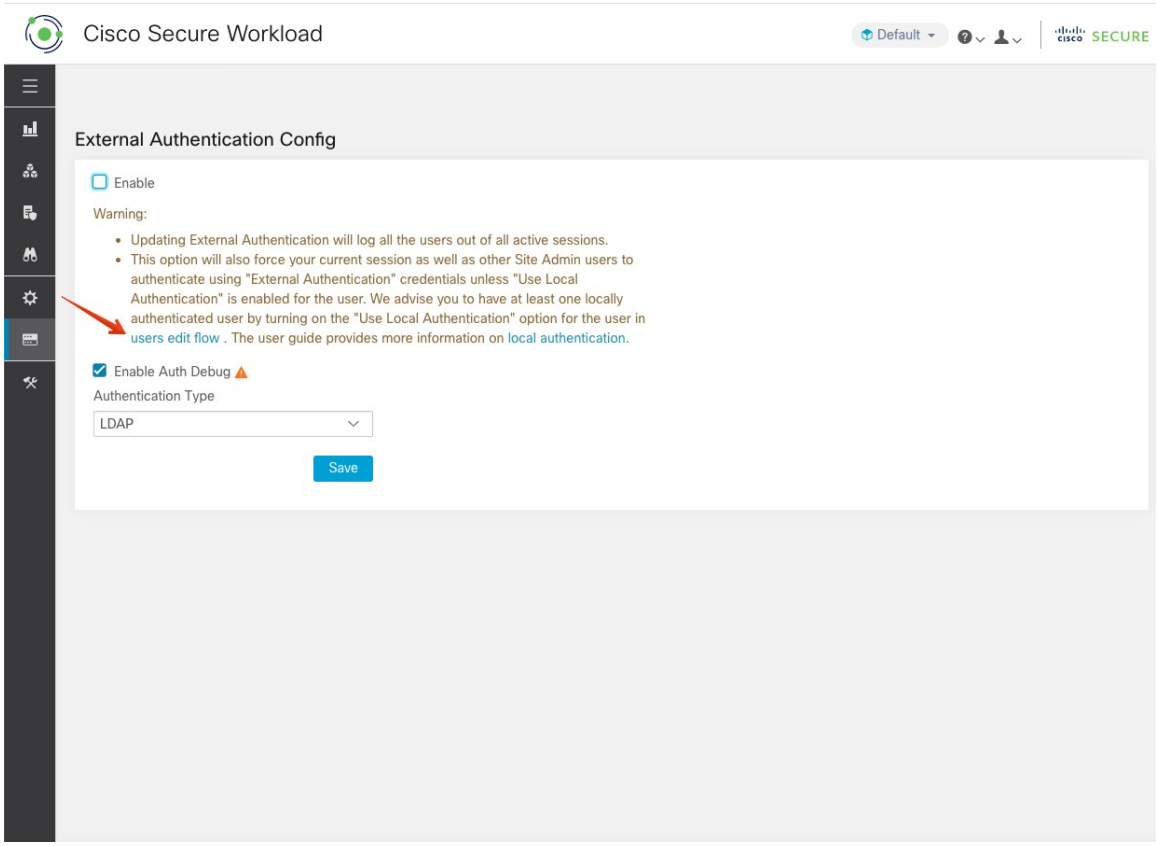


Figure 9: Avertissement relatif à l'authentification externe



Configuration du protocole LDAP (Lightweight Directory Access Protocol)

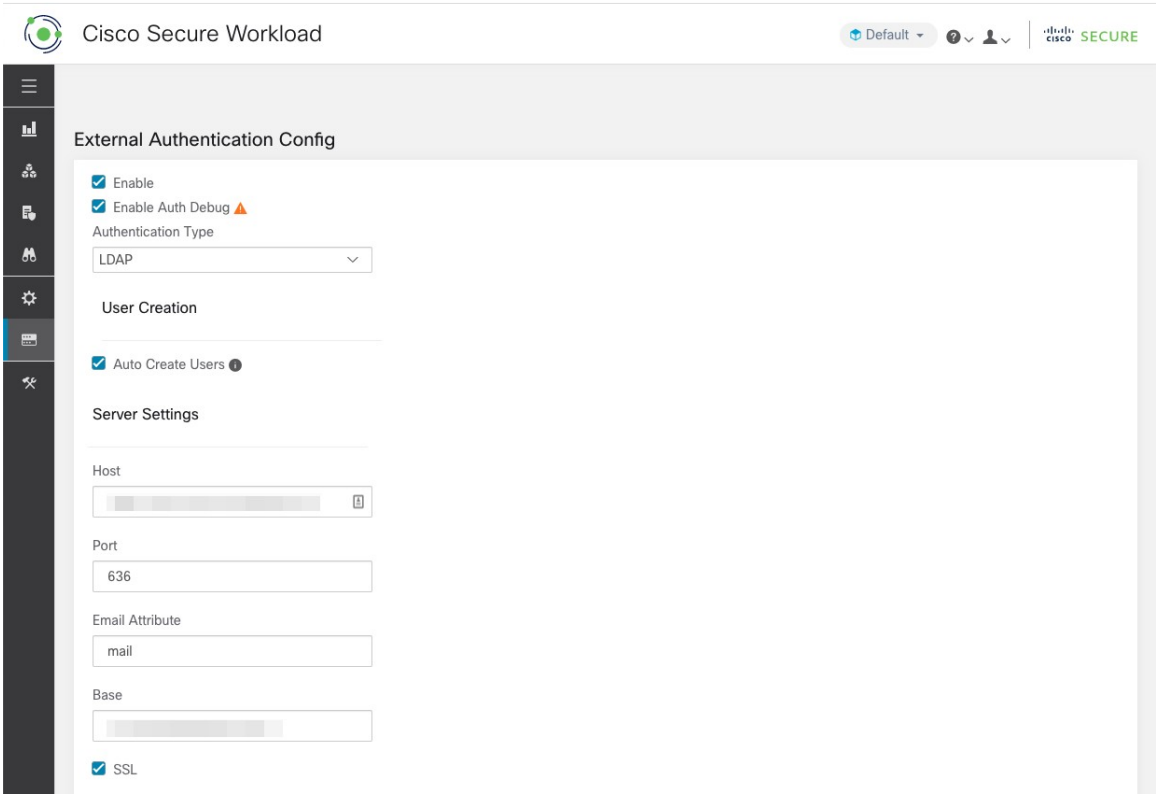
Choisissez l'option LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs. Cela signifie qu'une fois activée, tous les utilisateurs seront déconnectés et que les connexions ultérieures utiliseront leur adresse courriel et leur mot de passe LDAP pour s'authentifier.

LDAP n'est actuellement pas recommandé comme mécanisme d'authentification si la « Fédération » est activée.

Si LDAP est activé, le flux de travail recommandé pour la création de nouveaux utilisateurs est le suivant.

Les **administrateurs de site** sont invités à créer d'abord de nouveaux utilisateurs avec leurs courriels et à attribuer les rôles appropriés en Configurer l'autorisation LDAP (autorisation AD) avant que les nouveaux utilisateurs ne se connectent pour la première fois au moyen de LDAP. Si un nouvel utilisateur se connecte via LDAP sans jouer le rôle approprié, aucun rôle par défaut n'est attribué à l'utilisateur.

Figure 10: Configuration du protocole LDAP (Lightweight Directory Access Protocol)



Champ	Description
Créer des utilisateurs automatiquement	Si vous activez la création automatique des utilisateurs, des utilisateurs seront créés s'ils n'existent pas lors de la première connexion. Cela évite aux administrateurs du site d'avoir à mettre à disposition les utilisateurs avant de leur permettre de se connecter. Cette option doit être désactivée si l'accès Cisco Secure Workload est limité aux utilisateurs créés manuellement dans la page Utilisateurs.
Hébergement	Hôte LDAP qui sera utilisé pour l'authentification
Port	Port LDAP qui sera utilisé pour l'authentification.
Attribut du courriel	Nom d'attribut LDAP qui représente le courriel de l'organisation.
Base	Nom de domaine de base LDAP à partir duquel les utilisateurs seront recherchés.
SSL	Activez le chiffrement et utilisez « ldaps:// ».
Vérification SSL	Vérifier les attributs SSL du serveur tels que le nom de domaine complet (FQDN) en fonction du certificat du serveur.
Autorité de certification SSL Cert	Certificat de signature pour le certificat SSL du serveur LDAP Obligatoire si la chaîne de certificats du serveur ne peut pas être vérifiée publiquement.

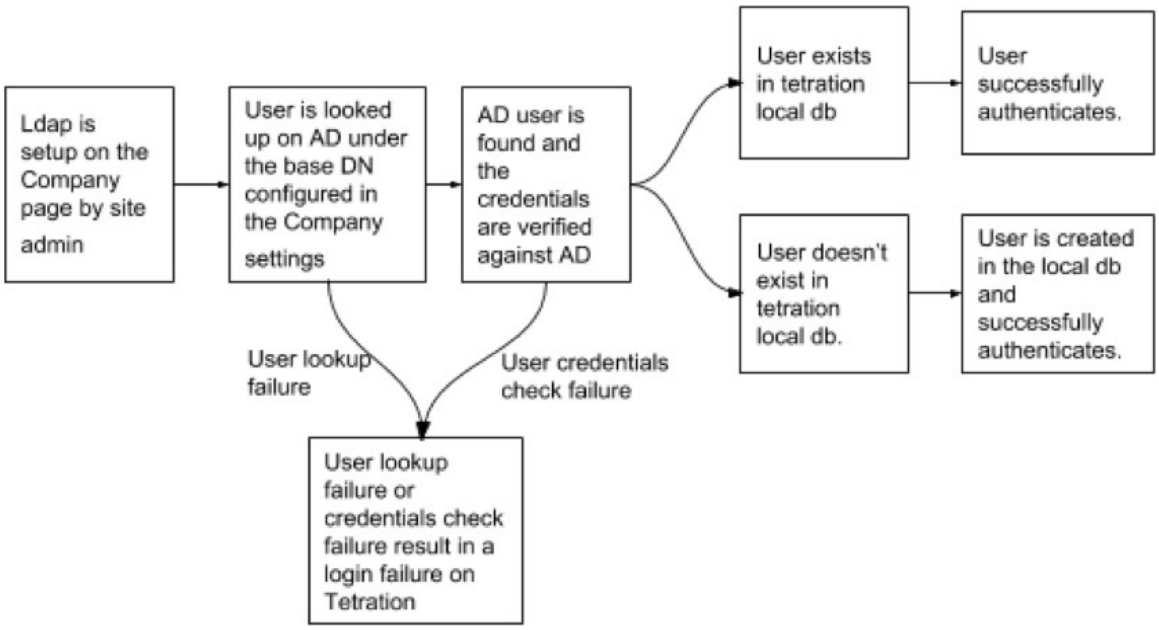
Champ	Description
Utilisateurs admin	Nom d'utilisateur admin LDAP (et non d'utilisateur Cisco Secure Workload) utilisé pour la liaison avec le serveur LDAP. Par exemple : [Utilisateur]@[Domaine] ou [Domaine]\\[Utilisateur]
Mot de passe de l'administrateur	Mot de passe d'administrateur LDAP utilisé pour la liaison avec le serveur LDAP.
Autorisation LDAP	L'autorisation LDAP peut être activée et configurée, comme expliqué dans Configurer l'autorisation LDAP (autorisation AD)

Une fois la configuration LDAP activée, tous les utilisateurs, à l'exception des utilisateurs avec l'Option « Use Local Authentication » (Utiliser l'authentification locale) activée, seront déconnectés de leurs sessions.

La configuration LDAP peut être enregistrée après avoir cliqué sur le bouton **« Save »** (Enregistrer). Nous vous recommandons d'attenter une minute après l'enregistrement de la configuration LDAP avant de tenter de tester la connexion LDAP.

La connexion LDAP peut être testée après l'enregistrement de la configuration LDAP à l'aide du bouton **« Test Connection (Tester la connexion) »**. Cela tente une liaison avec le serveur LDAP avec les informations d'authentification d'administrateur saisies.

Figure 11: Flux de travail de l'authentification



Résoudre les problèmes LDAP

Si une erreur se produit lorsque vous testez la connexion LDAP, vérifiez les éléments suivants :

- Vérifiez si les informations d'authentification de l'administrateur LDAP sont correctes.
- Vérifiez les paramètres de connexion tels que l'hôte, le port, SSL, etc.
- Vérifiez si le serveur LDAP est accessible à partir des VIP de l'interface utilisateur Cisco Secure Workload.

- Vérifiez si le serveur AD est opérationnel.
- Utilisez les outils de ligne de commande tels que **« ldapsearch »** avec les renseignements de connexion pour vérifier si une liaison peut être établie.

Si une erreur se produit lors de la connexion d'un utilisateur, vérifiez les éléments suivants :

- Vérifiez si l'utilisateur peut se connecter avec ses renseignements d'authentification LDAP à d'autres sites Web de l'entreprise qui utilisent l'authentification LDAP.
- Vérifiez si le DN de base spécifié dans les paramètres LDAP de l'entreprise est correct. Cela peut être fait en utilisant des outils de ligne de commande tels que **« ldapsearch »** pour rechercher l'utilisateur dans le DN de base.

Exemple de requête **« ldapsearch »** pour rechercher un utilisateur par son adresse courriel :

```
ldapsearch -H "ldap://<host>:<port>" -b "<base-dn>" -D "<ldap-admin-user>" -w
<ldap->admin-password> "(mail=<users-email-address>)"
```

Configurer l'autorisation LDAP (autorisation AD)

L'autorisation Active Directory peut être configurée en cochant la case « LDAP Authorization » (Autorisation LDAP) dans la section « Admin Credentials » (Renseignements d'authentification d'administrateur) de la configuration LDAP d'authentification externe. Une fois ce paramètre activé, l'administrateur du site doit configurer les mappages des groupes « MemberOf » (Membre de) LDAP avec les rôles Cisco Secure Workload dans la section ci-dessous. Par défaut, sans cette configuration, les utilisateurs d'Active Directory doivent être préconfigurés avec un ou plusieurs rôles Cisco Secure Workload avant une tentative de connexion.

Le mappage du groupe LDAP MemberOf vers Cisco Secure Workload doit être configuré si l'authentification externe LDAP est activée. L'option « Create Mapping » (créer un mappage) permet de configurer le mappage d'une valeur de groupe LDAP MemberOf à un rôle Cisco Secure Workload. Les rôles dans la liste déroulante des rôles sont préremplis en fonction de la portée sélectionnée dans le sélecteur de portée. Une fois que ces mappages sont enregistrés, tous les utilisateurs sont autorisés en fonction de ces valeurs lors de leur connexion ultérieure.

Ces mappages peuvent être réorganiser, modifiés ou supprimés. Toute modification des mappages sera reflétée dans les rôles attribués aux utilisateurs lors de leurs connexions ultérieures. Un maximum de 50 mises en correspondance de rôles LDAP MemberOf avec Cisco Secure Workload peut être créé.

Les noms de groupe MemberOf LDAP en double ne sont pas autorisés. Cependant, plusieurs groupes LDAP MemberOf peuvent être mappés au même rôle. Si plusieurs groupes sont mappés au même rôle, le dernier mappage sera stocké dans l'utilisateur en tant que MemberOf LDAP correspondant au rôle Cisco Secure Workload.

Figure 12: Configuration du groupe LDAP vers le rôle Cisco Secure Workload

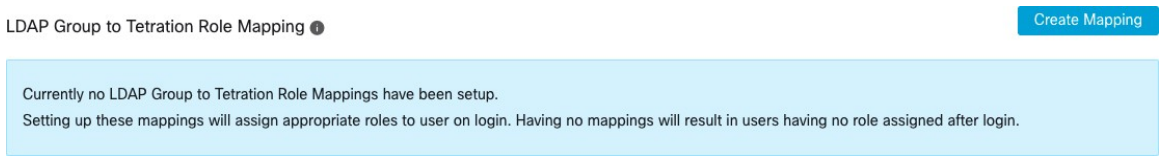
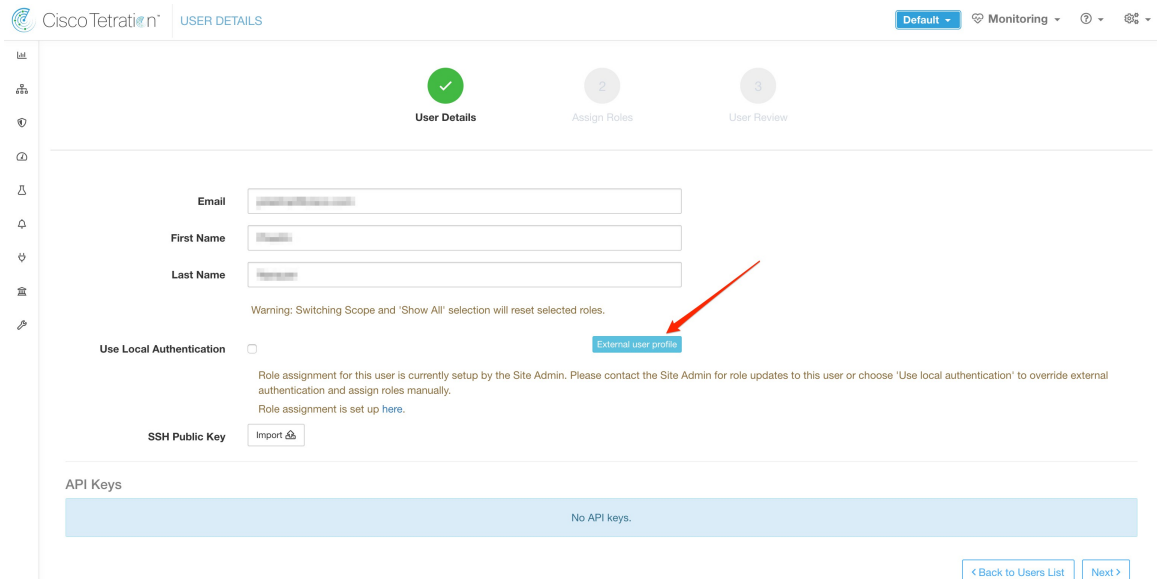


Figure 13: Mappage du groupe LDAP au rôle Cisco Secure Workload

Un utilisateur administrateur de site peut rapprocher l'attribution des rôles sur la base du mappage des rôles ci-dessus à l'aide des informations de l'utilisateur externe obtenues lors de la dernière connexion réussie de ce dernier.

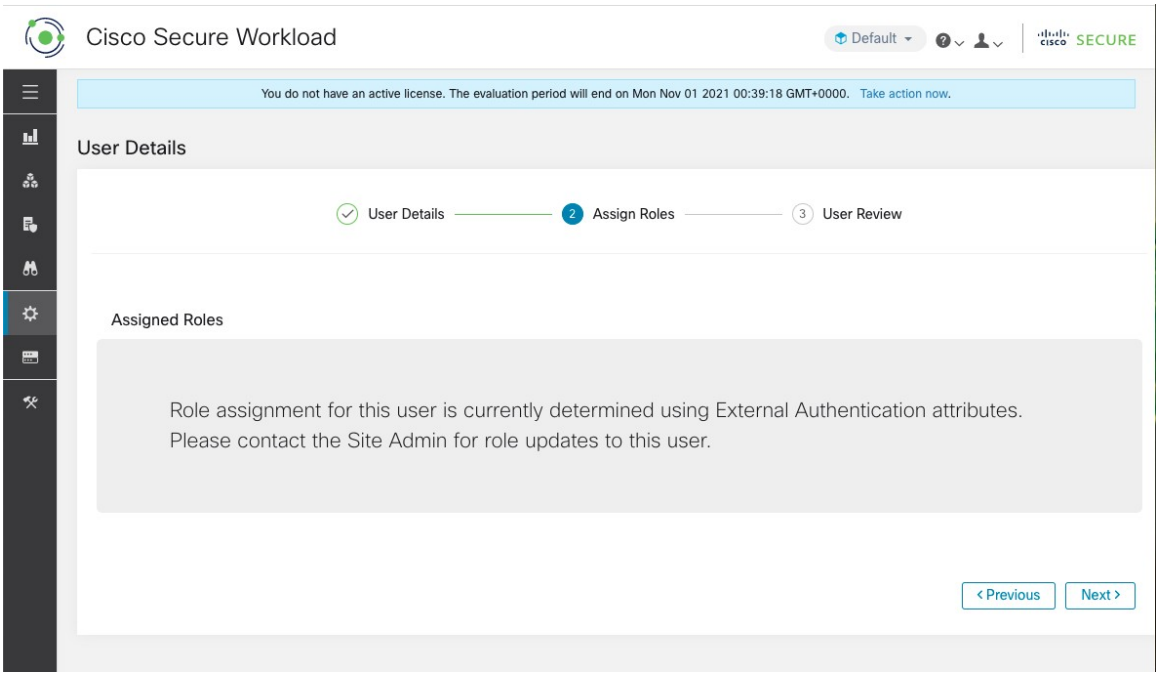
Note Une fois l'authentification externe activée, les utilisateurs peuvent la contourner pour un utilisateur spécifique, comme indiqué dans l'Option « Use Local Authentication » (Utiliser l'authentification locale). Ces utilisateurs contourneront également le processus d'autorisation configuré pour l'autorisation AD.

Figure 14: Renseignements sur l'utilisateur externe



Une fois l'autorisation activée, la sélection manuelle du rôle Cisco Secure Workload dans les flux de création d'utilisateurs (Ajouter un utilisateur, on page 62) et de modification d'utilisateurs (Modifier les détails ou le rôle d'un utilisateur) est **interdite**.

Figure 15: Page Utilisateurs



Les groupes MemberOf LDAP mappés aux rôles Cisco Secure Workload sont visibles sur la page de profil d'utilisateur.

Figure 16: Page Profil d'utilisateur

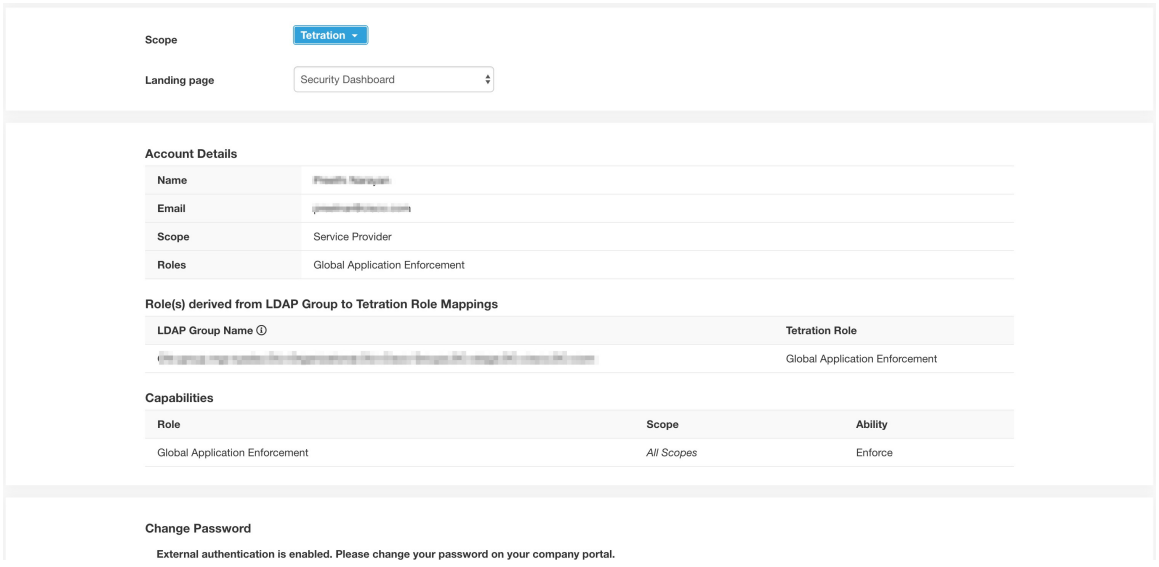
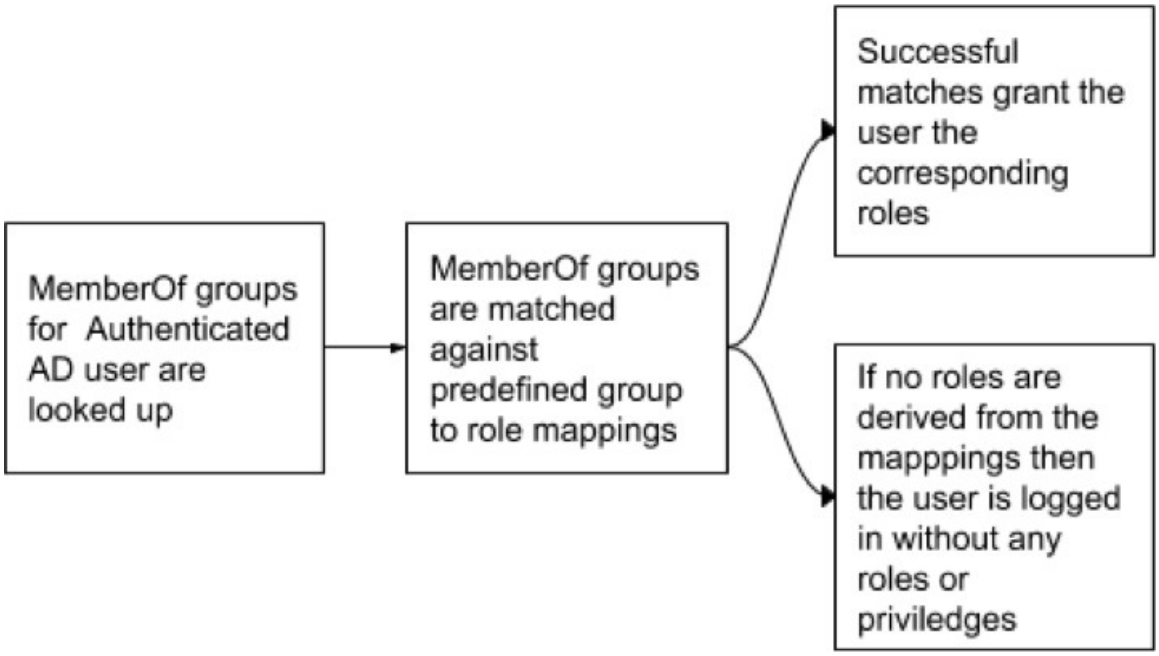


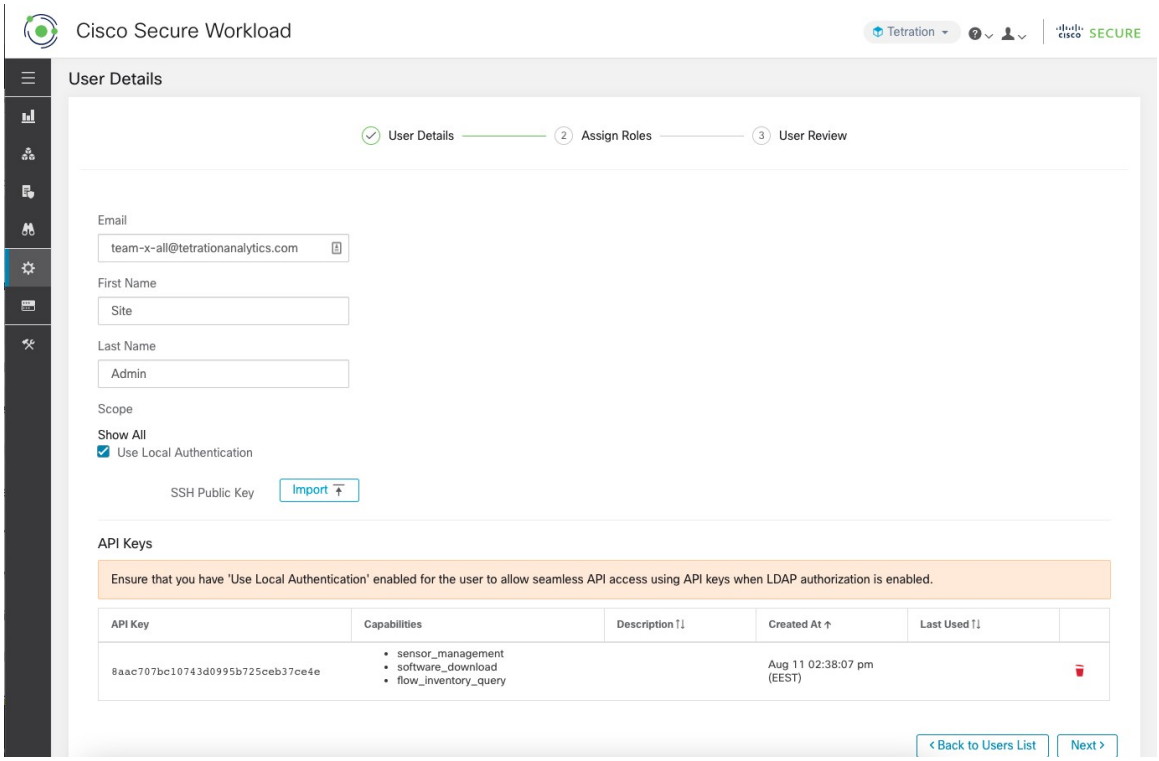
Figure 17: Flux de travail d'autorisation



Si l'autorisation LDAP est activée, l'accès à l'OpenAPI via les clés API ne fonctionne plus de manière transparente, car les rôles Cisco Secure Workload découlant des groupes LDAP MemberOf sont réévalués une fois la session de l'utilisateur terminée. Par conséquent, pour assurer un accès OpenAPI ininterrompu, nous recommandons aux utilisateurs dotés de clés API d'activer l'Option « Use Local Authentication » (Utiliser l'authentification locale).

Figure 18: Avertissement lié à la clé API d'autorisation LDAP

Figure 19: Avertissement lié à la clé API d'autorisation LDAP sur la page Users (Utilisateurs)



Dépannage des problèmes d'autorisation LDAP

Si les rôles ne sont pas attribués aux utilisateurs en fonction des mappages définis dans la section « Mappages du groupe LDAP aux rôles », vérifiez de nouveau la configuration et le format des mappages de rôles.

- La chaîne de groupe doit être au format de chaîne . Par exemple : CN=group.jacpang,OU=Organizational,OU=Cisco Groups,DC=stage,DC=cisco,DC=com
- Les noms des groupes doivent être identiques à ceux qui figurent dans AD, sans espaces ni caractères supplémentaires.
- Le mappage de rôles pour le groupe doit être sélectionné à partir du sélecteur de rôles.

Étapes de débogage du mappage des rôles d'utilisateur

- Vous devez avoir deux utilisateurs, dont l'un est l'administrateur du site. Le courriel de cet utilisateur ne doit pas être la même que celui de l'utilisateur AD.
- Cet utilisateur est appelé « utilisateur SA » pour les étapes ci-dessous.
  - L'utilisateur SA a déjà configuré les configurations de mappage de rôles sur la configuration d'authentification externe de la page de l'entreprise, comme décrit précédemment. Supposons qu'un « utilisateur SA » se connecte avec le courriel [site-admin]@[domaine].
  - Nous supposons que l'« utilisateur AD » est [ad-admin] @ [domaine]. Nous supposons que la configuration LDAP est terminée et que l'utilisateur AD est en mesure de se connecter, mais n'obtient pas le rôle qui lui est attribué.

- En tant qu'utilisateur AD, connectez-vous en utilisant une session de navigateur de navigation privée. Cela sépare l'état du navigateur de la session d'utilisateur SA.
- En tant qu'utilisateur SA, connectez-vous et accédez à la page Users (utilisateurs).
- Cliquez sur l'icône Edit (modifier) pour l'utilisateur AD pour lequel le mappage des rôles doit être configuré.
- Cliquez sur le bouton « External User Profile » (profil d'utilisateur externe) sur la page User Profile (Profil de l'utilisateur).
- Vous verrez un tableau de profils d'authentification externe qui comprend une section « memberof » (membre de).
- Il s'agit de l'une des valeurs « memberof » que vous pouvez utiliser pour le mappage des rôles sur la page de l'entreprise, la configuration d'authentification externe, du groupe LDAP à la section de mappage des rôles.
- Vous devez fournir la chaîne par ligne complète « memberof » pour établir la correspondance. Une fois que vous avez créé ce mappage de rôles, toute personne ayant le même attribut « memberof » se verra attribuer le rôle mappé.
- Pour que l'utilisateur AD reçoive le nouveau rôle mappé, l'utilisateur doit se déconnecter, puis se reconnecter pour permettre la réévaluation de ce profil de mappage.
- Une fois qu'un utilisateur se connecte et que des rôles sont attribués avec succès à la suite des mappages de rôles de groupe, les règles de correspondance sont visibles sur la page « Preferences » (Preferences) de cet utilisateur.

Configurer la connexion unique (SSO)

Si cette option est sélectionnée, la connexion unique (SSO) peut être utilisée pour authentifier les utilisateurs. Cela signifie que lorsque cette option est activée, tous les utilisateurs sont redirigés vers la page de connexion du fournisseur d'identité pour s'authentifier. Les utilisateurs dont l'Option « Use Local Authentication » (Utiliser l'authentification locale) est activée peuvent utiliser le courriel et le mot de passe de connexion de la page de connexion pour s'authentifier.

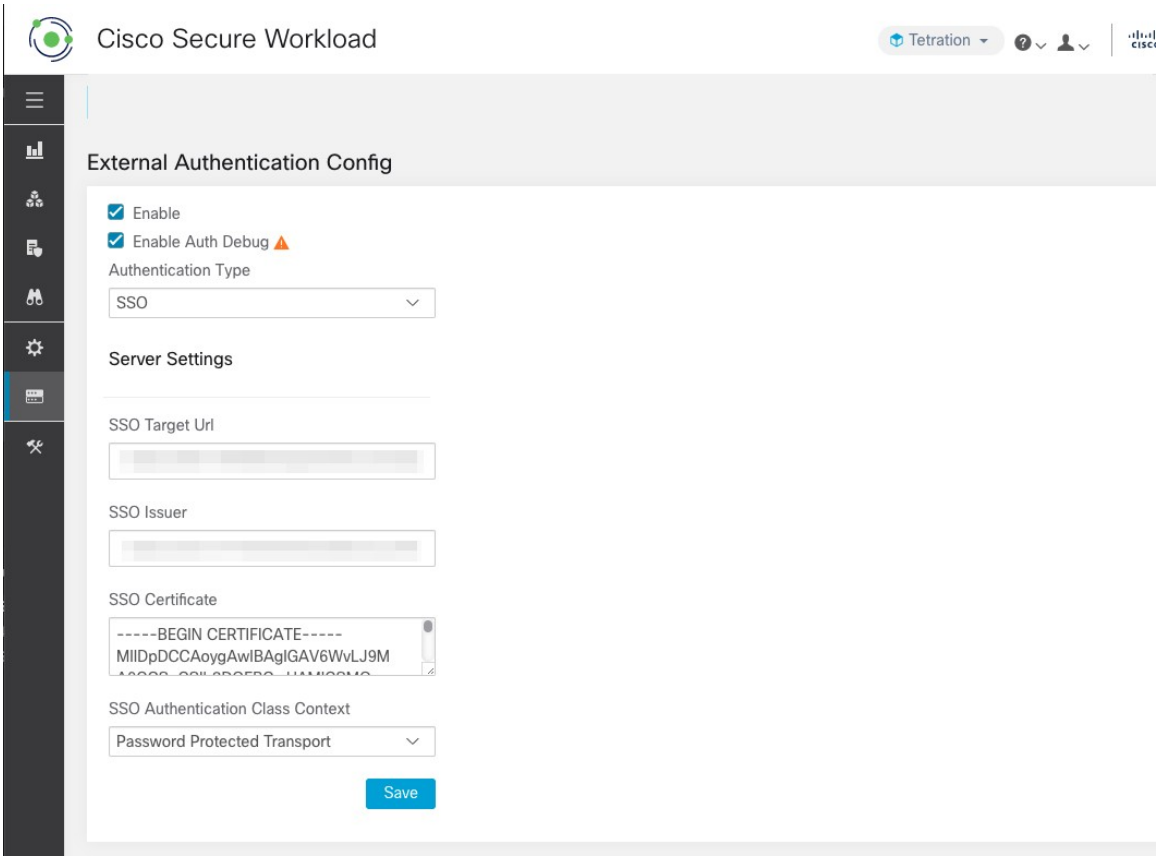
Il est important d'établir que la configuration SSO est configurée correctement, en particulier si aucun utilisateur n'utilise l'option Option « Use Local Authentication » (Utiliser l'authentification locale). L'approche recommandée est d'avoir au moins un utilisateur authentifié localement avec des informations d'authentification **Site Admin** (administrateur de site) en activant l'Option « Use Local Authentication » (Utiliser l'authentification locale). Cet utilisateur peut s'assurer que la configuration SSO est mise en place correctement. Une fois la connexion configurée avec succès, cet utilisateur peut également être transféré vers l'authentification externe en décochant l'option « Use Local Authentication » dans le flux de modification de l'utilisateur.

Si SSO est activée, le flux de travail recommandé pour la création de nouveaux utilisateurs est le suivant.

Les **administrateurs du site** et les **propriétaires de portée** sont invités à créer d'abord de nouveaux utilisateurs avec leurs adresses de courriel et à attribuer les rôles et les portées appropriés avant que le nouvel utilisateur ne se connecte pour la première fois via SSO. Si un nouvel utilisateur se connecte via SSO sans jouer le rôle approprié, aucun rôle par défaut n'est attribué à l'utilisateur.

Le tableau suivant décrit les champs qui doivent être définis pour configurer SSO sur Cisco Secure Workload. Cisco Secure Workload est le fournisseur de services (FS) dans ce cas.

Figure 20: Configuration de la connexion unique

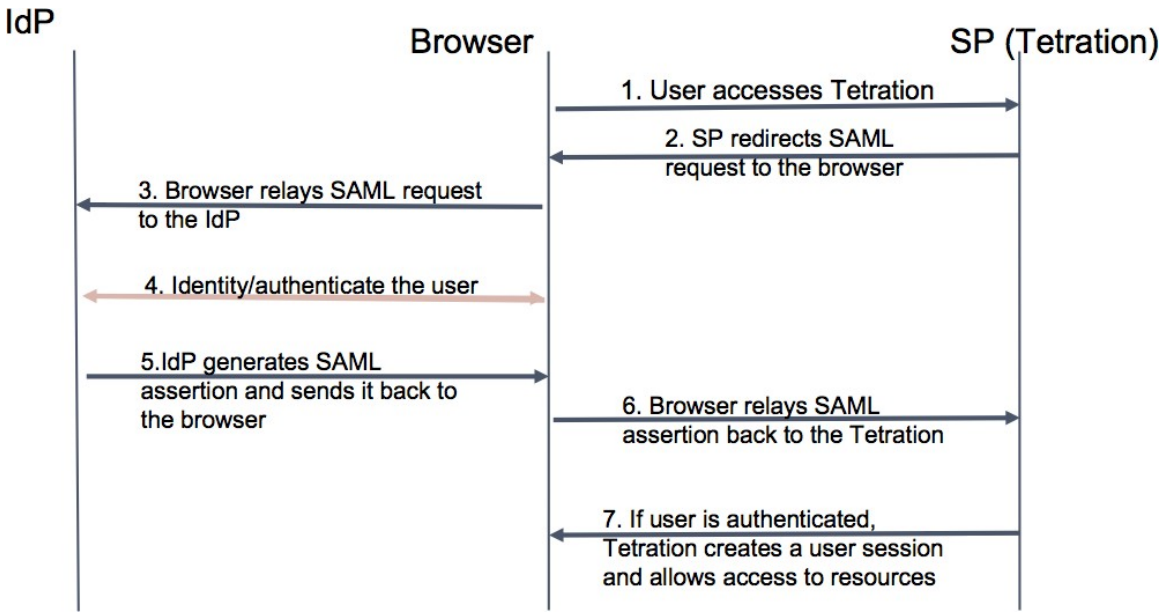


Champ	Description
URL SSO cible	URL cible du fournisseur d'identité SSO vers laquelle les utilisateurs seront redirigés pour la connexion.
Émetteur SSO	ID d'entité SSO de votre fournisseur de services, une URL qui identifie de manière unique votre fournisseur de services. Il s'agit généralement des métadonnées du fournisseur de services. Dans ce cas, il s'agit de : `https://<tetration-cluster-fqdn>/h4_users/saml/metadata`
Certificat SSO	Certificat SSO fourni par le fournisseur d'identité (IdP).
Contexte d'authentification SSO	Choix du contexte AuthN SSO spécifié dans la demande SAML. L'option par défaut est « Password Protected Transport » (transport protégé par un mot de passe). Les autres options sont « Authentification Windows intégrée » et « Certificat X.509 » pour l'authentification basée sur Windows et PIV.

Une fois la configuration SSO activée, tous les utilisateurs, à l'exception de ceux qui ont activé l'option Use Local Authentication, sont déconnectés de leurs sessions.

La configuration SSO est enregistrée lorsque vous avez cliqué sur le bouton **Save (Enregistrer)**.

Figure 21: Flux de travail de l'authentification



Renseignements partagés avec le fournisseur d'identité (IdP)

Le fournisseur d'identité a besoin de certaines informations de Cisco Secure Workload (SP) pour configurer le SSO en vue de l'authentification. Le tableau suivant décrit les champs qui doivent être configurés.

Champ	Description
URL SSO	Le point terminal d'authentification (URL) qui utilisera l'assertion SAML (réponse de l'IdP). Dans notre cas, ce sera : `https://<tetration-cluster-fqdn>/h4_users/saml/auth`
Identifiant de l'entité	Il s'agit des métadonnées pour le fournisseur de services. Dans ce cas, il s'agit de : `https://<tetration-cluster-fqdn>/ h4_users/saml/metadata`
Format de l'ID du nom	NameId est un courriel, c'est-à-dire `'urn:oasis:names:tc:SAML:1. 1:nameid-format:emailAddress'`
Attributs	que les attributs d'utilisateur sont extraits de l'IdP. Nous récupérons ces attributs dans le cadre de l'authentification : • courriel • Prénom • Nom Assurez-vous que les noms d'attributs sont tels que spécifiés précédemment.

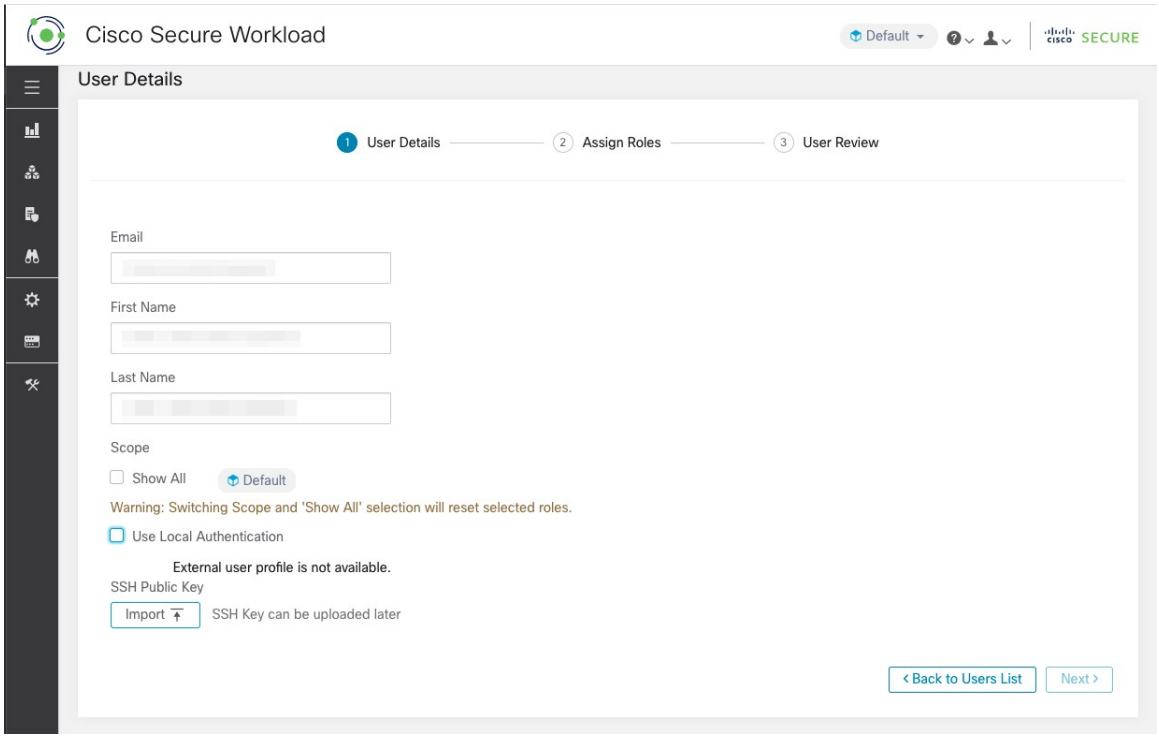
Résoudre les problèmes SSO

- Prévoyez un temps d'arrêt pour cette configuration SSO, car la seule façon de vérifier que l'authentification fonctionne (pour le fournisseur de services) est de l'avoir configurée.
- Vérifier et valider les métadonnées du fournisseur d'identité générées.
- Vérifier tous les paramètres de configuration qui sont échangés entre le fournisseur d'identité et le fournisseur de service.
    - Configuration au niveau du fournisseur d'identité : URL SSO, auditoire, ID de nom, attributs, etc.
    - Configuration sur la page de l'entreprise Cisco Secure Workload : URL de la cible SSO, émetteur SSO et certificat SSO.
- Obtenez un exemple d'assertion SAML renvoyée par le fournisseur d'identité à partir des journaux d'applications du serveur. Validez-la par rapport à un validateur SAML pour vous assurer qu'il s'agit d'une réponse SAML valide.
- Des erreurs dans la configuration du fournisseur de service SSO peuvent entraîner une erreur générée par le fournisseur d'identité. À l'aide de l'élément d'inspection du navigateur, vous pouvez voir les demandes réseau en cours.
- Si un utilisateur rencontre des problèmes pour se connecter, demandez à l'administrateur du fournisseur d'identité de vérifier si l'utilisateur a accès à l'application Cisco Secure Workload.

Option « Use Local Authentication » (Utiliser l'authentification locale)

Une fois la configuration mise en place, il est possible pour les administrateurs de site d'autoriser les utilisateurs à ne pas utiliser l'authentification externe. Cela peut être fait pour chaque utilisateur en activant l'indicateur « Use Local Authentication » (Utiliser l'authentification locale) dans la section de modification de l'utilisateur. La sélection de ce champ pour l'utilisateur déconnectera ce dernier de toutes les sessions.

Figure 22: Use Local Authentication (Utiliser l'authentification locale)



Warning **Assurez-vous qu'au moins un utilisateur dispose d'un accès à l'authentification locale!**

Si l'option « Use Local Authentication » est supprimée pour un utilisateur et que cet utilisateur est le dernier disposant de l'option, aucun utilisateur ne pourra se connecter à Cisco Secure Workload. Cela signifie qu'aucun utilisateur ne peut se connecter en cas de perturbations avec le système d'authentification externe, telles que des problèmes de configuration, de connectivité, etc. Vous verrez un avertissement si vous essayez de supprimer le dernier utilisateur authentifié localement.

Les utilisateurs se connectant par authentification externe ont des sessions plus courtes et seront invités à se connecter à l'expiration de la session. Les utilisateurs qui se connectent par authentification externe ne peuvent pas réinitialiser leur mot de passe sur le site (ils doivent le faire sur le site Web de leur entreprise). Toutefois, si l'indicateur « Use Local Authentication » est activé pour l'utilisateur, la réinitialisation du mot de passe est possible.

Certificat et clé SSL

Pour activer un accès HTTPS entièrement vérifiable à l'interface utilisateur Cisco Secure Workload, un certificat SSL spécifique au nom de domaine de l'interface utilisateur et à la clé privée RSA qui correspond à la clé publique du certificat SSL peut être téléversé dans la grappe.

Un certificat SSL peut être obtenu de deux manières, en fonction du format du nom de domaine complet (FQDN) utilisé pour faire référence à l'adresse IP virtuelle (VIP) de l'interface utilisateur Cisco Secure Workload. Si le nom de domaine complet Cisco Secure Workload est basé sur un nom de domaine d'entreprise comme tetration.cisco.com, l'autorité de certification (CA) de votre entreprise qui possède le domaine de base

vous délivre un certificat SSL. Sinon, vous pouvez utiliser un fournisseur de certificat SSL réputé pour vous délivrer un certificat SSL pour votre nom de domaine complet.

Note Il est important de noter que même si l'interface utilisateur Cisco Secure Workload prend en charge Server Name Indication (SNI), les autres noms de sujets (SAN) spécifiés dans le certificat ne seront pas mis en correspondance. Par exemple, si le nom commun (CN) du certificat est tetration.cisco.com et que le certificat inclut un SAN pour tetration1.cisco.com, les requêtes HTTPS envoyées avec un navigateur compatible SNI vers la grappe avec tetration1.cisco.com comme nom d'hôte ne seront pas servies avec ce certificat. Les demandes HTTPS faites à la grappe avec un nom d'hôte autre que le nom d'hôte spécifié dans le CN seront traitées à l'aide du certificat autosigné par défaut qui est installé sur la grappe. Ces demandes entraînent des avertissements du navigateur.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent utiliser des certificats SSL. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **SSL Certificate (Certificat SSL)** .

Pour importer le certificat et la clé, cliquez sur le bouton **Import New Certificate and Key** (Importer le nouveau certificat et la clé).

Note La première importation de la certification SSL et de la clé privée doit être effectuée par l'intermédiaire d'une connexion réseau de confiance vers la grappe afin que la clé privée ne puisse pas être interceptée par des tiers malveillants qui ont accès à la couche de transport.

Saisissez les informations suivantes pour votre certificat SSL et votre clé :

NAME peut être n'importe quel nom pour la paire de clés de certificat. Ce nom vous sera utile lorsque vous chercherez à savoir quel certificat SSL est installé.

Le champ **Certificat X509** accepte la chaîne de certificat SSL au format Privacy Enhanced Mail (PEM). Si votre certificat SSL nécessite un groupe d'autorités de certification intermédiaire, concaténez le groupe d'autorités de certification après votre certificat de sorte que le certificat SSL pour votre nom de domaine complet Cisco Secure Workload se trouve au début du fichier de certificat.

Il doit avoir le format suivant :

```
-----BEGIN CERTIFICATE-----

< Certificat pour Nom de domaine complet Cisco Secure Workload>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

<Contenu de l'autorité de certification intermédiaire 1>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

<Contenu de l'autorité de certification intermédiaire 2>

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
```

```
<Contenu de l'autorité de certification racine>

-----END CERTIFICATE-----
```

Le champ **Clé privée RSA** doit indiquer la clé privée RSA de la clé publique signée dans le certificat précédent. Il doit avoir le format suivant :

```
-----DÉBUT DE LA CLÉ PRIVÉE RSA-----

< données de la clé privée >

----FIN DE LA CLÉ PRIVÉE RSA----
```

Note La clé privée RSA doit être non chiffrée. Une « 500 Internal Server Error » (erreur du serveur interne 500) est émise si la clé privée RSA est chiffrée.

Après l'importation, des étapes de vérification sont exécutées pour s'assurer que la clé publique signée dans le certificat et la clé privée sont bien une paire de clés RSA. Si la vérification réussit, nous affichons le condensé SHA-1 (signature SHA-1 et heure de création) du lot de certificats.

Rechargez le navigateur pour constater que votre connexion SSL à l'interface utilisateur Cisco Secure Workload utilise maintenant le certificat SSL nouvellement importé.

Configuration de grappe

Cette section affiche la configuration d'exécution de la grappe Cisco Secure Workload pour le réseau et les contacts administratifs du client. Les valeurs modifiables sont indiquées par une icône en forme de crayon.

Note Strong SSL Ciphers for Agent Connections (chiffrements SSL forts pour les connexions d'agents) : lorsque cette option est activée, les protocoles TLS-1.0 et TLS-1.1 et les chiffrements suivants ne seront pas acceptés par la grappe Cisco Secure Workload pendant les négociations SSL : DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Les connexions suivantes les respectent et utilisent des chiffrements forts pendant l'établissement de liaison TLS :

1. Toutes les connexions d'API et d'interface utilisateur à Cisco Secure Workload.
2. Toutes les connexions des agents de visibilité et d'application à Cisco Secure Workload.

Remarque : les anciennes bibliothèques SSL peuvent ne pas prendre en charge cette option.

Les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle** peuvent accéder à ce paramètre. Dans la barre de navigation à gauche, cliquez sur **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)**.

Une fois la configuration modifiée, il faut un certain temps avant que la nouvelle configuration soit appliquée à l'ensemble de la grappe, ce qui est indiqué par la mise en surbrillance de la configuration particulière.

Connectivité de grappe IPv6 externe

Les grappes physiques Cisco Cisco Secure Workload peuvent être configurées pour se connecter à des réseaux externes IPv4 et IPv6. La connectivité IPv4 est obligatoire, mais la connectivité IPv6 est facultative. Une fois la connectivité IPv6 configurée, elle ne peut pas être désactivée. L'activation de la connectivité IPv6 pour la mise en réseau externe de la grappe ne peut se faire que lors du déploiement ou de la mise à niveau. Consultez le Guide de mise à niveau Cisco Cisco Secure Workload pour en savoir plus sur l'activation de la connectivité de grappe IPv6 externe lors de la mise à niveau ou le Guide de déploiement de matériel Cisco Cisco Secure Workload pour en savoir plus sur l'activation de la connectivité de grappe IPv6 externe lors du déploiement.

Before you begin

Pour que les agents fonctionnent en mode double pile (prise en charge d'IPv4 et d'IPv6)

Préalables

- IPv6 doit être activé sur la grappe.
- Créez des enregistrements A et AAAA (pour IPv4 et IPv6) dans le DNS pour un nom de domaine complet et attendez que les noms de domaine se résolvent.

Configurer « Sensor VIP FQDN » (Nom de domaine complet de la VIP du capteur) pour que les agents fonctionnent en mode double pile.

Procedure

Étape 1 Choisissez **Platform(Plateforme)** > **Cluster Configuration (Configuration de la grappe)** dans la barre de navigation à gauche.

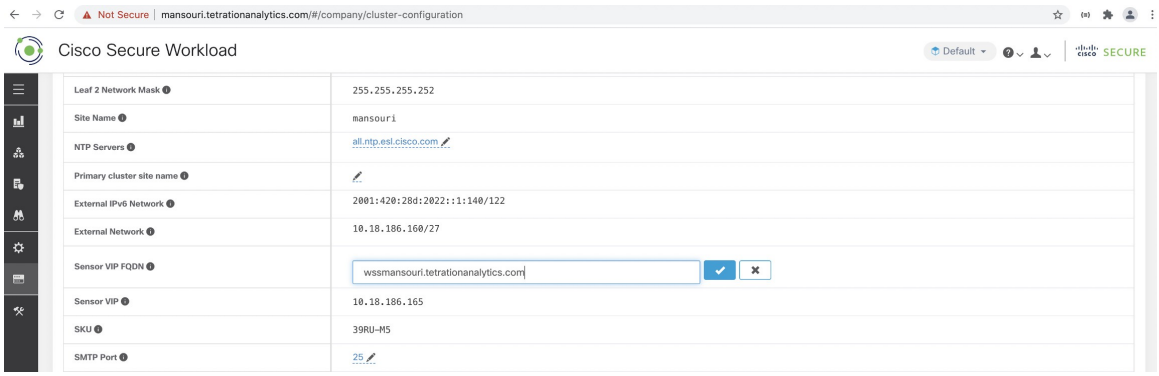
Étape 2 Recherchez les champs « Sensor IPv6 VIP », « Sensor VIP » et « Sensor VIP FQDN ». Les options « Sensor IPv6 VIP » et « Sensor VIP » devraient déjà être définies.

Étape 3 Si « Sensor VIP FQDN » n'est pas défini, définissez-le sur le nom de domaine complet créé ci-dessus. Les enregistrements A et AAAA dans le DNS pour le nom de domaine complet doivent être résolus avant que vous ne fassiez cela.

Étape 4 Si le nom de domaine complet du capteur Sensor VIP FQDN a déjà été défini, assurez-vous qu'il y a des enregistrements A et AAAA dans le DNS correspondant au nom de domaine complet, comme défini dans le champ « Sensor VIP FQDN », puis cliquez dans le champ « Sensor VIP FQDN » et enregistrez-le à la même valeur afin qu'il soit mis à jour.

Étape 5 Une fois la mise à jour du champ terminée (après environ 20 minutes, l'état est mis à jour automatiquement), les agents pourront se connecter à la grappe par IPv4 et IPv6.

Étape 6 Un « Sensor VIP FQDN » (Nom de domaine complet de la VIP du capteur) valide ne peut être défini qu'une seule fois.



Note Aucune prise en charge de la mise en application IPv6 pour AIX. Pour en savoir plus sur les exigences et les limites du mode double pile, consultez le Guide de mise à niveau de Cisco Cisco Secure Workload.

Authentification NTP

La version sur site de Cisco Secure Workload prend en charge la version 4 du protocole NTP (Network Time Protocol) et l'authentification SHA-1. Configurez le serveur NTP à l'aide de l'interface utilisateur de configuration ou utilisez la page de configuration de la grappe pour déployer l'appareil sur Cisco Secure Workload.

Pour configurer l'authentification NTP à l'aide de l'interface utilisateur de Cisco Secure Workload :

Procedure

Étape 1 Configurez le serveur NTP : Un système exécutant CentOS 7 fournit les configurations suivantes à titre de référence, et les configurations varient en fonction du système d'exploitation.

a) Assurez-vous que les entrées suivantes sont disponibles dans le dossier `/etc/ntp.conf`.

```
# Key file containing the keys and key identifiers used when operating with symmetric
key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
trustedkey 1
controlkey 1
requestkey 1
```

b) Saisissez la clé côté serveur sous `/etc/ntp/keys`.

```
# For more information about this file, see the man page ntp_auth(5).
# id type key
1 SHA1 <password>
```

c) Redémarrez le serveur NTP : `# service ntpd restart`

d) Démarrez le service pour le serveur NTP :

```
# ntpq -p
     remote           refid      st   t  when   poll   reach   delay   offset  jitter
```

```
===============================================================================
<ntp.server.com> <refid>      5  u  17     64     377  0.000  0.000   0.000
```

Étape 2 Sur l'interface utilisateur de Cisco Secure Workload, accédez à **Platform (Plateforme)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 3 Dans le champ **Authenticated NTP Server** (serveur NTP authentifié), saisissez le nom ou l'adresse IP du serveur NTP.

Étape 4 Dans le champ **Password For Authenticated NTP Server** (mot de passe du serveur NTP authentifié), saisissez le mot de passe du serveur NTP.

Après avoir configuré et authentifié le serveur NTP, ce dernier prévaut sur tous les serveurs NTP non authentifiés que vous saisissez dans Cisco Secure Workload.

Désactiver le téléchargement et l'enregistrement des agents non pris en charge

En tant qu'administrateur système, vous avez la possibilité d'empêcher les agents dont les versions ne sont pas prises en charge de s'enregistrer auprès de la grappe ou d'être installés à l'aide du script d'installation. Cela est géré par une nouvelle configuration qui bloque efficacement les nouvelles installations d'agents dotés des versions obsolètes.

Par exemple, si vous utilisez Cisco Secure Workload version 3.9 et que l'agent que vous essayez de télécharger ou d'enregistrer utilise la version 3.7 ou une version antérieure, l'agent ne pourra pas télécharger ou s'enregistrer. Cette fonctionnalité est conçue pour garantir que tous les agents de la grappe fonctionnent sur des versions prises en charge, ce qui peut permettre de prévenir les problèmes de compatibilité ou les vulnérabilités de sécurité qui pourraient exister avec les anciennes versions du logiciel.

Désactiver les agents non pris en charge

Pour activer la configuration **Disable Unsupported Agents** (désactiver les agents non pris en charge), procédez comme suit :

Procedure

Étape 1 Connectez-vous à l'interface utilisateur de Cisco Secure Workload en tant qu'administrateur.

Étape 2 Dans le volet de navigation, choisissez **Platforms (Plateformes)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 3 Définissez le champ de configuration **Disable Unsupported Agents** (désactiver les agents non pris en charge) sur **True** (Vrai). Par défaut, cette fonction est désactivée.

What to do next

Après avoir activé la configuration, les agents dont les versions ne sont pas prises en charge ne pourront pas s'inscrire auprès de la grappe ou être installés à l'aide du script d'installation. Cela bloque efficacement l'installation des agents avec des versions obsolètes, garantissant que seules les versions d'agent prises en charge sont utilisées dans l'environnement.

Pour poursuivre l'inscription de l'agent, nous vous recommandons de télécharger la dernière version de l'agent logiciel.

Désactiver le téléchargement de l'agent

Pour empêcher l'installation d'agents ayant des versions de logiciels obsolètes, procédez comme suit :

Procedure

Étape 1 Dans le volet de navigation, choisissez **Platforms (Plateformes)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 2 Activez la configuration de **Disable Agent Download** (désactivation du téléchargement de l'agent).

Une fois la configuration activée, l'agent ne peut plus télécharger avec succès, quelle que soit la version de l'agent logiciel.

Désactiver l'enregistrement de l'agent

Pour empêcher l'enregistrement de nouveaux agents :

Procedure

Étape 1 Connectez-vous à l'interface utilisateur de Cisco Secure Workload en tant qu'administrateur.

Étape 2 Dans le volet de navigation, choisissez **Platforms (Plateformes)** > **Cluster Configuration (Configuration de la grappe)** .

Étape 3 Activez la configuration de **Désactiver l'enregistrement de l'agent**. Après avoir activé la configuration, vous ne pouvez pas enregistrer de nouvel agent sur l'appareil qui ne correspond pas à la version du logiciel.

Note Après avoir activé la configuration, si vous tentez de télécharger ou d'enregistrer un agent avec une version non prise en charge, l'enregistrement sur l'appareil échoue et un message d'avertissement s'affiche sur l'interface graphique (GUI) indiquant : "Package download or registration for the old agent version is disabled." ("Le téléchargement ou l'enregistrement de paquets pour l'ancienne version de l'agent est désactivé.") Cela garantit que seuls les agents dont les versions sont prises en charge peuvent être enregistrés ou installés, ce qui empêche l'utilisation de versions d'agent obsolètes dans l'environnement.

Note Par défaut, les configurations **Disable Unsupported Agents (Désactiver les agents non pris en charge)**, **Disable Agent Download (Désactiver le téléchargement de l'agent)** et **Disable Agent Registration (Désactiver l'enregistrement des agents)** sont désactivées.

Analyse de l'utilisation

Les administrateurs de site et **les utilisateurs du service d'assistance à la clientèle** peuvent activer ou désactiver l'analyse de l'utilisation. Dans la barre de navigation, cliquez sur **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Usage Analytics (Analyse de l'utilisation)**.

Cisco Secure Workload collecte les données et les restitue de manière anonyme grâce au condensé unidirectionnel avant de les envoyer au serveur. Configurez les paramètres de confidentialité par appareil pour un appareil sur site et par détenteur pour le logiciel-service Cisco Cisco Secure Workload. Vous pouvez également activer la collecte de données et basculer la collecte sur cette page.

Fédération

La Fédération permet de réunir plusieurs appareils Cisco Secure Workload et de consolider la majeure partie de leur gestion en un seul appareil désigné comme le **leader** (chef de file).

Remarque

- Cette fonctionnalité nécessite que tous les appareils de la Fédération exécutent la version 3.4.x ou une version ultérieure.
- Communiquez avec le centre d'assistance technique de Cisco pour activer l'option de Fédération.

Configurer la Fédération

Procédure

Étape 1 Sur le **leader** chef de file) désigné , accédez à **Platform(Plateforme)** > **Federation (Fédération)** et cliquez sur le bouton **Create New Federation** (Créer une nouvelle Fédération).

Étape 2 Pour ajouter le premier appareil **suiveur**, entrez son nom et son nom de domaine complet (FQDN), puis cliquez sur le bouton **Add** (ajouter).

Étape 3 Cliquez sur le lien pour télécharger le fichier de certificat de jonction.

Étape 4 Sur le **suiveur**, accédez à **Platform** > **Federation**, cliquez sur **Join Existing Fédération** (Rejoindre la Fédération existante), puis sélectionnez le certificat de jonction créé ci-dessus.

Étape 5 Répétez les étapes 2 à 4 pour chaque **suiveur** qui fera partie de la Fédération.

Illustration 23 : Créer ou rejoindre une Fédération

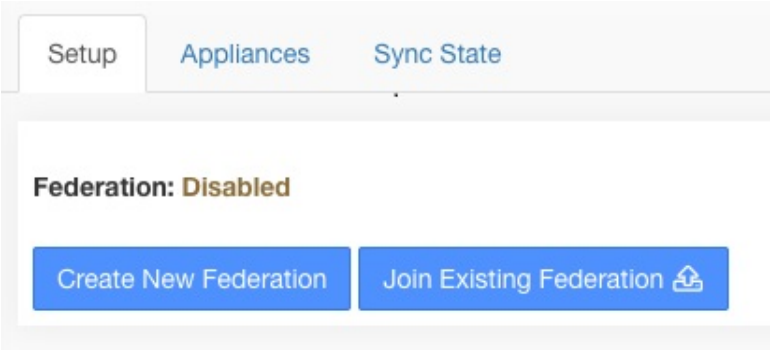
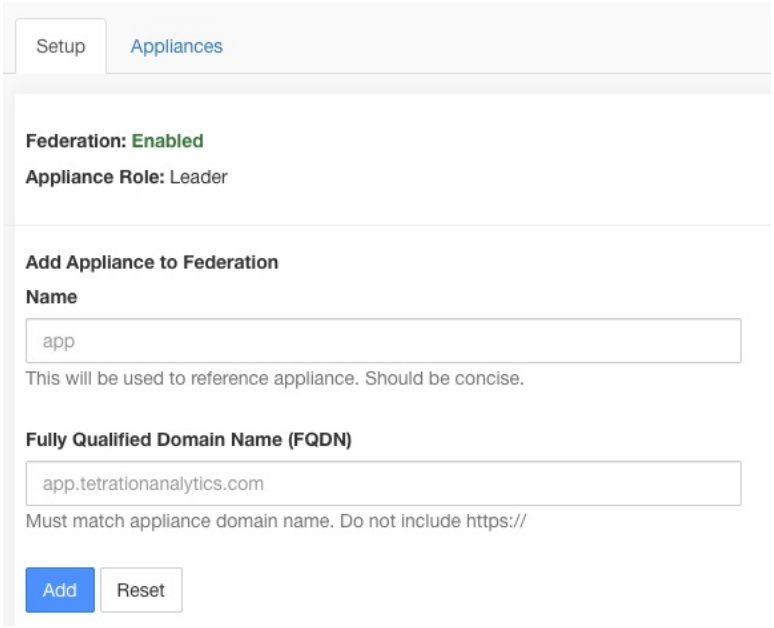
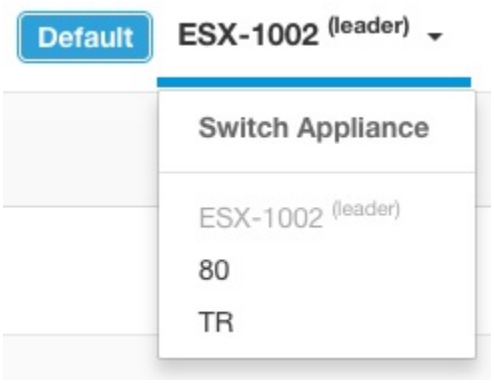


Illustration 24 : Formulaire d'ajout de suiveur à la Fédération



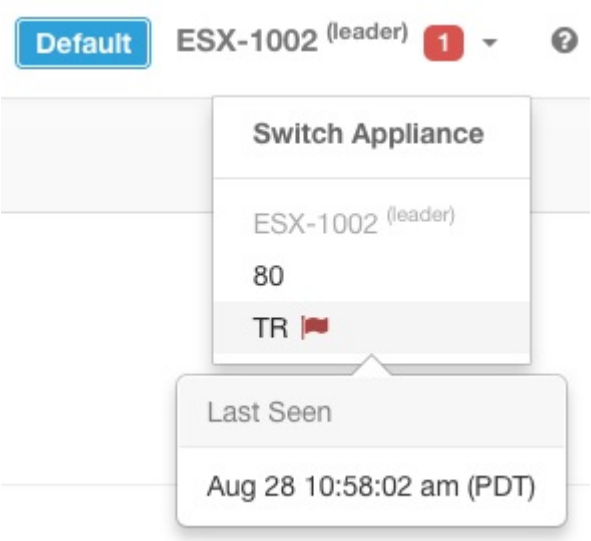
Lorsque la Fédération est activée, l'en-tête comprend le nom de l'appareil et un sélecteur pour la modification des appareils.

Illustration 25 : Sélecteur d'appareils



Si au moins un appareil de la Fédération n'a pas été vu par le chef de file après plus de 10 minutes, une alerte s'affiche dans le sélecteur d'appareils et les appareils problématiques sont signalés. Passer le curseur sur eux permet d'afficher la dernière fois qu'ils se sont synchronisés avec le chef de file.

Illustration 26 : Sélecteur d'appareils avec alertes



Configuration de l'authentification

L'authentification avec Fédération activée est configurée à l'aide de la connexion unique (SSO). La SSO doit être configurée sur chaque appareil de la Fédération. La configuration de la SSO est configurée sur le leader (chef de file) et chacun des suiveurs sur la page d'**authentification externe** > **de la plateforme** , comme indiqué dans la section Configurer la connexion unique (SSO) sur chaque appareil.

Tâches administratives

Selon la tâche administrative, certaines doivent être effectuées sur le **leader (chef de file)** et d'autres sur les **suiveurs**. Le tableau suivant indique le type d'appareil pour chaque tâche.

Tableau 1 : Tâches administratives dans l'appareil de Fédération

Tâche	Appareil
Utilisateurs	Chef de file
Portées	Chef de file
Rôles	Chef de file
Détenteurs	Chef de file
Clé API	Chef de file
Règles de collecte	Chef de file
Configuration de l'agent logiciel	Chef de file
Agents logiciels	Suiveurs

Tâche	Appareil
Mise à niveau de l'agent logiciel	Suiveurs
Rétrogradation de l’agent logiciel	Suiveurs
Filtres d’inventaire	Chef de file
Téléversement de l’inventaire	Chef de file
Configuration par défaut de la découverte des politiques	Chef de file
Ordre des politiques	Chef de file

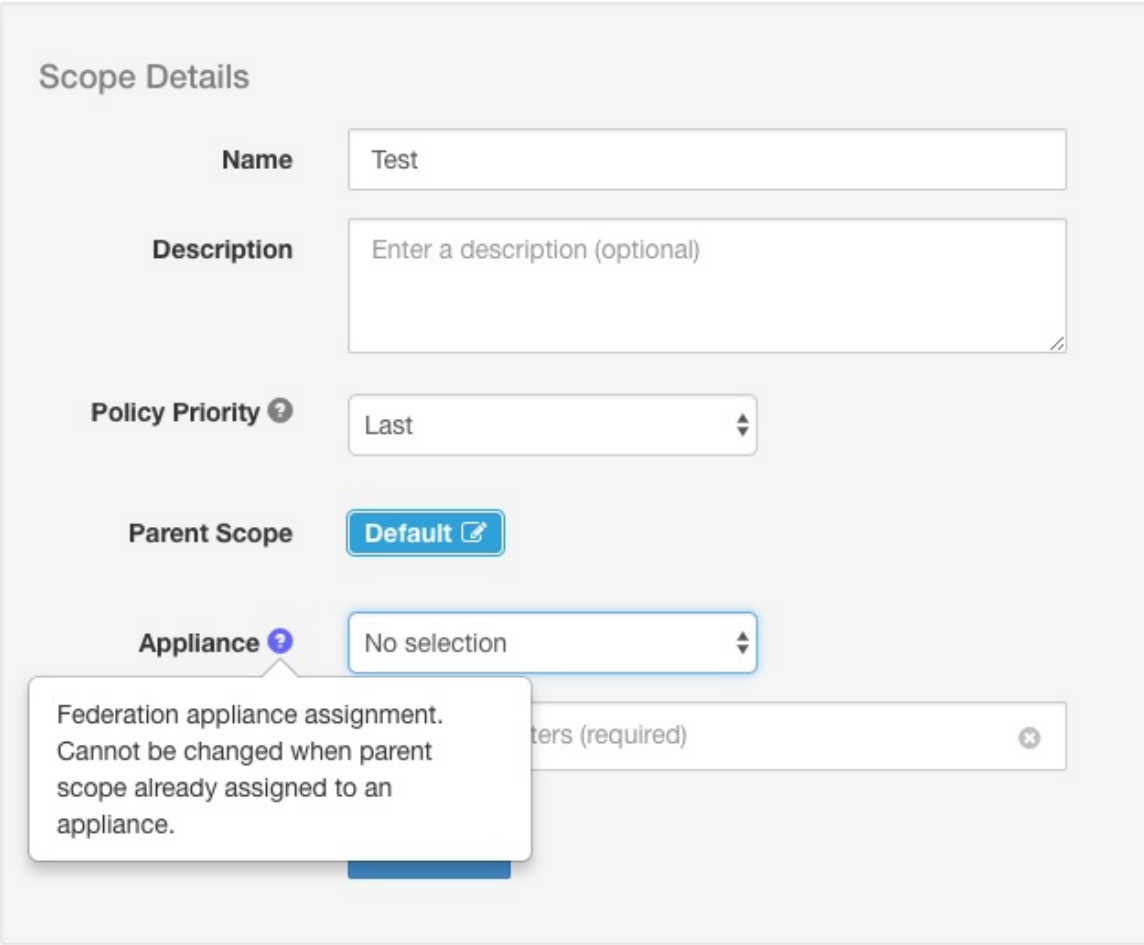
Portées

Lorsque l'inventaire d’une portée est géré par un seul appareil, cette portée peut être attribuée à l’appareil. Cela permet la découverte, l’analyse et l’application automatiques des politiques dans les espaces de travail associés à cette portée. Cela garantit également que les politiques créées sur cette portée s’appliquent uniquement aux agents connectés à l’appareil.

Les applications créées sur des portées globales (non affectées à un appareil) ne peuvent pas être utilisées pour la découverte ou l’analyse automatique des politiques. Cependant, elles peuvent être utilisées pour appliquer les politiques sur tous les appareils de la Fédération.

Un appareil peut être affecté à une portée lors de la création ou en modifiant la portée. Toutes les portées enfants héritent de l’appareil parent et ne peuvent pas être affectées à un autre appareil.

Illustration 27 : Affecter l'appareil à la portée



Remarque Les portées au niveau racine (détenteurs) sont toujours globales et ne peuvent pas être affectées à un appareil.

Espaces de travail

Tous les espaces de travail (« applications ») doivent être gérés sur l'appareil **chef de file**. Cependant, les organigrammes basés sur les flux ne peuvent être affichés que sur l'appareil **suiveur** correspondant. Ceux-ci comprennent les tableaux affichés sous les onglets **Policy Analysis** (Analyse des politiques) et **Enforcement** (Mise en application). Sur l'appareil **leader** (chef de file), cliquez sur **View Charts on Local Appliance** (Afficher les graphiques sur l'appareil local) pour accéder à l'appareil **follower** (suiveur) correspondant.

Illustration 28 : Analyse des politiques sur le chef de file

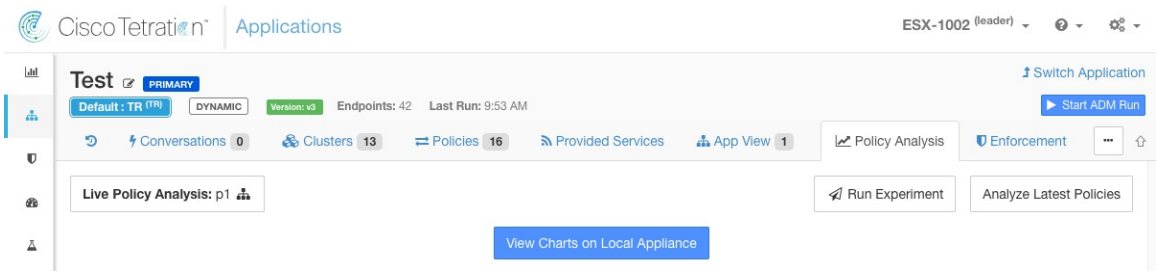
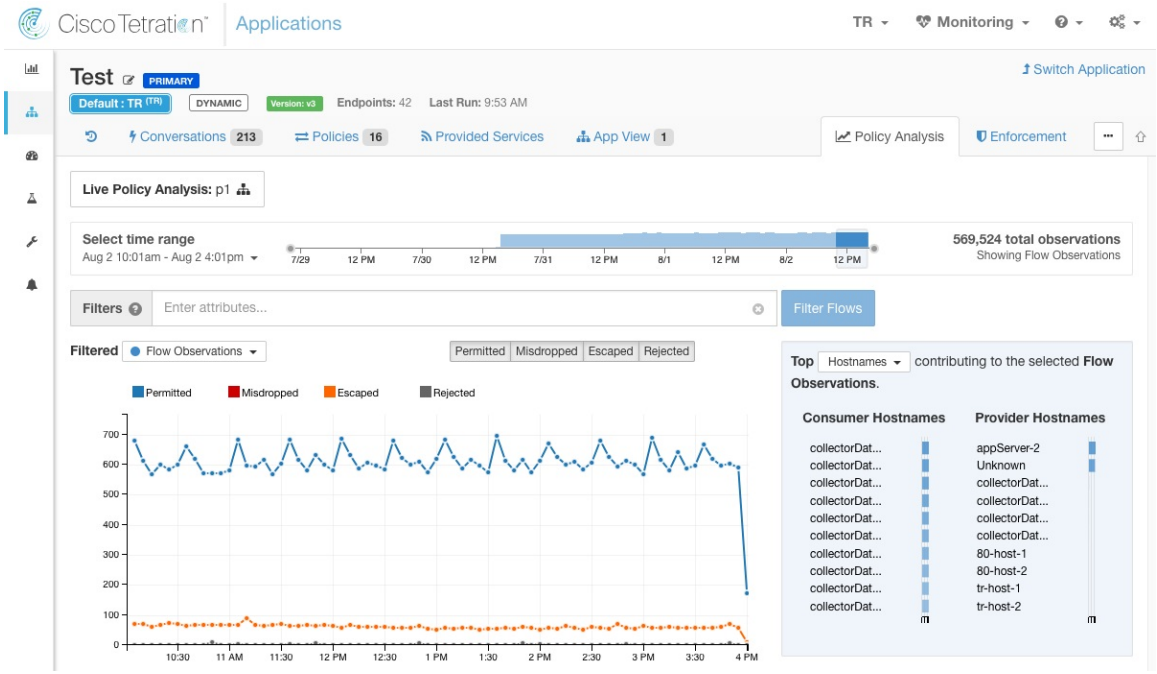
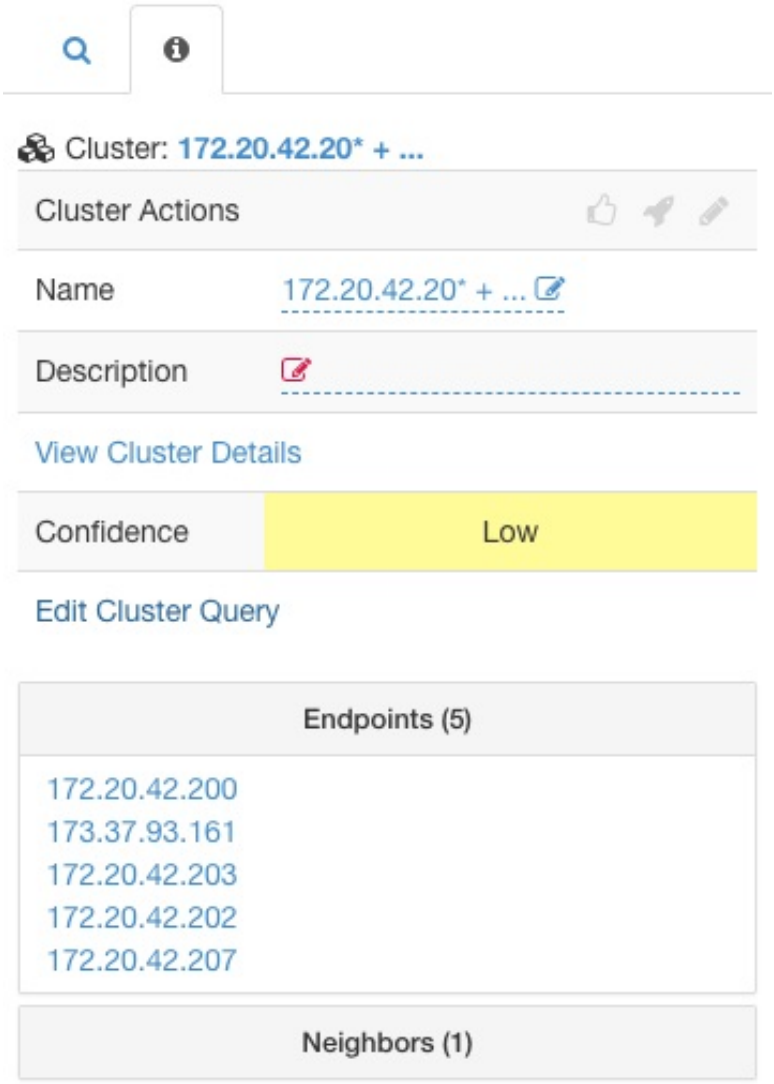


Illustration 29 : Analyse des politiques sur le suiveur



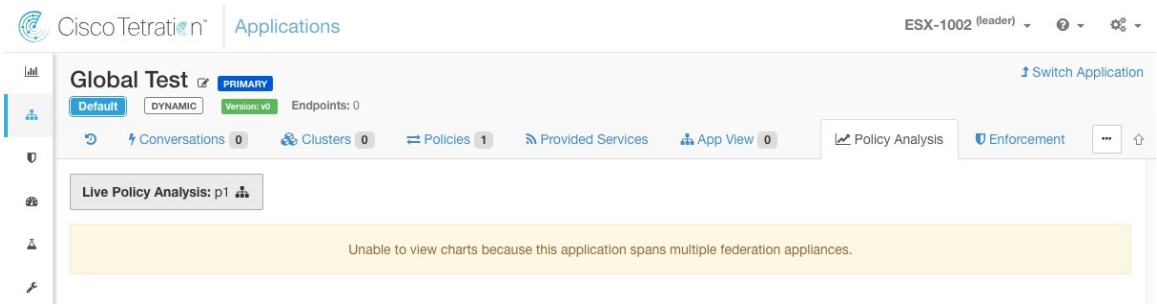
En outre, les recherches dans l'inventaire (à l'exception de la page de découverte automatique des politiques) sont toujours effectuées localement. Par conséquent, il est nécessaire d'accéder au **suiveur** pour afficher les points de terminaison de la grappe, du filtre et de la portée. La même logique s'applique à l'affichage des détails de la grappe, du filtre et de la portée.

Illustration 30 : Panneau latéral de la grappe



Comme expliqué ci-dessus, les espaces de travail créés sur des portées globales ne peuvent pas être utilisés pour la découverte ou l'analyse automatique des politiques. Bien que les politiques puissent être appliquées, les tableaux d'application basés sur les flux ne sont pas disponibles.

Illustration 31 : Analyse des politiques désactivée pour les portées globales



Avertissement Les politiques utilisant un filtre de portée ou d'inventaire restreint associé à un appareil ne seront appliquées que sur cet appareil.

Agents logiciels

Tous les agents logiciels connectés à n'importe quel appareil de la Fédération sont visibles sur le **leader** (chef de file).

Procédure

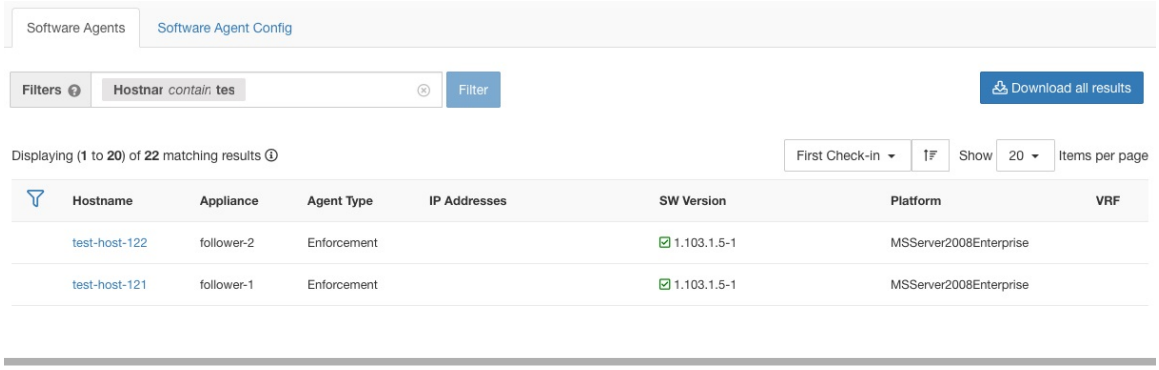
Étape 1 Cliquez sur le **Settings menu** (menu Paramètres) dans le coin supérieur droit.

Étape 2 Sélectionnez **Agent Config** (Configuration de l'agent).
La page **Agent Config** (Configuration de l'agent) s'affiche.

Étape 3 Cliquez sur l'onglet **Software Agents** (Agents logiciels).
L'onglet **Software Agents** (agents logiciels) s'ouvre.

Étape 4 Recherchez un ou plusieurs agents à déplacer et cochez les cases correspondant aux lignes du tableau.

Étape 5 La colonne **Appliance** (Appareil) indique l'endroit où l'agent est connecté.



Déplacement d'agents logiciels entre appareils suiveurs

Les agents logiciels peuvent être déplacés entre les appareils **suiveurs**. À partir de l'appareil auquel l'agent ou les agents sont connectés, procédez comme suit :

Procédure

Étape 1 Cliquez sur le **Settings menu** (menu Paramètres) dans le coin supérieur droit.

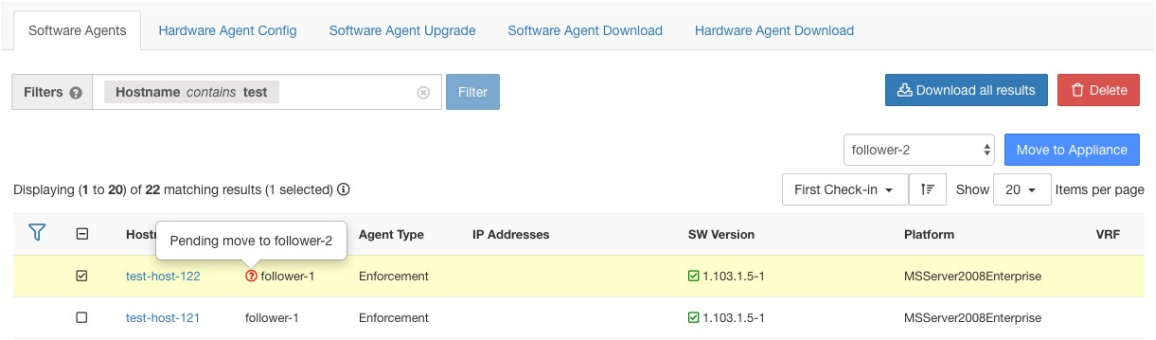
Étape 2 Sélectionnez **Agent Config**(Configuration de l'agent). La page s'affiche.

Étape 3 Cliquez sur l'onglet **Software Agents** (Agents logiciels). L'onglet **Software Agents** (agents logiciels) s'ouvre.

Étape 4 Recherchez un ou plusieurs agents à déplacer et cochez les cases correspondant aux lignes du tableau.

Étape 5 Dans la liste déroulante **-Select Appliance-** (sélectionner un appareil), sélectionnez l'appareil souhaité pour ces agents.

Étape 6 Cliquez sur le bouton **Move to Appliance** (Déplacer vers l'appareil).



Le tableau est mis à jour pour indiquer qu'un déplacement est en attente. Lors de la prochaine connexion de l'agent, il recevra un message l'invitant à déplacer les appareils. Une fois le déplacement terminé, l'agent ne sera plus visible sur l'appareil d'origine. Visiter la page des**Softxare Agents** (agents logiciels) du nouvel appareil pour vérifier que le déplacement a réussi.

Autres tâches

En général, les requêtes basées sur les flux et l'inventaire doivent être effectuées sur les appareils **suiveurs**. Le tableau suivant indique le type d'appareil pour quelques tâches courantes.

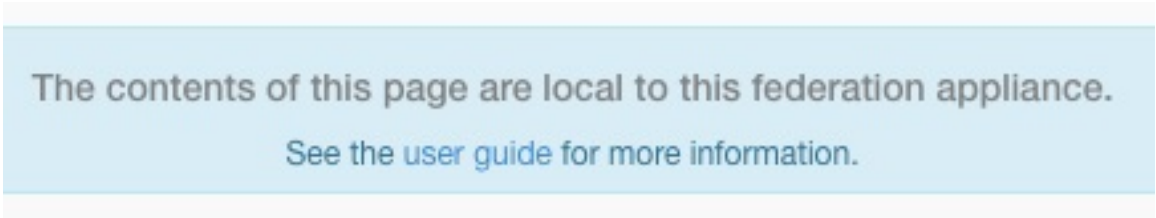
Tableau 2 : Type d'appareil de Fédération pour les tâches courantes

Tâche	Appareil
Visibilité > > **Recherche de flux**	Suiveurs
Visibilité > **Recherche d'inventaire**	Suiveurs
Visibilité > **Filtres d'inventaire**	Suiveurs
Visibilité > **Orchestrateurs externes**	Suiveurs
Segmentation > **Découverte automatique des politiques**	Chef de file
Segmentation > **Analyse des politiques**	Chef de file
Segmentation > **Historique de l'application**	Chef de file

Tâche	Appareil
Segmentation > **Conversations**	Suiveurs
Segmentation > **Résultats de l'analyse**	Suiveurs
Segmentation > **Résultats de l'application**	Suiveurs
Surveillance > **Agents**	Suiveurs
Surveillance > **État d'application**	Suiveurs
Surveillance > **Licences**	Suiveurs
Agents logiciels > **Modifier les appareils**	Suiveurs

Toutes les autres tâches non incluses ci-dessus doivent être considérées comme *locales* à l'appareil. Par conséquent, toutes les modifications apportées ou les résultats affichés ne représentent que l'état de l'appareil actuel, et non l'état de la Fédération. Sur ces pages, l'alerte suivante s'affichera.

Illustration 32 : Alerte d'appareil local



Déploiement existant

Les sections suivantes fournissent un ensemble de directives pour la conservation des données sur les appareils qui rejoignent une Fédération.

Données conservées

L'utilisateur est responsable de la copie des utilisateurs, des rôles, des règles de collecte, des profils criminalistiques, des étiquettes téléversées par l'utilisateur et des configurations d'agent du follower (suiveur) vers le leader (chef de file) avant de l'ajouter à une Fédération. Les données du suiveur qui ne sont pas copiées sur le chef de file sont effacées et remplacées par les données du chef de file.

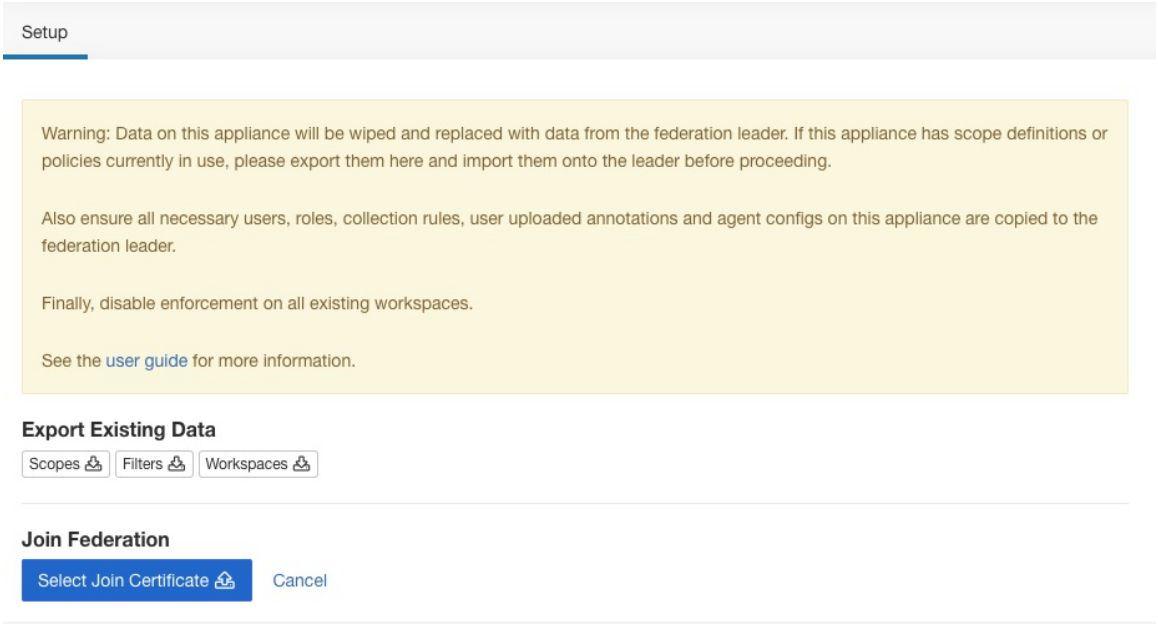
Effectuez les actions suivantes pour préserver les portées, les filtres et les politiques sur les **suiveurs** en les exportant vers des fichiers qui peuvent ensuite être importés sur le **chef de file**.

Procédure

Étape 1 Sur l'appareil suiveur, accédez à **Platform (Plateforme)** > **Federation (Fédération)** et cliquez sur le bouton **Join New Federation** (Rejoindre une nouvelle Fédération).

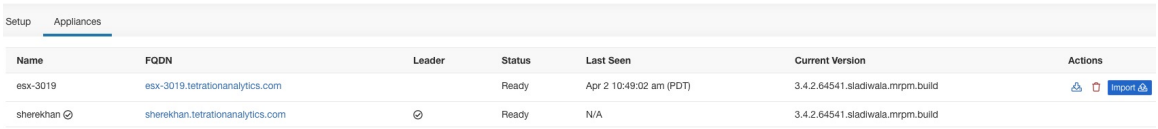
Téléchargez les portées, les filtres et les espaces de travail localement sur l'appareil.

Illustration 33 : Flux de travail d'exportation de déploiement existant sur l'appareil suiveur



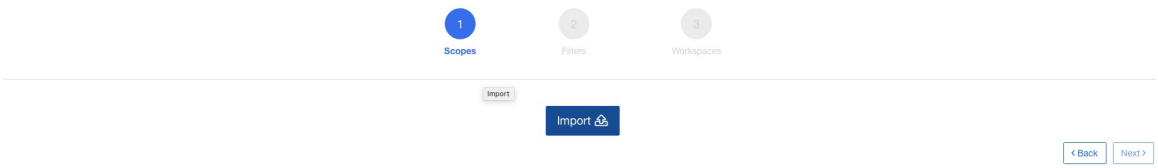
Étape 2 Sur le **chef de file**, accédez à **Platform (Plateforme)** > **Federation (Fédération)**. Ajoutez le suiveur en saisissant son nom et son nom de domaine complet (FQDN) et en cliquant sur le bouton **Add** (ajouter). Passez ensuite à la vue des appareils et cliquez sur le bouton **Import** (Importer) à droite du nom de domaine complet de l'appareil.

Illustration 34 : Icône Importation de déploiement existant sur le suiveur



Vous pouvez charger des portées , des filtres et des espaces de travail téléchargés à partir du suiveur. À chaque étape, résolvez tout conflit avant de passer à l'étape suivante.

Illustration 35 : Assistant d'importation de déploiement existant sur le suiveur



Les conflits entre les entrées sur le chef de file et le suiveur sont détectés en comparant les noms de ces entrées sur les deux appareils. Par exemple, considérons une portée **Default:host** qui existe à la fois sur le chef de file et le suiveur. Sur l'appareil chef de file, la requête pour cette portée est définie sur **Hostname eq foo** et sur l'appareil suiveur, il s'agit de **Hostname eq bar**. L'assistant d'importation avertit l'utilisateur qu'un conflit existe pour cette portée et choisit la requête du chef de file(c'est-à-dire **Hostname eq foo**).

Étape 3 Enfin, vous devez *désactiver la mise en application* sur tous les espaces de travail existants sur le suiveur avant de l'ajouter à la Fédération.

Étape 4 Les étapes 1 à 3 doivent être répétées pour chaque appareil suiveur qui rejoint la Fédération.

Données non conservées

1. Les appliances virtuelles (y compris celles utilisées avec les connecteurs) doivent être remises en service sur un appareil suiveur après qu'il ait rejoint la Fédération.
2. Les données de flux sur un suiveur jusqu'au moment où il rejoint la Fédération sont inaccessibles pour les portées communes avec le chef de file.

Mode de fonctionnement déconnecté

Remarque Applicable aux suiveurs.

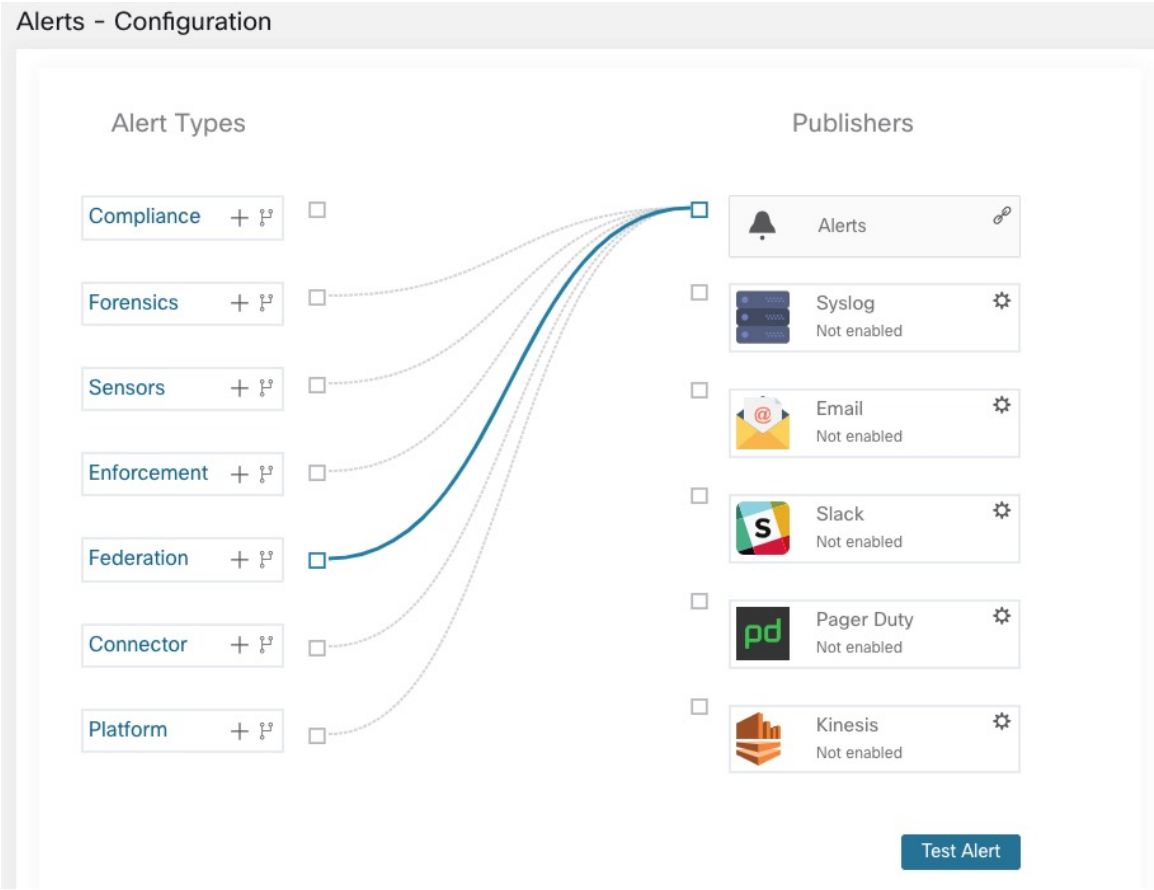
Dans certaines circonstances, par exemple en cas de partition réseau, il est logique de désactiver la Fédération sur un ou plusieurs **suiveurs**, ce qui leur permet de fonctionner en mode autonome. Pour ce faire, accédez à **Platform** (plateforme **)** et cliquez sur le bouton **Disable** (désactiver). Un suiveur qui est déconnecté de la Fédération continue de fonctionner en tant que grappe autonome.

Les nouvelles portées, les filtres d'inventaire et les espaces de travail du suiveur peuvent être préservés en les exportant vers des fichiers qui sont ensuite importés sur le leader (chef de file) avant de le réintégrer dans la Fédération. Cela conserve les modifications apportées aux politiques pour les espaces de travail existants. Cependant, les modifications apportées aux portées et aux filtres d'inventaire déjà présents sur le leader sont perdues lorsque le suiveur rejoint la Fédération.

Configurer les alertes

Pour activer les alertes, dans le volet de navigation, choisissez **Manage** > **Workloads** > **Alert Configs** (Gestion > Charges de travail > Configurations des alertes). Mettre à jour la configuration des alertes pour la Fédération.

Illustration 36 : Alertes de la Fédération



Vous pouvez générer des alertes pour les événements suivants :

- Générez des alertes sur le contrôleur chef de file de niveau de gravité MOYENNE lorsqu'un ou plusieurs appareils de la Fédération n'ont pas été en contact avec lui depuis plus de 10 minutes.
- Générer des alertes sur le suiveur avec un niveau de gravité MOYENNE lorsqu'il ne peut pas contacter le contrôleur chef de file pendant plus de 10 minutes.

Détails de l'alerte

Consultez la Structure commune des alertes pour obtenir la structure générale des alertes et des informations sur les champs. Le champ *alert_détails* est structuré et contient les sous-champs suivants pour les alertes de Fédération

Remarque *Appliance*, il s'agit de l'appareil qui a déclenché l'alerte.

Tableau 3 : Détails de l'alerte de Fédération

Champ	Type d'alerte	Format	Explication
ID	*tous*	chaîne	ID de dispositif
Nom	*tous*	chaîne	Nom de l'appareil
fqdn	*tous*	chaîne	Nom de domaine complet (FQDN) de l'appareil
is_leader	*tous*	booléen	True (vrai) si l'appareil est le leader (chef de file)
état	*tous*	chaîne	État de l'appareil
current_sw_version	*tous*	chaîne	Version du logiciel sur l'appareil
last_seen_at	*tous*	nombre entier	Horodatage Unix du moment où l'appareil a été vu pour la dernière fois
created_at	*tous*	nombre entier	Horodatage Unix de la création de l'appareil
updated_at	*tous*	nombre entier	Horodatage Unix de la mise à jour de l'appareil
created_at	*tous*	nombre entier	Horodatage Unix de la création de l'appareil
deleted_at	*tous*	nombre entier	Horodatage Unix de la suppression de l'appareil.
disconnected	*tous*	booléen	Défini à « vrai » lorsque l'abonné s'est déconnecté du leader. Toujours mettre à « faux » pour le leader

Exemple de alert_détails pour une alerte de suiveur déconnecté

```
{
  "id": "5f219ad8755f024b46c2524a",
  "name": "esx-3018",
  "fqdn": "esx-3018.tetrationanalytics.com",
  "is_leader": false,
  "status": "Ready",
  "current_sw_version": "3.4.0.39.devel",
  "last_seen_at": 1596140582,
  "created_at": 1596037848,
  "updated_at": 1596140582,
  "deleted_at": 0,
  "disconnected": true
}
```

Exemple de alert_details pour une alerte de leader déconnecté

```
{
  "id": "5f219acc755f024b46c25248",
  "name": "sherekhan",
  "fqdn": "sherekhan.tetrationanalytics.com",
  "is_leader": true,
  "status": "Ready",
  "current_sw_version": "3.4.0.39.devel",
  "last_seen_at": 1596140582,
  "created_at": 1596037848,
  "updated_at": 1596140582,
  "deleted_at": 0,
  "disconnected": false
}
```


API

Remarque Les renseignements d'authentification pour une grappe de Fédération doivent être générés sur le chef de file et peuvent être utilisés pour interroger les suiveurs.

Cette section répertorie les API ajoutées ou mises à jour pour la Fédération :

Appareils

Le point terminal des appareils permet à l'utilisateur de récupérer l'état d'un appareil dans une Fédération.

Objet appareil

Les attributs de l'objet appareil sont décrits dans le tableau suivant :

Attribut	Type	Description
ID	chaîne	Identifiant unique pour l'appareil.
name	chaîne	Nom précisé par l'utilisateur pour l'appareil.
fqdn	chaîne	Nom de domaine complet (FQDN) de l'appareil spécifié par l'utilisateur.
is_leader	booléen	Indique si l'appareil est un leader (chef de file).
status	chaîne	État de l'appareil.
current_sw_version	chaîne	Version du logiciel Cisco Secure Workload sur l'appareil.
last_seen_at	nombre entier	Horodatage Unix du moment où le suiveur a été vu pour la dernière fois par le leader. Il est toujours nul pour le leader.

Attribut	Type	Description
deleted_at	nombre entier	Horodatage Unix de la suppression de l'appareil.
disconnected	booléen	Indique si le suiveur a perdu le contact avec le leader. La valeur est Faux (False) pour le chef de file.

Répertorier les appareils

Ce point terminal renvoie un tableau d'appareils dans le regroupement Fédération.

```
GET /openapi/v1/appliances
```

Paramètres : Aucun

Objet de réponse : renvoie un tableau des objets de l'appareil.

Exemple de code Python

```
restclient.get('/appliances')
```

Portées

Le Objet portée comprend maintenant l'ID de l'appareil associé à une portée. Il est défini à null pour les portées globales.

Les API suivantes acceptent maintenant un ID d'appareil lors de la création ou de la mise à jour des portées.

Créer une portée

Un ID d'appareil fourni lors de la création d'une portée l'associe à un appareil spécifique.

```
POST /openapi/v1/app_scopes
```

Paramètres :

Nom	Type	Description
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.
parent_app_scope_id	chaîne	ID de la portée parente.
policy_priority	nombre entier	La valeur par défaut est « dernier ». Utilisé pour trier les priorités de l'espace de travail. Voir le classement des politiques sous Consulter les politiques découvertes automatiquement.

Nom	Type	Description
appliance_id	chaîne	Identifiant unique pour l'appareil.

Exemple de code Python

```
req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "parent_app_scope_id": <parent_app_scope_id>,
    "appliance_id": <appliance_id>,
}
resp = restclient.post('/app_scopes', json_body=json.dumps(req_payload))
```

Mettre à jour une portée

Cette API permet d'associer des portées existantes à des appareils en utilisant leur ID d'appareil.

```
PUT /openapi/v1/app_scopes/{app_scope_id}
```

Paramètres :

Nom	Type	Description
short_name	chaîne	Nom spécifié par l'utilisateur de la portée.
description	chaîne	Description de la portée précisée par l'utilisateur.
short_query	JSON	Filtre (ou critères de correspondance) associé à la portée.
appliance_id	chaîne	Identifiant unique pour l'appareil.

Renvoie l'objet de portée modifié associé à l'ID spécifié.

Exemple de code Python

```
req_payload = {
    "short_name": "App Scope Name",
    "short_query": {
        "type":"eq",
        "field":"ip",
        "value": <....>
    },
    "appliance_id": <appliance_id>,
}
resp = restclient.put('/app_scopes/%s' % <app_scope_id>,
                      json_body=json.dumps(req_payload))
```

Session inactive

Pour ceux qui s’authentifient à l’aide d’une base de données locale, cette section explique comment des tentatives de connexion infructueuses peuvent verrouiller le compte d’utilisateur :

Procedure

Étape 1 Cinq tentatives infructueuses de connexion à l’aide d’une adresse de courriel et d’un mot de passe entraînent le verrouillage du compte.

Note Par mesure de sécurité contre les tentatives de connexion malveillantes, aucun message précis indiquant le verrouillage ne s’affichera dans l’interface de connexion lorsque vous tenterez de vous connecter à un compte verrouillé.

Étape 2 La durée du verrouillage est de 30 minutes. Une fois le compte déverrouillé, utilisez le mot de passe correct pour vous connecter ou lancez la récupération du mot de passe en cliquant sur *Mot de passe oublié?*

Note Une fois que l'utilisateur s'est connecté avec succès, il est déconnecté après une heure d'inactivité. Ce délai d’expiration est configuré à partir de **Manage (Gestion)** > **Service Settings (Paramètres de service)** > **Session Configuration (Configuration de session)**.

Préférences

La page **Preferences** (Préférences) affiche les détails de votre compte et vous permet de mettre à jour vos préférences d’affichage, de modifier votre page de destination, de modifier votre mot de passe et de configurer l’authentification à deux facteurs.

Modifier vos préférences de page de destination

Pour modifier la page qui s’affiche lorsque vous vous connectez :

Procedure

Étape 1 Dans le coin supérieur droit de la fenêtre, cliquez sur l’icône d’utilisateur et choisissez **User Preferences** (Préférences de l’utilisateur).

Étape 2 Choisissez une page de destination dans le menu déroulant. Vos préférences sont enregistrées comme page d’accueil ou par défaut lorsque vous vous connectez. Pour afficher la modification, cliquez sur le logo Cisco Secure Workload dans le coin supérieur gauche de la page.

Modification d'un mot de passe

Procedure

Étape 1 Cliquez sur l'icône d'utilisateur dans le coin supérieur droit.

Étape 2 Sélectionnez **User Preferences** (Préférences utilisateur).

Étape 3 Dans le volet **Change Password** (modifier le mot de passe), saisissez votre mot de passe actuel dans le champ **Old Password** (Ancien mot de passe).

Étape 4 Saisissez votre nouveau mot de passe dans le champ **Password** (Mot de passe).

Étape 5 Saisissez votre nouveau mot de passe dans le champ **Password** (Mot de passe).

Étape 6 Cliquez sur **Change Password** (modifier le mot de passe) pour soumettre la modification.

Note **Le mot de passe doit comporter entre 8 et 128 caractères et contenir au moins un des éléments suivants :**

- Lettres minuscules (a b c d .)
- Lettres majuscules (A B C D .)
- Chiffres (0 1 2 3 4 5 6 7 8 9)
- Caractères spéciaux (! " # $ % & ’ ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ' { | } ~), espace compris

Récupération des mots de passe

Cette section explique comment récupérer votre mot de passe.

Before you begin

Pour réinitialiser un mot de passe, vous devez d’abord avoir un compte. Un nouveau compte peut être ajouté par les **administrateurs du site** et **les utilisateurs du service d'assistance à la clientèle**.

Procedure

Étape 1 Pointez votre navigateur sur l’URL Cisco Secure Workload de Cisco et cliquez sur le lien **Mot de passe oublié**. La boîte de dialogue **Mot de passe oublié?** s'affiche.

Étape 2 Saisissez votre adresse courriel dans le champ **Adresse de courriel**.

Étape 3 Cliquez sur **Réinitialiser le mot de passe**.

Des instructions de réinitialisation de mot de passe sont envoyées à votre adresse courriel.

Note La procédure de récupération du mot de passe pour l’authentification à deux facteurs nécessite de contacter le service d'assistance à la clientèle Cisco Secure Workload, car la récupération du mot de passe par courriel ne peut pas contenir le mot de passe à usage unique.

Activation de l'authentification à deux facteurs

Cette section explique comment activer l’authentification à deux facteurs.

Procedure

Étape 1 Cliquez sur l'icône d'utilisateur dans le coin supérieur droit.

Étape 2 Sélectionnez **User Preferences** (Préférences utilisateur).

Étape 3 Dans le volet **Two-factor authentication** (Authentification à deux facteurs), cliquez sur le bouton **Enable** (activer). Un nouveau volet **d’authentification à deux facteurs** s’affiche.

Étape 4 Saisissez votre mot de passe.

Étape 5 Balayez le code QR qui s’affiche dans le champ **Current Password** (Mot de passe actuel) à l’aide d’une application de mot de passe à usage unique basé sur le temps (TOTP), comme Google Authenticator (pour Android ou iOS) ou Authenticator (pour Windows Phone).

Étape 6 Saisissez le code de validation affiché par l’application TOTP de votre choix.

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

Figure 37: Volet Authentification à deux facteurs

La prochaine fois que vous vous connecterez au système, vous devrez cocher la case **Use two-factor authentication** (utiliser l'authentification à deux facteurs) et saisir le code de vérification qui s'affiche dans votre application TOTP pour vous connecter.

Note La procédure de récupération du mot de passe pour l'authentification à deux facteurs nécessite de contacter le service d'assistance à la clientèle Cisco Secure Workload, car la récupération du mot de passe par courriel ne peut pas contenir le mot de passe à usage unique.

Désactivation de l'authentification à deux facteurs

Cette section explique comment désactiver l'authentification à deux facteurs.

Procedure

Étape 1 Cliquez sur l'icône d'utilisateur dans le coin supérieur droit.

Étape 2 Sélectionnez **User Preferences** (Préférences utilisateur).

Étape 3 Sous Two-factor authentication (Authentification à deux facteurs), cliquez sur le bouton **Disable** (désactiver). Le volet **Authentification à deux facteurs** s'affiche.

Étape 4 Saisissez votre mot de passe.

Étape 5 Cliquez à nouveau sur le bouton **Disable** (désactiver).

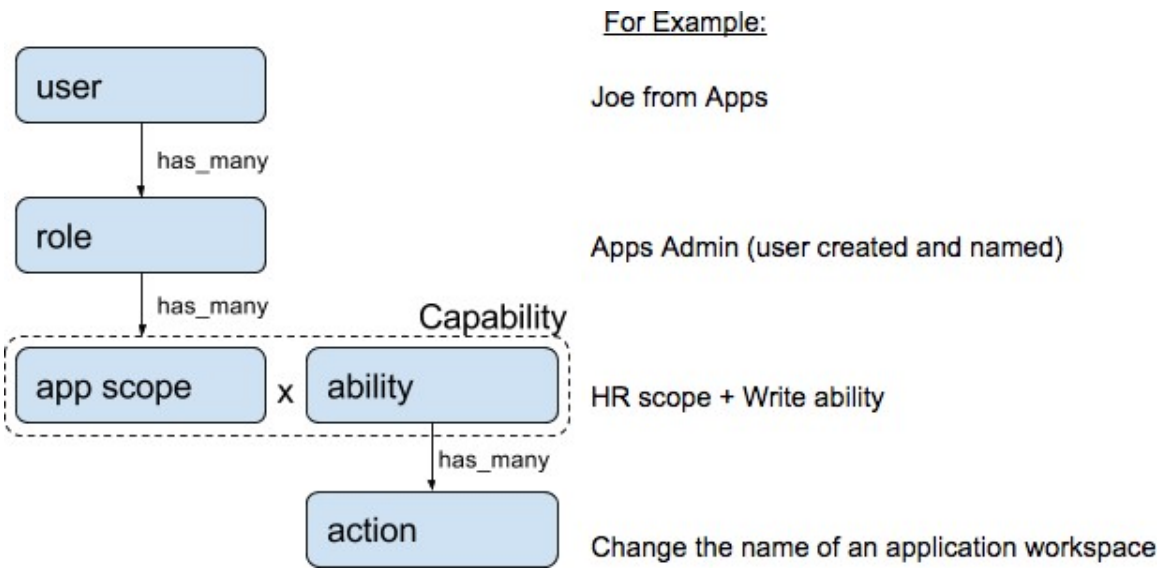
Vous ne serez plus tenu de saisir un code d'authentification à deux facteurs lors de la connexion.

Rôles

Vous pouvez restreindre l'accès aux fonctionnalités et aux données à l'aide du modèle de contrôle d'accès basé sur les rôles (RBAC).

- Utilisateur : personne avec un accès de connexion à Cisco Cisco Secure Workload.
- Rôle : ensemble de capacités créé par l'utilisateur qui est affecté à un utilisateur.
- Capability (Capacité) : couple portée + aptitude
- Ability (Aptitude) : ensembles d'actions
- Action : action de bas niveau de l'utilisateur, comme « modifier le nom de l'espace de travail »

Figure 38: Modèle de rôle



Un utilisateur peut avoir n'importe quel nombre de rôles. Les rôles peuvent avoir un nombre illimité de capacités. Par exemple, le rôle « Ingénieur de recherche en ressources humaines » pourrait avoir deux capacités :

« Lire sur la portée des ressources humaines » pour donner de la visibilité et du contexte et « Exécuter dans la fonctionnalité « Recherche RH » pour permettre aux ingénieurs ayant ce rôle d'apporter des modifications précises qui sont nécessaires. liées à leurs demandes.

Les rôles contiennent des ensembles de capacités et sont affectés aux utilisateurs dans la page **Users** (Utilisateurs). Un utilisateur peut avoir n'importe quel nombre de rôles. Les rôles peuvent avoir un nombre illimité de capacités.

Rôle	Description
Programme d'installation de l'agent	Fournir la capacité de gérer le cycle de vie des agents, y compris l'installation, la surveillance, la mise à niveau et la conversion, mais **ne pas pouvoir** supprimer les agents et accéder au profil de configuration de l'agent.
Le service d'assistance à la clientèle	Pour l'assistance technique ou les services avancés. Fournit un accès aux fonctionnalités d'entretien de la grappe. Autorise le même accès que l'administrateur du site, mais **ne peut pas** modifier les utilisateurs.
Le service d'assistance à la clientèle	Pour l'assistance technique ou les services avancés. Fournit un accès aux fonctionnalités d'entretien de la grappe. Autorise le même accès que l'administrateur du site, mais **ne peut pas** modifier les utilisateurs.
Administrateur du site	Offre la possibilité de gérer les utilisateurs, les agents, etc. Peut afficher et modifier toutes les fonctionnalités et toutes les données. Il doit y avoir au moins un administrateur de site.
Mise en application mondiale des applications	Fournit la capacité Mise en application sur chaque portée.
Gestion d'application mondiale	Fournit la capacité d'exécution sur chaque portée.
Lecture seule mondiale	Fournit la capacité de lecture sur chaque portée.

Aptitudes et capacités

Les rôles sont composés de capacités, qui comprennent une portée et une aptitude. Celles-ci définissent les actions autorisées et l'ensemble de données auquel elles s'appliquent. Par exemple, la capacité (RH, Lecture) doit être lue et interprétée comme « Capacité de lecture sur la portée des ressources humaines ». Cette fonctionnalité permet d'accéder à la portée des ressources humaines et à tous ses enfants.

Capacité	Description
Programme d'installation	Installer, surveiller et mettre à niveau les agents logiciels.
Vérification	Prendre en charge globalement la lecture des données des appareils et accéder aux journaux des modifications.
Lecture	Lire toutes les données, y compris les flux, les filtres d'application et d'inventaire.
Écriture	Apporter des modifications aux applications et aux filtres d'inventaire.
Exécuter	Exécuter Découvrir automatiquement les politiques, exécuter et publier les politiques pour analyse.

Capacité	Description
Appliquer	Appliquer les politiques définies dans les espaces de travail d'application associés à la portée donnée.
Owner (responsable)	Requis pour basculer un espace de travail d'application de secondaire à principal. Accès aux capacités d'administration des dérivations de données, comme la gestion des sessions d'application utilisateur, l'ajout de dérivations de données et la création de sources de données de visualisation.

Important Les capacités sont héritées, par exemple, la capacité d'exécution permet toutes les actions de lecture, d'écriture et d'exécution.

Important Les capacités s'appliquent à la portée et à tous ses enfants.

Accès au menu par rôle

Les menus qu'un utilisateur peut voir et utiliser dépendent du rôle qui lui est attribué :

Table 4: Menu Overview (Aperçu)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Aperçu	Aperçu	Oui	Oui	Oui	Oui	Oui	Non

Table 5: Menu Overview (Aperçu)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Aperçu	Aperçu	Oui	Oui	Oui	Oui	Oui	Oui	Non
Création de rapports	Aperçu	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 6: Menu Organize (Organiser)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Organiser	Portées et inventaire	Oui	Oui	Oui	Oui	Oui	Non
Organiser	Utiliser les étiquettes téléversées	Oui	Oui	Non	Non	Non	Non
Organiser	Filtres d'inventaire	Oui	Oui	Oui	Oui	Oui	Non

Table 7: Menu Organize (Organiser)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Organiser	Portées et inventaire	Oui	Oui	Oui	Oui	Oui	Oui	Non
Organiser	Gestion des étiquettes	Oui	Oui	Oui	Oui	Oui	Oui	Non
Organiser	Filtres d'inventaire	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 8: Menu Defend (Défendre)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Défendre	Segmentation	Oui	Oui	Oui	Oui	Non	Non
Défendre	État d'application	Oui	Oui	Non	Non	Non	Non
Défendre	Modèles de politiques	Oui	Oui	Non	Non	Non	Non

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Défendre	Règles criminalistiques	Oui	Oui	Non	Non	Non	Non

Table 9: Menu Defend (Défendre)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Défendre	Segmentation	Oui	Oui	Oui	Oui	Oui	Oui	Non
Défendre	État d'application	Oui	Oui	Oui	Oui	Oui	Oui	Non
Défendre	Modèles de politiques	Oui	Oui	Oui	Oui	Oui	Oui	Non
Défendre	Règles criminalistiques	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 10: Menu Investigate (Enquêter)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Gestion d'application mondiale	Lecture seule mondiale	Mise en application mondiale des applications	Programme d'installation de l'agent
Analyse	Trafic	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Alertes	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Vulnérabilités	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Criminalistique	Oui	Oui	Oui	Oui	Oui	Non
Analyse	Quartier	Oui	Oui	Oui	Oui	Oui	Non

Table 11: Menu Investigate (Enquêter)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Analyse	Trafic	Oui	Oui	Oui	Oui	Oui	Oui	Non
	Alertes	Oui	Oui	Oui	Oui	Oui	Oui	Non
	Vulnérabilités	Oui	Oui	Oui	Oui	Oui	Oui	Non
	Criminalistique	Oui	Oui	Oui	Oui	Oui	Oui	Non

Table 12: Menu Manage (Gestion)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Gérer	Configurations d'alertes	Oui	Oui	Oui	Oui	Oui	Oui	Non
Gérer	Journaux des modifications	Oui	Non	Oui	Non	Non	Non	Non
Gérer	Connecteurs	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Orchestrateurs externes	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Connecteur sécurisé	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Appliances virtuelles	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Utilisateurs	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Rôles	Oui	Oui	Oui	Non	Non	Non	Non
Gérer	Informations sur les menaces	Oui	Oui	Oui	Non	Non	Non	Non
Gérer	Licences	Oui	Non	Non	Non	Non	Non	Non
Gérer	Règles de collecte	Oui	Oui	Oui	Oui	Oui	Oui	Non

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Gérer	Configuration de session	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Analyse de l'utilisation	Oui	Oui	Non	Non	Non	Non	Non
Gérer	Administrateur de surveilleur de données	Oui	Non	Non	Non	Non	Non	Non

Table 13: Menu Platform (Plateforme)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Observations	Détenteurs	Oui	Oui	Non	Non	Non	Non	Non
Observations	Configuration de grappe	Oui	Oui	Non	Non	Non	Non	Non
Observations	HTTP sortant	Oui	Oui	Non	Non	Non	Non	Non
Observations	Collecteurs	Oui	Oui	Non	Non	Non	Non	Non
Observations	Authentification extérieure	Oui	Oui	Non	Non	Non	Non	Non
Observations	Certificat SSL	Oui	Oui	Non	Non	Non	Non	Non
Observations	Message de page de connexion	Oui	Oui	Non	Non	Non	Non	Non
Observations	Fédération	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non
Observations	Sauvegarde des données	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Observations	Restauration des données	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non
Observations	Mise à niveau automatique	Oui	Oui	Non	Non	Non	Non	Non

Note

- L'option Fédération est accessible pour les rôles d'administrateur du site et de service d'assistance à la clientèle si la Fédération est activée.
- Les options de sauvegarde et de restauration des données sont accessibles aux administrateurs du site et aux rôles de service d'assistance à la clientèle si la sauvegarde et la restauration des données sont activées.

Table 14: Menu Troubleshoot (Dépannage)

Menu	Option	Administrateur du site	Le service d'assistance à la clientèle	Le service d'assistance à la clientèle	Mise en application mondiale des applications	Gestion d'application mondiale	Lecture seule mondiale	Programme d'installation de l'agent
Dépanner	État du service	Oui	Oui	Oui	Non	Non	Non	Non
Dépanner	État de la grappe	Voir ci-dessous	Voir ci-dessous	Non	Non	Non	Non	Non
Dépanner	Machine virtuelle	Oui	Oui	Oui	Non	Non	Non	Non
Dépanner	Instantanés	Oui	Oui	Non	Non	Non	Non	Non
Dépanner	Explorateur de maintenance	Oui	Oui	Non	Non	Non	Non	Non
Dépanner	Resque	Oui	Oui	Non	Non	Non	Non	Non
Dépanner	Hawkeye (Graphiques)	Oui	Oui	Oui	Non	Non	Non	Non
Dépanner	Abyss (Pipeline)	Oui	Oui	Oui	Non	Non	Non	Non

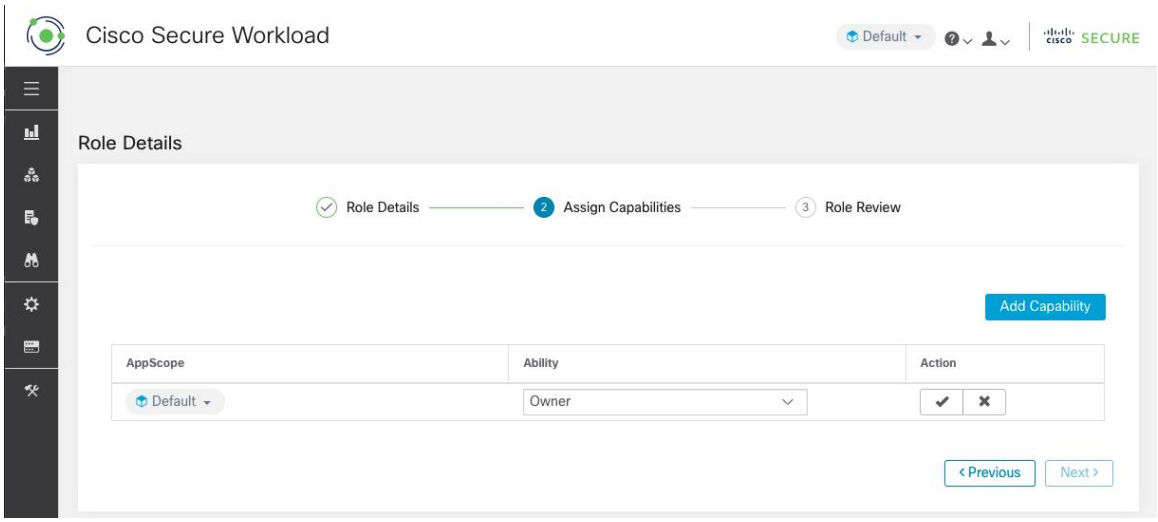
Note L'option État de la grappe est accessible aux administrateurs du site et aux rôles de service d'assistance à la clientèle selon le type de grappe.

Créer un rôle

Before you begin

Vous devez déjà avoir un rôle d' **administrateur du site** ou de service d'assistance à la clientèle.

1. Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Roles (Rôles)** .
2. Cliquez sur **Create New Role** (Créer un nouveau rôle). Le panneau **Roles** (Rôles) s'affiche.



La création d'un rôle à l'aide de l'assistant de création de rôle est un processus en trois étapes.

Procedure

Étape 1 a) Saisissez les valeurs appropriées dans les champs suivants :

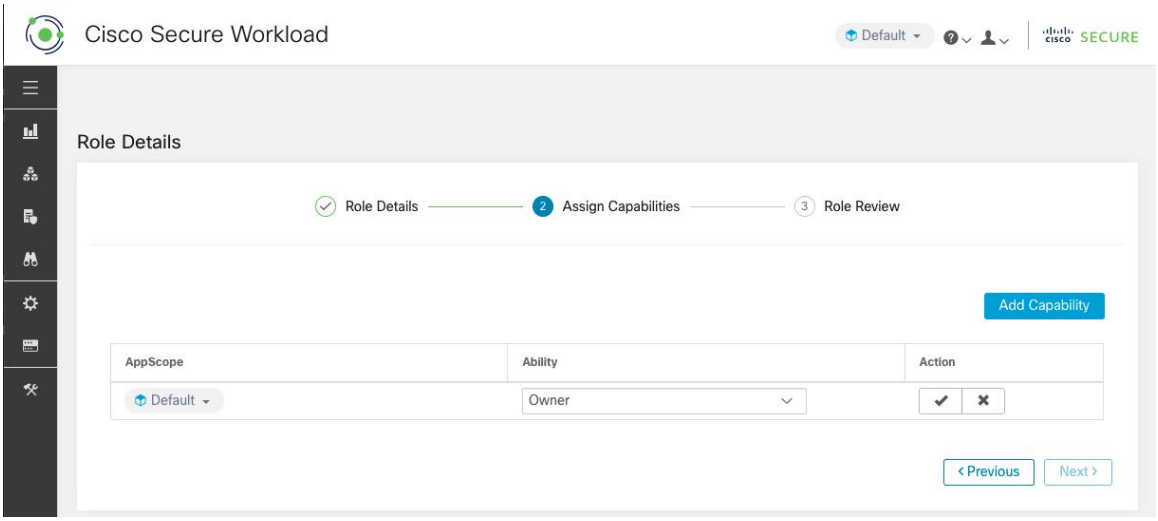
Champ	Description
Nom	Le nom pour identifier le rôle.
Description	Une brève description du rôle pour ajouter du contexte.

b) Cliquez sur le bouton **Next** (suivant) pour passer à l'étape suivante ou sur **Back to Roles Page** pour revenir à la page des rôles.

Étape 2 a) Cliquez sur le bouton **Add Capability** (ajouter une capacité) pour afficher le formulaire de création dans la rangée supérieure.

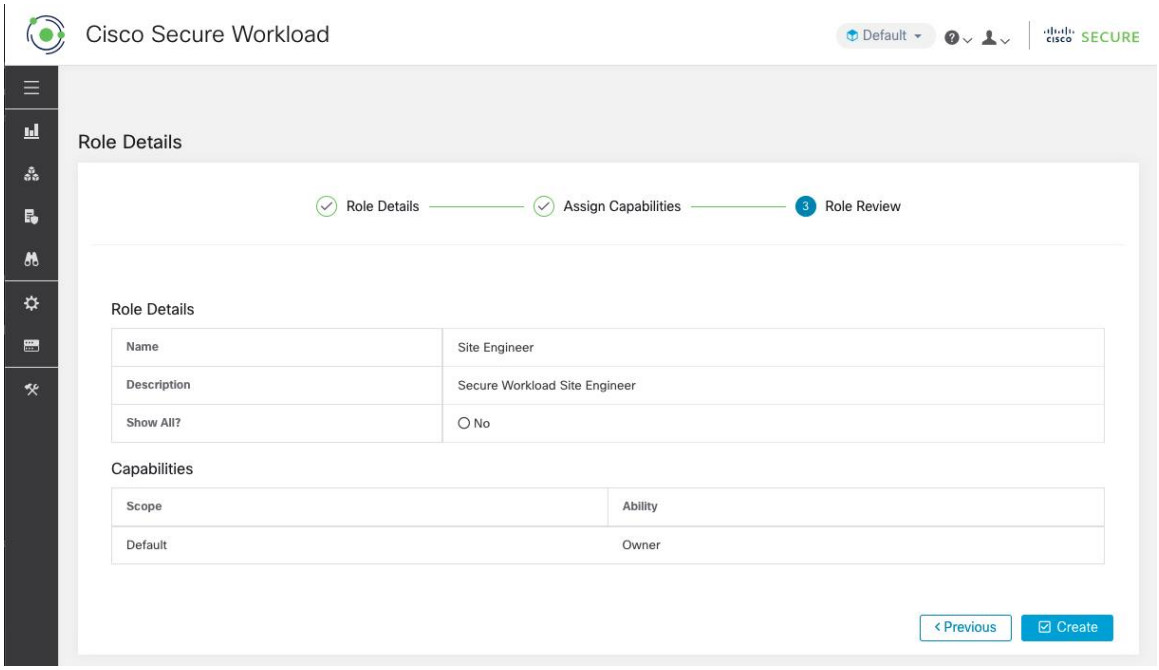
b) Sélectionnez la portée et la fonctionnalité.
c) Cliquez sur le bouton **Checkmark** (Coche) pour créer une nouvelle capacité ou sur le bouton **Cancel** (Annuler) pour annuler.
d) Cliquez sur **Next** (suivant) pour consulter les détails du rôle ou sur **Previous** (Précédent) pour revenir en arrière et modifier.

Figure 39: Affectation de capacité



Étape 3
a) Passez en revue les détails et les capacités du rôle.
b) Cliquez sur **Create** (créer) pour créer un rôle.

Figure 40: Examen du rôle



Modifier un rôle

Cette section explique comment les **administrateurs de site** et **les utilisateurs du service d'assistance à la clientèle** peuvent modifier des rôles.

Before you begin

Vous devez être l'administrateur du site ou l'utilisateur du service d'assistance à la clientèle.

1. Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Roles (Rôles)** .
2. Sur la ligne du rôle à modifier, cliquez sur le bouton **Edit** (modifier) dans la colonne de droite. Le panneau **Roles** (Rôles) s'affiche.

La modification d'un rôle à l'aide de l'assistant de modification de rôle est un processus en trois étapes.

Procedure

Étape 1

a) Mettez à jour le nom ou la description si vous le souhaitez.
b) Cliquez sur le bouton **Next** (suivant) pour passer à l'étape suivante ou sur **Back to Roles Page** pour revenir à la page des rôles.

Étape 2

a) Supprimez une capacité le cas échéant. Sur la ligne représentant la capacité à supprimer, cliquer sur l'icône **Delete** (Supprimer) dans la colonne de droite.

b) Pour en ajouter, une cliquez sur le bouton **Add Capability** (Ajouter une capacité) afin d'afficher le formulaire de création dans la rangée supérieure.
c) Sélectionnez la portée et la fonctionnalité.
d) Cliquez sur **Next** (suivant) pour consulter les détails du rôle ou sur **Previous** (Précédent) pour revenir en arrière et modifier.

Étape 3

a) Passez en revue les détails et les capacités du rôle.
b) Cliquez sur **Update** (Mettre à jour) pour créer le rôle ou sur **Previous** (Précédent) pour revenir en arrière et modifier. Les modifications apportées aux détails du rôle et à l'attribution des capacités sont enregistrées après la **mise à jour**.

Note Les capacités ne peuvent pas être modifiées, elles doivent être supprimées et recréées.

Portées

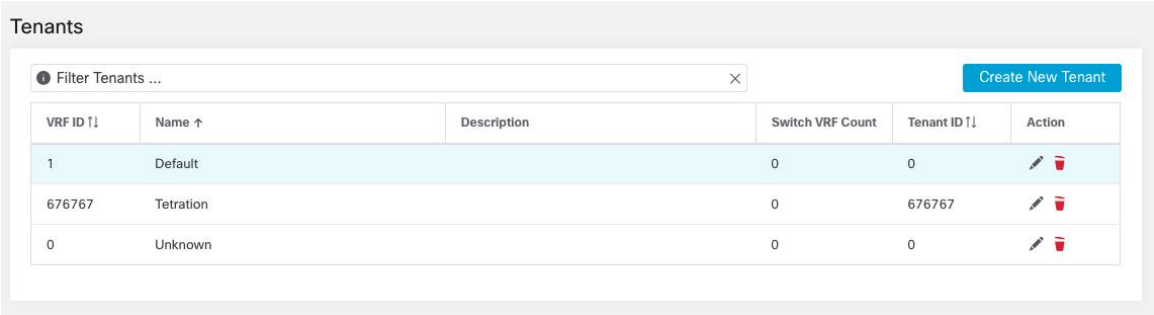
Note La page **Scopes** (Portées) est fusionnée avec **Inventory Search** (Recherche dans l'inventaire). (Pour obtenir de plus amples renseignements, consultez la page Scopes and Inventory (Portées et inventaire).

Détenteurs

Les **administrateurs du site** et les **utilisateurs du service d'assistance à la clientèle** peuvent accéder à la page **Tenants** (Détenteurs) dans le menu **Platform (Plateforme)** > **Tenants** (Détenteurs) dans le volet de navigation de gauche. La page Tenants (Détenteurs) affiche les détenteurs et les VRF actuellement configurés Cisco Secure Workload est préconfiguré avec un ou plusieurs détenteurs et VRF, et vous pouvez ajouter, modifier et supprimer des détenteurs.

Note Ces valeurs affectent les résultats de la sortie de la grappe. Nous vous recommandons de consulter le service d'assistance technique Cisco TAC avant de modifier ces valeurs pour comprendre l'incidence sur le système.

Figure 41: Page Tenants (Détenteurs)



Ajouter un détenteur

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur du **service d'assistance à la clientèle**.

Procedure

Étape 1 Dans le volet de navigation de gauche, cliquez sur **Platform(Plateforme)** > **Tenants (Détenteurs)** .

Étape 2 Cliquez sur **Créer un nouveau détenteur**.

Étape 3 Saisissez les valeurs appropriées dans les champs suivants :

Champ	Description
Nom	Saisissez le nom souhaité pour le détenteur.
Description	(Facultatif) Le champ de description contient des informations supplémentaires sur le détenteur.

Étape 4 Cliquez sur **Create** (créer).

Modifier un détenteur

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur du **service d'assistance à la clientèle**.

Procedure

Étape 1 Dans le volet de navigation de gauche, cliquez sur **Platform(Plateforme)** > **Tenants (Détenteurs)** .

Étape 2 Recherchez le locataire que vous souhaitez modifier et cliquez sur l'icône en forme de **crayon** dans la colonne de droite.

Champ	Description
Nom	Saisissez un nom pour le détenteur.
Description	(Facultatif) Mettez à jour le champ de description qui contient des informations supplémentaires sur le détenteur.
ID VRF	Affiche l'ID de ce détenteur ou VRF particulier.
Journal des modifications	Cliquez sur les icônes du journal des modifications pour afficher une nouvelle page qui affiche le journal des modifications pour le détenteur ou VRF.

Étape 3 Cliquez sur **Update** (mettre à jour).

Utilisateurs

Les administrateurs du site et les propriétaires de portée racine peuvent accéder à la page **Users** (Utilisateurs) dans le menu **Manage(Gestion)** > **User Access (Accès des utilisateurs)** dans la barre de navigation à gauche de la fenêtre.

Cette page affiche tous les utilisateurs du fournisseur de services et les utilisateurs associés à la portée dans l'en-tête de page.

Multidétenteurs

Pour prendre en charge l'architecture à détenteurs multiples, affectez les utilisateurs à une portée racine. Les utilisateurs disposant de la capacité « Propriétaire » sur la portée racine gèrent ces utilisateurs et attribuent des rôles qui sont associés à la même portée.

Les fournisseurs de services sont des utilisateurs sans portée; affectez un rôle leur permettant d'effectuer des actions dans plusieurs portées racine.

Ajouter un utilisateur

Before you begin

- Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée** pour ajouter des utilisateurs à Cisco Secure Workload.
- Si une portée multi-détenteurs est attribuée à un utilisateur, seuls les rôles attribués à la même portée peuvent être sélectionnés.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Le cas échéant, sélectionnez la portée racine appropriée dans l'en-tête de page.

Étape 2 Dans le volet de navigation, choisissez **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 3 Cliquez sur **Create New User** (Créer un nouvel utilisateur).
La page **User Details** (des détails de l'utilisateur) s'affiche.

Étape 4 Mettez à jour les champs suivants sous **User Details** (Détails sur l'utilisateur) .

Table 15: Description des champs des détails de l'utilisateur

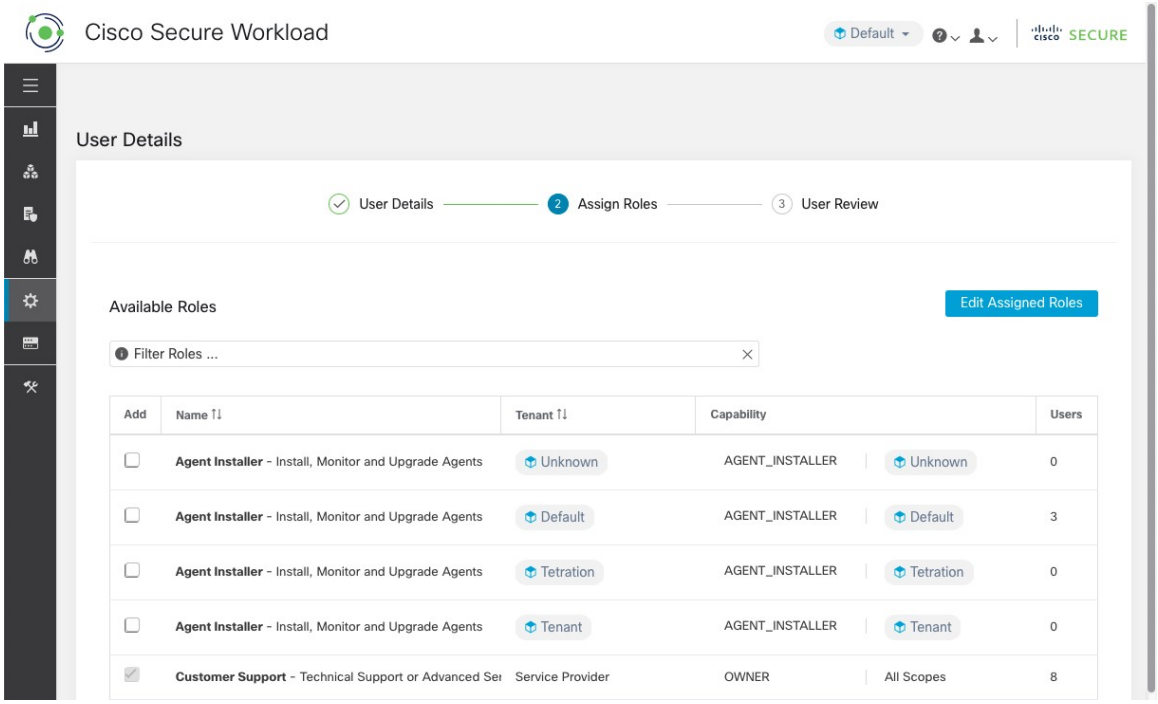
Champ	Description
Email	Saisissez l'identifiant de courriel de l'utilisateur. Il n'est pas sensible à la casse. Nous utilisons la version en lettres minuscules de votre courriel s'il contient des lettres.
Prénom	Saisissez le prénom de l'utilisateur.
Nom	Saisissez le nom de famille de l'utilisateur.
Scope	La portée racine qui est affectée à l'utilisateur pour l'architecture multidétenteurs. (Disponible pour les administrateurs du site)
Clé publique SSH	(Facultatif) Cliquez sur **Import** (importer) pour importer une clé publique SSH. Vous pouvez également en importer une ultérieurement.

Étape 5 Cliquez sur **Next** (suivant).

Étape 6 Sous **Assign Roles** (Affecter des rôles), ajoutez ou supprimez des rôles attribués à l'utilisateur.

- Cliquez sur **Add rôles** (Ajouter des rôles) pour attribuer de nouveaux rôles, puis cochez la case **Add** (ajouter).

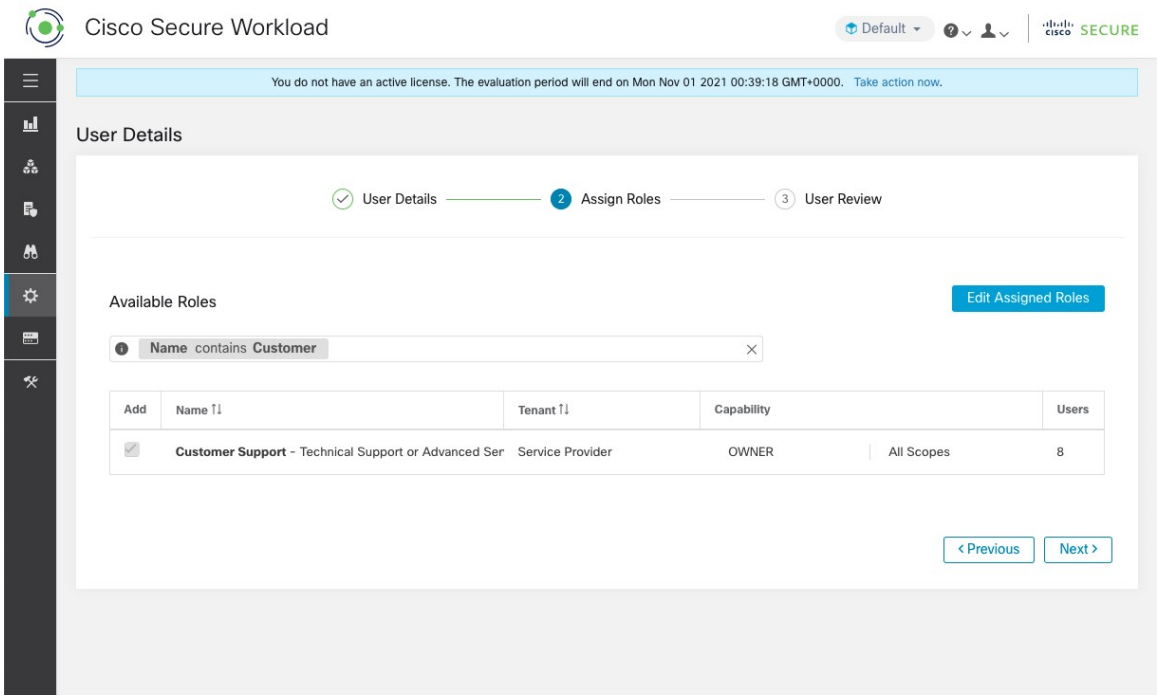
Figure 42: Rôles d'utilisateurs attribués



- Sélectionnez les rôles attribués, cliquez sur **Edit Assigned Roles** (Modifier les rôles attribués), puis cliquez sur l'icône **Remove** (Supprimer).

- Vous pouvez filtrer les rôles d'utilisateur à l'aide du **nom** ou du **détenteur**.

Figure 43: Filtrer les rôles d'utilisateur



Étape 7 Cliquez sur **Next** (suivant).

Étape 8 Sous **User Review** (Révision de l'utilisateur), vérifiez les détails de l'utilisateur et les rôles qui lui sont attribués. Cliquez sur **Create** (créer).

Si l'authentification externe est activée, les détails de l'authentification s'affichent.

Note Une fois l'utilisateur ajouté à Cisco Secure Workload, un courriel d'activation est envoyé à l'ID de courriel enregistré pour configurer le mot de passe.

Modifier les détails ou le rôle d'un utilisateur

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée racine** pour modifier des utilisateurs dans Cisco Secure Workload.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Le cas échéant, sélectionnez la portée racine appropriée dans l'en-tête de page.

Étape 2 Dans le volet de navigation, choisissez **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 3 Pour le compte d'utilisateur requis, sous **Actions**, cliquez sur **Edit** Modifier).
La page **User Details** (des détails de l'utilisateur) s'affiche.

Étape 4 Modifiez les détails suivants.

a) Mettez à jour les champs suivants sous **User Details** (Détails sur l'utilisateur) .

Table 16: Description des champs des détails de l'utilisateur

Champ	Description
Email	Mettez à jour l'identifiant de courriel de l'utilisateur.
Prénom	Mettez à jour le prénom de l'utilisateur.
Nom	Mettez à jour le nom de famille de l'utilisateur.
Scope	La portée racine qui est affectée à l'utilisateur pour l'architecture multidétenteurs. (Disponible pour les administrateurs du site)

b) Cliquez sur **Next** (suivant).

c) Sous **Assign Roles** (Affecter des rôles), ajoutez ou supprimez des rôles attribués à l'utilisateur.

- Cliquez sur **Add rôles** (Ajouter des rôles) pour attribuer de nouveaux rôles, puis cochez la case **Add** (ajouter).
- Sélectionnez les rôles attribués, cliquez sur **Edit Assigned Roles** (Modifier les rôles attribués), puis cliquez sur l'icône **Remove** (Supprimer).

d) Cliquez sur **Next** (suivant).

e) Sous **User Review** (Révision de l'utilisateur), vérifiez les détails de l'utilisateur et les rôles qui lui sont attribués. Cliquez sur **Update** (Mettre à jour) pour mettre à jour le compte d'utilisateur.

Si l'authentification externe est activée, les détails de l'authentification s'affichent.

Désactivation d'un compte d'utilisateur

Note Pour maintenir la cohérence des vérifications des journaux des modifications, les utilisateurs ne peuvent qu'être désactivés, ils ne sont pas supprimés de la base de données.

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée racine** pour ce faire.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 2 Le cas échéant, sélectionnez la portée racine appropriée dans le coin supérieur droit de la page.

Étape 3 À la ligne du compte que vous souhaitez désactiver, cliquez sur le bouton **Deactivate** (Désactiver) dans la colonne de droite.

Pour afficher les utilisateurs désactivés, utilisez le bouton à bascule **Hide Deleted Users** (Masquer les utilisateurs supprimés).

Réactivation d'un compte d'utilisateur

Si un utilisateur a été désactivé, vous pouvez le réactiver.

Before you begin

Vous devez être un **administrateur de site** ou un utilisateur **propriétaire de la portée racine** pour ce faire.

Note Cette page est filtrée en fonction de la préférence de portée sélectionnée dans l'en-tête de page.

Procedure

Étape 1 Dans la barre de navigation à gauche, cliquez sur **Manage (Gestion)** > **User Access (Accès utilisateur)** > **Users (Utilisateurs)**.

Étape 2 Le cas échéant, sélectionnez la portée racine appropriée dans le coin supérieur droit de la page.

Étape 3 Activez ou désactivez l'option **Hide Deleted Users** (Masquer les utilisateurs supprimés) pour afficher tous les utilisateurs, y compris les utilisateurs désactivés.

Étape 4 Pour le compte désactivé requis, cliquez sur **Restore** (Restaurer) dans la colonne de droite pour réactiver le compte.

Importer une clé publique SSH

Pour activer l'accès SSH en tant qu'utilisateur **ta_guest** via l'une des adresses IP de collecteur, la clé publique SSH peut être importée pour chaque utilisateur. Ce menu est uniquement disponible pour les **administrateurs de site** et les utilisateurs avec la capacité `SCOPE_OWNER` (Propriétaire de portée) sur la portée racine. La clé publique SSH expire automatiquement dans 7 jours.

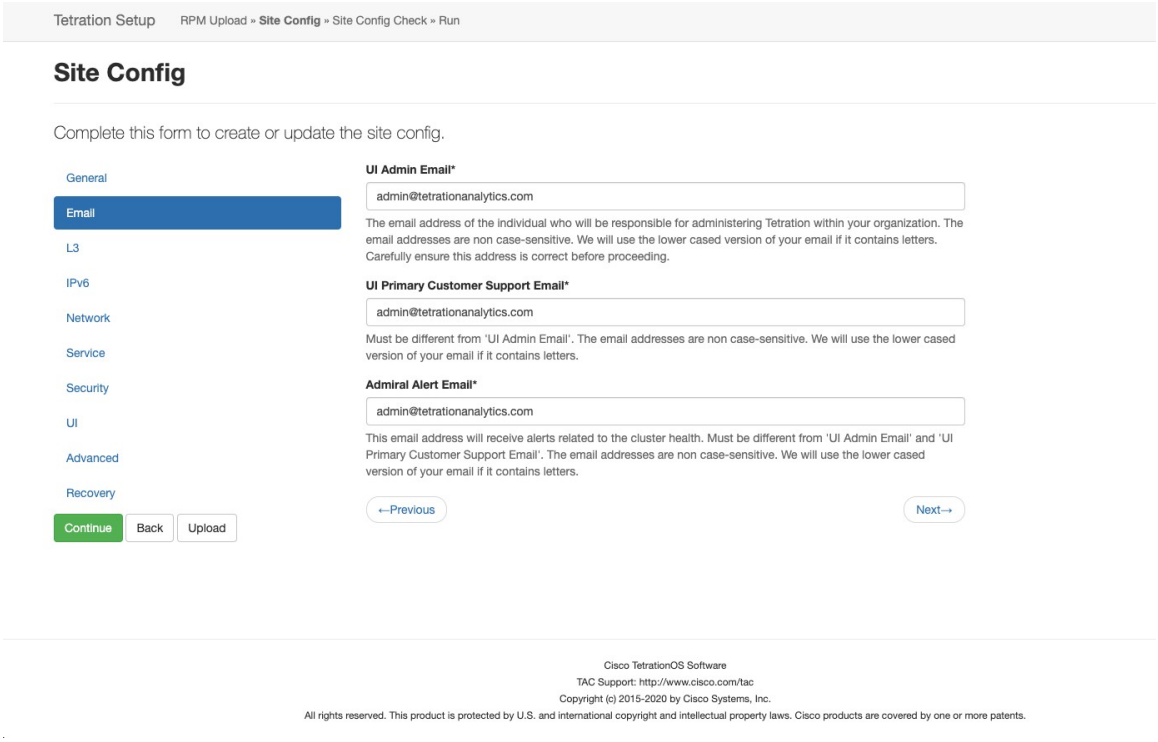
Configuration du site dans l'installation de Cisco Secure Workload

Cette section explique comment les **administrateurs de site** peuvent configurer un site pendant le processus de configuration Cisco Secure Workload.

Champ	Description
Courriel de l'administrateur 'interface utilisateur	L'adresse courriel de la personne qui sera responsable de l'administration de Cisco Secure Workload au sein de votre organisation.
Adresse courriel principale du service d'assistance à la clientèle de l'interface utilisateur	L'adresse courriel du service d'assistance principal. Doit être différent du courriel de l'administrateur de l'interface utilisateur.
Courriel d'alerte Admiral	Cette adresse courriel reçoit les alertes relatives à l'intégrité de la grappe. Doit être différent de l'adresse courriel de l'administrateur de l'interface utilisateur et de l'adresse courriel du service d'assistance à la clientèle principal de l'interface utilisateur.

Les adresses courriel ne sont pas sensibles à la casse. Nous utilisons la version en minuscules de votre courriel s'il contient des lettres.

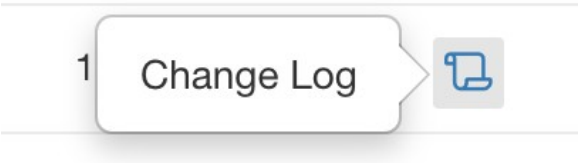
Figure 44: Configurer les courriels d'alerte de l'administrateur de l'interface utilisateur, du service d'assistance à la clientèle principal et de l'administrateur Admiral



Journal des modifications : Utilisateurs

Les **administrateurs de site** et les utilisateurs qui ont la capacité `SCOPE_OWNER` (PROPRIÉTAIRE_PORTÉE) sur la portée racine peuvent afficher les journaux des modifications pour chaque utilisateur en cliquant sur l'icône dans la colonne **Actions**, comme l'illustre la figure suivante.

Figure 45: Journal des modifications



Pour en savoir plus sur le **journal des modifications**, consultez le Journal des modifications. Les propriétaires de la portée racine peuvent uniquement afficher les entrées du journal des modifications pour les entités appartenant à leur portée.

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.