Acquérir les informations d'authentification de l'utilisateur final

Cette rubrique contient les sections suivantes :

Survol de l'acquisition des informations d'authentification de l'utilisateur final

Type de serveur/domaine	Schéma d'authentification	Protocole réseau pris en charge	Notes
Active Director	Kerberos NTLMSSP Basic (niveau de base)	HTTP, HTTPS FTP natif, FTP sur HTTP SOCKS (Authentification de base)	Kerberos n'est pris en charge qu'en mode standard. Il n'est pas pris en charge en mode Cloud Connector.
LDAP	Basic (niveau de base)	HTTP, HTTPS FTP natif, FTP sur HTTP SOCKS	—

Survol des tâches d'authentification

Étape	Tâche	Liens vers des rubriques et des procédures connexes
1	Créez un domaine d'authentification.	• Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique), on page 22 • Création d'un domaine d'authentification LDAP, on page 25
2	Configurez des paramètres d'authentification globaux.	• Configuration des paramètres d'authentification globaux, on page 31
3	Configurez l'authentification extérieure. Vous pouvez authentifier les utilisateurs au moyen d'un serveur LDAP ou RADIUS externe.	• Authentification extérieure, on page 16
4	(Facultatif) Créez et organisez des domaines d'authentification supplémentaires. Créez au moins un domaine d'authentification pour chaque combinaison de protocole et de schéma d'authentification que vous prévoyez d'utiliser.	• Création de séquences d'authentification, on page 40
5	(Facultatif) Configurez le chiffrement des informations d'authentification.	• Configuration du chiffrement des informations d'authentification, on page 49
6	Créer des profils d'identification pour classer les utilisateurs et les logiciels clients en fonction des exigences d'authentification.	• Classification des utilisateurs et logiciels clients
7	Créez des politiques pour gérer les demandes Web provenant des utilisateurs et groupes d'utilisateurs pour lesquels vous avez créé des profils d'identification.	• Bonnes pratiques en matière de gestion des demandes Web au moyen de politiques

Bonnes pratiques en matière d'authentification

- Créez aussi peu de domaines Active Directory que possible. Plusieurs domaines Active Directory nécessitent une utilisation de mémoire supplémentaire pour l'authentification.
- Si vous utilisez NTLMSSP, authentifiez les utilisateurs à l'aide de Secure Web Appliance ou du serveur proxy en amont, mais pas des deux. (Recommander Secure Web Appliance)
- Si vous utilisez Kerberos, authentifiez-vous à l'aide de Secure Web Appliance.
- Pour des performances optimales, authentifiez les clients sur le même sous-réseau à l'aide d'un seul domaine.

- Certains agents utilisateurs sont connus pour avoir des problèmes avec les informations d'authentification de l'ordinateur ou des échecs d'authentification, ce qui peut avoir une incidence négative sur leurs opérations normales. Vous devez contourner l'authentification avec ces agents utilisateurs. Consultez Contournement de l'authentification avec des agents utilisateur problématiques , on page 42.
- L'authentification active d'un client est une tâche exigeante en ressources. Les substitutions d'authentification peuvent être utilisées pour améliorer les performances d'authentification en se souvenant d'un utilisateur authentifié pendant un certain temps (par défaut 3600 secondes et configurable dans [**Global Authentication** > **Surrogate Timeout** (Authentification globale > Expiration des substitutions)]) une fois l'authentification terminée. Les substitutions IP doivent être utilisées chaque fois que possible pour limiter le nombre d'événements d'authentification actifs.

Planification de l'authentification

Active Directory/Kerberos

Renvoi explicite	Mise en cache transparente basée sur IP	Mise en cache transparente basée sur les témoins
Avantages : • Performance et interopérabilité améliorées par rapport à NTLM • Fonctionne avec les clients Windows et non Windows qui ont rejoint le domaine • Pris en charge par tous les navigateurs et la plupart des autres applications • Basé sur les RFC • Surcharge minimale (la réauthentification n'est pas requise) • Fonctionne pour les demandes HTTPS (CONNECT) • Comme la phrase secrète n'est pas transmise au serveur d'authentification, elle est encore plus sécurisée • La connexion est authentifiée, pas l'hôte ou l'adresse IP • Réalise une véritable connexion unique dans un environnement Active Directory lorsque les applications clientes sont configurées pour faire confiance au Secure Web Appliance	**Avantages :** • Performance et interopérabilité améliorées par rapport à NTLM • Fonctionne avec les clients Windows et non Windows qui ont rejoint le domaine • Fonctionne avec tous les principaux navigateurs • Pour le cas des agents utilisateur qui ne prennent pas en charge l'authentification, les utilisateurs doivent seulement s'authentifier dans un navigateur pris en charge. • Surdébit relativement faible • Fonctionne pour les demandes HTTPS si l'utilisateur s'est déjà authentifié avec une requête HTTP	**Avantages** : • Performance et interopérabilité améliorées par rapport à NTLM • Fonctionne avec les clients Windows et non Windows qui ont rejoint le domaine • Fonctionne avec tous les principaux navigateurs • L'authentification est associée à l'utilisateur plutôt qu'à l'hôte ou à l'adresse IP **Inconvénients** : • Chaque nouveau domaine Web nécessite l'ensemble du processus d'authentification, car les témoins sont propres au domaine • Nécessite l'activation des témoins • Ne fonctionne pas pour les demandes HTTPS

Active Directory/Basique

Renvoi explicite	Mise en cache transparente basée sur IP	Mise en cache transparente basée sur les témoins
Avantages : • Pris en charge par tous les navigateurs et la plupart des autres applications • Basé sur les RFC • Surcharge minimale • Fonctionne pour les demandes HTTPS (CONNECT) • Comme la phrase secrète n'est pas transmise au serveur d'authentification, elle est encore plus sécurisée • La connexion est authentifiée, pas l'hôte ou l'adresse IP • Réalise une véritable connexion unique dans un environnement Active Directory lorsque les applications clientes sont configurées pour faire confiance au Secure Web Appliance **Inconvénients** : • Phrase secrète envoyée en texte clair (Base64) pour chaque demande • Absence de connexion unique • Surdébit modéré : chaque nouvelle connexion doit être réauthentifiée • Principalement pris en charge sur Windows uniquement et avec les principaux navigateurs uniquement	**Avantages :** • Fonctionne avec tous les principaux navigateurs • Pour le cas des agents utilisateur qui ne prennent pas en charge l'authentification, les utilisateurs doivent seulement s'authentifier dans un navigateur pris en charge. • Surdébit relativement faible • Fonctionne pour les demandes HTTPS si l'utilisateur s'est déjà authentifié avec une requête HTTP **Inconvénients** : • Les informations d'authentification sont associées à l'adresse IP, pas à l'utilisateur (ne fonctionne pas dans les environnements Citrix et RDP ou si l'utilisateur change d'adresse IP) • Absence de connexion unique • La phrase secrète est envoyée en texte clair (Base64)	**Avantages** : • Fonctionne avec tous les principaux navigateurs • L'authentification est associée à l'utilisateur plutôt qu'à l'hôte ou à l'adresse IP **Inconvénients** : • Chaque nouveau domaine Web nécessite l'ensemble du processus d'authentification, car les témoins sont propres au domaine • Nécessite l'activation des témoins • Ne fonctionne pas pour les demandes HTTPS • Absence de connexion unique • La phrase secrète est envoyée en texte clair (Base64)

Active Directory/NTLMSSP

Renvoi explicite	Transparent
Avantages : • Comme la phrase secrète n'est pas transmise au serveur d'authentification, elle est encore plus sécurisée • La connexion est authentifiée, pas l'hôte ou l'adresse IP • Réalise une véritable connexion unique dans un environnement Active Directory lorsque les applications clientes sont configurées pour faire confiance au Secure Web Appliance **Inconvénients :** • Surdébit modéré : chaque nouvelle connexion doit être réauthentifiée • Principalement pris en charge sur Windows uniquement et avec les principaux navigateurs uniquement	**Avantages :** • Plus de flexibilité L'authentification NTLMSSP transparente est similaire à l'authentification de base transparente, sauf que le proxy Web communique avec les clients à l'aide d'un processus de test-réponse au lieu du nom d'utilisateur et de la phrase secrète de base en texte clair. Les avantages et les inconvénients de l'authentification MSTN transparente sont les mêmes que ceux de l'authentification de base transparente, sauf qu'elle présente l'avantage supplémentaire de ne pas envoyer de phrase secrète au serveur d'authentification et que vous pouvez réaliser une connexion unique lorsque les applications clientes sont configurées pour faire confiance à Secure Web Appliance**.**

LDAP/Basic

Renvoi explicite	Transparent
Avantages : • Basé sur les RFC • Davantage de navigateurs pris en charge que NTLM • Surcharge minimale • Fonctionne pour les demandes HTTPS (CONNECT) **Inconvénients :** • Absence de connexion unique • Phrase secrète envoyée en texte clair (Base64) pour chaque demande **Solutions :** • Échec de l'authentification, on page 41	**Avantages :** • Plus flexible que le renvoi explicite. • Davantage de navigateurs pris en charge que NTLM • Pour le cas des agents utilisateur qui ne prennent pas en charge l'authentification, les utilisateurs doivent seulement s'authentifier dans un navigateur pris en charge. • Surdébit relativement faible • Fonctionne pour les demandes HTTPS si l'utilisateur s'est déjà authentifié avec une requête HTTP **Inconvénients :** • Absence de connexion unique • La phrase secrète est envoyée en texte clair (Base64) • Les informations d'authentification sont associées à l'adresse IP, pas à l'utilisateur (ne fonctionne pas dans les environnements Citrix et RDP ou si l'utilisateur change d'adresse IP) **Solutions :** • Échec de l'authentification, on page 41

Identification transparente des utilisateurs

Habituellement, les utilisateurs sont identifiés et authentifiés en les invitant à saisir un nom d'utilisateur et une phrase secrète. Ces informations d'authentification sont validées par rapport à un serveur d'authentification, puis le proxy Web applique les politiques appropriées à la transaction en fonction du nom d'utilisateur authentifié.

Cependant, vous pouvez configurer Secure Web Appliance pour authentifier les utilisateurs de manière transparente, c'est-à-dire sans demander à l'utilisateur final de fournir ses informations d'authentification. L'identification transparente authentifie l'utilisateur au moyen d'informations d'authentification obtenues à partir d'une autre source de confiance, en supposant que l'utilisateur a déjà été authentifié par cette source de confiance, puis applique les politiques appropriées.

Vous pourriez souhaiter identifier les utilisateurs de manière transparente pour :

- Créer un environnement de connexion unique de sorte que les utilisateurs ne soient pas informés de la présence d'un proxy sur le réseau.
- Appliquer des politiques basées sur l'authentification aux transactions émanant d'applications clientes qui sont incapables d'afficher une invite d'authentification aux utilisateurs finaux.

L'identification transparente des utilisateurs affecte uniquement la façon dont le proxy Web obtient le nom d'utilisateur et attribue un profil d'identification. Après avoir obtenu le nom d'utilisateur et attribué un profil d'identification, il applique normalement toutes les autres politiques, quelle que soit la façon dont il a attribué le profil d'identification.

Si l'authentification transparente échoue, vous pouvez configurer le traitement de la transaction : vous pouvez accorder à l'utilisateur un accès invité ou forcer l'affichage d'une invite d'authentification à l'attention de l'utilisateur.

Lorsqu'une invite d'authentification apparaît à un utilisateur final en raison d'un échec de l'identification transparente de l'utilisateur et que l'authentification échoue en raison d'informations d'authentification non valides, vous pouvez choisir d'autoriser ou non l'accès de l'utilisateur invité.

Note Lorsque vous activez la réauthentification et qu'une transaction est bloquée par le filtrage d'URL, une page de notification à l'utilisateur final s'affiche avec l'option de connexion sous un autre nom d'utilisateur. Les utilisateurs qui cliquent sur le lien sont invités à s'authentifier. Pour en savoir plus, consultez Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes, on page 45.

Comprendre l'identification transparente de l'utilisateur

Les méthodes disponibles pour l'identification transparente de l'utilisateur sont les suivantes :

- **Transparently identify users with ISE** (Identifier en toute transparence les utilisateurs avec ISE) : disponible lorsque le service de moteur de services de vérification des identités (ISE) ou du connecteur d'identité passif (ISE-PIC) est activé [Network > Identity Services Engine (Réseau > Moteur ISE)]. Pour ces transactions, le nom d'utilisateur et les étiquettes Groupe sécurisé associées seront obtenus à partir d'un serveur de moteur de services d'identité. Si vous utilisez ISE-PIC, on obtiendra le nom d'utilisateur et les groupes ISE Secure associés. Consultez Tâches relatives à l'intégration du service ISE/ISE-PIC.
- **Transparently identify users with ASA** (Identification transparente des utilisateurs avec ASA) : les utilisateurs sont identifiés par le mappage adresse IP actuel-nom d'utilisateur reçu d'une appliance Cisco Adaptive Security Appliance (pour les utilisateurs à distance seulement). Cette option est disponible lorsqu'AnyConnect Secure Mobility est activé et intégré à un ASA. Le nom d'utilisateur sera obtenu auprès de l'ASA, et les groupes d'annuaires associés seront obtenus à partir du domaine ou de la séquence d'authentification précisée sur la Secure Web Appliance. Consultez Utilisateurs à distance.
- **Transparently identify users with authentication realms** (Identification transparente des utilisateurs avec des domaines d'authentification) : cette option est disponible lorsqu'un ou plusieurs domaines d'authentification sont configurés pour prendre en charge l'identification transparente à l'aide de l'un des serveurs d'authentification suivants :
  - **Active Directory** : crée un domaine d'authentification NTLM ou Kerberos et active une identification transparente des utilisateurs. En outre, vous devez déployer un agent Active Directory distinct comme l'agent Context Directory de Cisco. Pour en savoir plus, consultez Identification transparente de l'utilisateur avec Active Directory, on page 9.
  - **LDAP** : crée un domaine d'authentification LDAP configuré comme un eDirectory et active une identification transparente des utilisateurs. Pour en savoir plus, consultez Identification transparente de l'utilisateur avec LDAP, on page 10.

AsyncOS pour le Web communique à des intervalles réguliers avec eDirectory ou un agent Active Directory pour maintenir les mappages qui font correspondre les noms d'utilisateurs authentifiés à leurs adresses IP actuelles.

Identification transparente de l'utilisateur avec Active Directory

Active Directory n'enregistre pas les informations de connexion de l'utilisateur dans un format permettant aux autres systèmes d'interroger facilement d'autres systèmes, par exemple Secure Web Appliance. Les agents Active Directory, tels que l'agent Context Directory Agent (CDA) de Cisco, sont nécessaires pour interroger les journaux des événements de sécurité Active Directory pour obtenir des renseignements sur les utilisateurs authentifiés.

Note CDA n'est pas pris en charge par Active Directory dans Windows Server 2016. Vous pouvez utiliser le service ISE (Identity Services Engine - Moteur du service de vérification des identités) ou ISE-PIC (ISE Passive Identity Controller) pour recevoir les informations de l'utilisateur et obtenir une identification transparente de l'utilisateur. Vous devez configurer les profils d'identification et les politiques d'accès pertinentes, ainsi que les politiques de déchiffrement qui utilisent CDA, avec les informations ISE/ISE-PIC lorsque vous passez de CDA à ISE/ISE-PIC.

AsyncOS pour le Web communique avec l'agent Active Directory pour conserver une copie locale des mappages adresse IP-nom d'utilisateur. Quand AsyncOS pour le Web doit associer une adresse IP à un nom d'utilisateur, il vérifie d'abord sa copie locale des mappages. Si aucune correspondance n'est trouvée, il interroge un agent Active Directory pour trouver une correspondance.

Pour en savoir plus sur l'installation et la configuration d'un agent Active Directory, consultez la section « Configuration d'un agent Active Directory pour fournir des informations à Secure Web Appliance » ci-dessous.

Prenez en compte les éléments suivants lorsque vous identifiez les utilisateurs de manière transparente à l'aide d'Active Directory :

- L'identification transparente des utilisateurs avec Active Directory fonctionne uniquement avec un schéma d'authentification NTLM ou Kerberos. Vous ne pouvez pas l'utiliser avec un domaine d'authentification LDAP qui correspond à une instance Active Directory.
- L'identification transparente de l'utilisateur fonctionne avec les versions d'Active Directory prises en charge par un agent Active Directory.
- Vous pouvez installer une deuxième instance d'un agent Active Directory sur un autre ordinateur pour atteindre une disponibilité élevée. Lorsque vous faites cela, chaque agent Active Directory gère les mappages de l'adresse IP au nom d'utilisateur indépendamment de l'autre agent. AsyncOS pour le Web utilise l'agent Active Directory de secours après trois tentatives ping infructueuses vers l'agent principal.
- L'agent Active Directory utilise le mode à la demande lorsqu'il communique avec Secure Web Appliance.
- L'agent Active Directory envoie les informations de déconnexion de l'utilisateur vers Secure Web Appliance. Parfois, certaines informations de déconnexion d'utilisateurs ne sont pas enregistrées dans les journaux de sécurité Active Directory. Cela peut se produire si l'ordinateur client tombe en panne ou si l'utilisateur éteint l'appareil sans se déconnecter. Si les journaux de sécurité ne contiennent aucune information de déconnexion de l'utilisateur, un agent Active Directory ne peut pas informer l'appliance que l'adresse IP n'est plus attribuée à cet utilisateur. Pour éviter cette possibilité, vous pouvez définir pendant combien de temps AsyncOS met en cache les mappages adresse IP-utilisateur lorsqu'il n'y a aucune mise à jour d'un agent Active Directory. Pour en savoir plus, consultez Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur, on page 12.

- L'agent Active Directory enregistre le nom `sAMAccountName` de chaque utilisateur se connectant à partir d'une adresse IP particulière afin de s'assurer que le nom d'utilisateur est unique.
- Les adresses IP des clients que les ordinateurs clients présentent au serveur Active Directory et au Secure Web Appliance doivent être identiques.
- AsyncOS pour le Web recherche uniquement les groupes parents directs pour un utilisateur. Il ne recherche pas les groupes imbriqués.

Configuration d'un agent Active Directory pour fournir des informations à Secure Web Appliance

Comme AsyncOS pour le Web ne peut pas obtenir les adresses IP des clients directement à partir d'Active Directory, il doit obtenir les informations de mappage adresse IP-nom d'utilisateur auprès d'un agent Active Directory.

Installez un agent Active Directory sur un ordinateur du réseau qui est accessible à Secure Web Appliance et qui peut communiquer avec tous les contrôleurs de domaine Windows visibles. Pour de meilleures performances, cet agent doit être physiquement aussi proche que possible de Secure Web Appliance. Dans les environnements réseau plus petits, vous pouvez installer l'agent Active Directory directement sur le serveur Active Directory.

Note L'instance de l'agent Active Directory utilisée pour communiquer avec Secure Web Appliance peut également prendre en charge d'autres appliances, y compris l'appliance ASA (Adaptive Security Appliance) de Cisco et d'autres Secure Web Appliance.

Obtention, installation et configuration de l'agent Context Directory Agent de Cisco

Pour en savoir plus sur le téléchargement, l'installation et la configuration de l'agent Cisco Context Directory, consultez l'adresse suivante :
http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html.

Note Secure Web Appliance et l'agent Active Directory communiquent à l'aide du protocole RADIUS. L'appliance et l'agent doivent être configurés avec le même secret partagé pour brouiller les phrases secrètes des utilisateurs. Les autres attributs utilisateur ne sont pas masqués.

Identification transparente de l'utilisateur avec LDAP

AsyncOS pour le Web peut communiquer avec un serveur eDirectory configuré comme domaine LDAP (Lightweight Directory Access Protocol) en maintenant les mappages de l'adresse IP sur le nom d'utilisateur. Lorsqu'un utilisateur se connecte par l'intermédiaire d'un client eDirectory, il est authentifié sur le serveur eDirectory. Une fois l'authentification réussie, l'adresse IP du client est enregistrée sur le serveur eDirectory en tant qu'attribut (NetworkAddress) de l'utilisateur qui s'est connecté.

Tenez compte des éléments suivants lorsque vous identifiez les utilisateurs de manière transparente à l'aide de LDAP (eDirectory) :

- Le client eDirectory doit être installé sur chaque poste de travail client et les utilisateurs finaux doivent l'utiliser pour s'authentifier sur un serveur eDirectory.

- L'arborescence LDAP utilisée par la connexion du client eDirectory doit être la même que celle configurée dans le domaine d'authentification.
- Si les clients eDirectory utilisent plusieurs arborescences LDAP, créez un domaine d'authentification pour chaque arborescence, puis créez une séquence d'authentification qui utilise chaque domaine d'authentification LDAP.
- Lorsque vous configurez le domaine d'authentification LDAP en tant que domaine eDirectory, vous devez préciser un ND de liaison pour les informations d'authentification de requête.
- Le serveur eDirectory doit être configuré pour mettre à jour l'attribut NetworkAddress de l'objet utilisateur lorsqu'un utilisateur se connecte.
- AsyncOS pour le Web recherche uniquement les groupes parents directs pour un utilisateur. Il ne recherche pas les groupes imbriqués.
- Vous pouvez utiliser l'attribut NetworkAddress pour un utilisateur eDirectory afin de déterminer l'adresse IP de connexion la plus récente de l'utilisateur.

Règles et directives pour une identification transparente de l'utilisateur

Tenez compte des règles et directives suivantes lorsque vous utilisez une identification transparente de l'utilisateur avec un serveur d'authentification :

- Lorsque vous utilisez DHCP pour affecter des adresses IP aux ordinateurs clients, vérifiez que les mappages adresse IP-nom d'utilisateur sont mis à jour sur Secure Web Appliance plus fréquemment que le bail DHCP. Utilisez la commande de l'interface de ligne de commande `tuiconfig` pour mettre à jour l'intervalle de mise à jour du mappage. Pour en savoir plus, consultez Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur, on page 12.
- Si un utilisateur se déconnecte d'une appliance et qu'un autre utilisateur se connecte à la même appliance avant la mise à jour du mappage adresse IP-nom d'utilisateur sur le Secure Web Appliance, le proxy Web connecte le client en tant qu'utilisateur précédent.
- Vous pouvez configurer la façon dont le proxy Web traite les transactions en cas d'échec de l'identification transparente de l'utilisateur. Il peut accorder aux utilisateurs un accès invité ou forcer l'affichage d'une invite d'authentification pour les utilisateurs finaux.
- Lorsqu'une invite d'authentification s'affiche en raison d'un échec de l'identification transparente de l'utilisateur et que l'authentification échoue en raison de l'échec de l'identification transparente de l'utilisateur, vous pouvez choisir d'autoriser ou non l'accès de l'utilisateur en tant qu'invité.
- Lorsque le profil d'identification attribué utilise une séquence d'authentification avec plusieurs domaines dans lesquels l'utilisateur existe, AsyncOS pour le Web récupère les groupes d'utilisateurs des domaines dans l'ordre dans lequel ils apparaissent dans la séquence.
- Lorsque vous configurez un profil d'identification pour identifier les utilisateurs de manière transparente, le modèle d'authentification doit être l'adresse IP. Vous ne pouvez pas sélectionner un type de substitution différent.
- Lorsque vous affichez le détail des transactions pour les utilisateurs, la page de suivi Web indique quels utilisateurs ont été identifiés de manière transparente.
- Vous pouvez consigner les utilisateurs qui ont été identifiés de manière transparente dans les journaux d'accès et WC3 à l'aide des champs personnalisés `%m` et `x-auth-mecanism`. Une entrée de journal `SSO_TUI` indique que le nom d'utilisateur a été obtenu en faisant correspondre l'adresse IP du client à un nom d'utilisateur authentifié à l'aide d'une identification transparente de l'utilisateur. (De même, la valeur

`SSO_ASA` indique que l'utilisateur est un utilisateur distant et que le nom d'utilisateur a été obtenu auprès d'un Cisco ASA à l'aide d'AnyConnect Secure Mobility.)

Configuration de l'identification transparente de l'utilisateur

La configuration de l'identification et de l'autorisation transparentes des utilisateurs est décrite en détail dans Survol de l'acquisition des informations d'authentification de l'utilisateur final, on page 1. Les étapes élémentaires sont les suivantes :

- Créer et trier les domaines d'authentification.
- Créer des profils d'identification pour classer les utilisateurs et les logiciels clients.
- Créer des politiques pour gérer les demandes Web émanant des utilisateurs et groupes d'utilisateurs identifiés.

Utilisation de l'interface de ligne de commande pour configurer les paramètres d'identification transparente avancée de l'utilisateur

AsyncOS pour le Web fournit les commandes CLI suivantes liées à l'interface TUI :

- **`tuiconfig`** – Configurez les paramètres avancés associés à l'identification transparente de l'utilisateur. Le mode par lots peut être utilisé pour configurer plusieurs paramètres simultanément.
  - **`Configure mapping timeout for Active Directory agent`** (Configurer le délai d'expiration de mappage pour l'agent Active Directory) : durée, en minutes, pendant laquelle les mappages adresse IP-utilisateur sont mis en cache pour les adresses IP récupérées par l'agent AD quand aucune mise à jour de l'agent n'est effectuée.
  - **`Configure proxy cache timeout for Active Directory agent`** (Configurer le délai d'expiration du cache de proxy pour l'agent Active Directory) : durée, en secondes, pendant laquelle les mappages adresse IP-utilisateur spécifiques au proxy sont mis en cache, en secondes; les valeurs correctes vont de cinq à 1200 secondes. La valeur par défaut et recommandée est de 120 secondes. La définition d'une valeur inférieure peut avoir un impact négatif sur les performances du proxy.
  - **`Configure mapping timeout for Novell eDirectory`** (Configurer le délai de mappage pour Novell eDirectory) : durée, en secondes, pendant laquelle les mappages adresse IP-utilisateur sont mis en cache pour les adresses IP extraites du serveur eDirectory quand aucune mise à jour n'est effectuée à partir du serveur.
  - **`Configure query wait time for Active Directory agent`** (Configurer le temps d'attente de la requête pour l'agent Active Directory) : temps, en secondes, d'attente d'une réponse de l'agent Active Directory. Lorsque la requête prend plus de temps que cette valeur, l'identification transparente de l'utilisateur est considérée comme ayant échoué. Cela limite le délai d'authentification de l'utilisateur final.
  - **`Configure query wait time for Novell eDirectory`** (Configurer le temps d'attente de la requête pour Novell eDirectory) : temps, en secondes, d'attente d'une réponse du serveur eDirectory. Lorsque la requête prend plus de temps que cette valeur, l'identification transparente de l'utilisateur est considérée comme ayant échoué. Cela limite le délai d'authentification de l'utilisateur final.

Les paramètres Active Directory s'appliquent à tous les domaines AD qui utilisent un agent AD pour l'identification transparente de l'utilisateur. Les paramètres eDirectory s'appliquent à tous les domaines LDAP qui utilisent eDirectory pour l'identification transparente des utilisateurs.

Si la validation échoue pour un paramètre, aucune valeur ne sera modifiée.

- **tuistatus** : cette commande fournit les sous-commandes liées à AD suivantes :
  - **adagentstatus** : affiche l'état actuel de tous les agents AD, ainsi que des informations sur leurs connexions avec les contrôleurs de domaine Windows.
  - **listlocalmaippings** : répertorie tous les mappages adresse IP-nom d'utilisateur stockés sur le Secure Web Appliance, tels qu'ils ont été récupérés par le ou les agents AD. Ce paramètre ne répertorie pas les entrées stockées sur le ou les agents, ni les mappages pour lesquels des requêtes sont actuellement en cours.

Configuration de la connexion unique

L'obtention des informations d'authentification facilite la création d'un environnement de connexion unique en toute transparence. L'identification transparente de l'utilisateur est un paramètre du domaine d'authentification.

Pour Internet Explorer, assurez-vous que le nom d'hôte de redirection est le nom d'hôte court (ne contenant pas de points) ou le nom NetBIOS plutôt qu'un domaine qualifié complet. Vous pouvez également ajouter le nom d'hôte de l'appliance à la zone intranet local d'Internet Explorer [Tools > Internet options > Security tab (Outils > options Internet > onglet Sécurité)]. Cependant, cela sera requis sur chaque client. Pour plus d'informations à ce sujet, consultez Comment puis-je configurer correctement NTLM avec SSO (les informations d'authentification envoyées de manière transparente)?

Avec les navigateurs Firefox et d'autres navigateurs autres que Microsoft, les paramètres **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** et **network.automatic-ntlm-auth.trusted-uris** doivent être définis sur le nom d'hôte de redirection en mode transparent. Vous pouvez également vous reporter à Firefox n'envoie pas les informations d'authentification de manière transparente (SSO). Cet article fournit des informations générales sur la modification des paramètres de Firefox.

Pour en savoir plus sur le nom d'hôte de redirection, consultez Configuration des paramètres d'authentification globaux, on page 31 ou la commande d'interface de ligne de commande `sethostname`.

Création d'un compte de service dans Windows Active Directory pour l'authentification Kerberos dans les déploiements à haute disponibilité

Utilisez cette procédure si vous rencontrez des problèmes avec la haute disponibilité avec l'authentification Kerberos. Les scénarios, où des problèmes peuvent survenir lors de l'utilisation de l'authentification Kerberos dans les déploiements à haute disponibilité sont les suivants :

- L'attribut servicePrincipalName du nom d'hôte à haute disponibilité est ajouté à plusieurs comptes d'ordinateurs dans Active Directory.
- L'authentification Kerberos fonctionne si servicePrincipalName a été ajouté au compte d'ordinateur unique dans Active Directory. Lorsque le nœud principal change, la haute disponibilité peut être affectée, car différents nœuds de l'appliance utilisent différentes chaînes de chiffrement pour déchiffrer les tickets de service Keberos.

Avant de commencer

- Choisissez le nom d'utilisateur à utiliser pour la haute disponibilité avec l'authentification Keberos. Nous vous recommandons de créer un nouveau nom d'utilisateur, qui sera utilisé uniquement à cette fin.
- Si vous préférez utiliser un nom d'utilisateur existant :
  - Définissez un mot de passe si le nom d'utilisateur n'en a pas.
  - Dans la boîte de dialogue des propriétés du compte d'utilisateur (dans les utilisateurs et les ordinateurs Active Directory) :

    Assurez-vous que la case User must change password at next logon (L'utilisateur doit changer le mot de passe à la prochaine connexion) n'est pas cochée.

    Cochez la case Password never expires (Le mot de passe n'expire jamais).

Étape 1 Créez un nouveau nom d'utilisateur dans les utilisateurs et les ordinateurs Active Directory.

- Spécifiez un mot de passe.
- Décochez la case User must change password at next logon (L'utilisateur doit changer le mot de passe à la prochaine connexion).
- Cochez la case Password never expires (Le mot de passe n'expire jamais).

Étape 2 Vérifiez si le nom SPN du nom d'hôte à haute disponibilité est associé à l'objet utilisateur Active Directory créé ou choisi. Le SPN se compose d'un préfixe http/ et est suivi du nom d'hôte à haute disponibilité de l'appliance. Assurez-vous que les clients sont en mesure de résoudre le nom d'hôte.

1. Utilisez la commande `setspn -q` dans Windows pour rechercher toute association existante.

   Exemple : `setspn -q http/highavail.com`

   Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance.

2. Supprimez ou ajoutez le SPN en fonction des résultats de la requête :

Remarque Les mots de passe des comptes de service Kerberos à haute disponibilité ne peuvent inclure que des lettres, des chiffres, des espaces et des caractères ~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>. Si l'un de ces trois caractères spéciaux « $, ' ou » est utilisé dans le mot de passe du compte de service Kerberos à haute disponibilité, il en résultera un échec lors de la pré-authentification à partir de l'interface utilisateur graphique et de l'interface de ligne de commande. Cependant, l'authentification est réussie pour tous les types de caractères utilisés dans le mot de passe.

Résultat de la requête	Action
Aucun SPN de ce type trouvé.	Associez le nom SPN du nom d'hôte à haute disponibilité associé à l'objet utilisateur Active Directory. • Utilisez la commande `setspn -s` : `setspn -s http/highavail.com hausername` Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance et hausername est le nom d'utilisateur créé ou choisi.

Résultat de la requête	Action
SPN existant trouvé! Le nom commun (CN) indique le nom d'utilisateur créé ou choisi. Exemple : CN = hausername	Aucune autre action n'est nécessaire dans Active Directory.

SPN existant trouvé!
Le nom d'utilisateur usuel (CN) n'affiche pas le nom d'utilisateur créé ou choisi.
	1. Supprimez le SPN.
	Utilisez la commande `setspn -d` :
	`setspn -d http/highavail.com jeandupont`
	Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance et jeandupont est le nom d'utilisateur à dissocier.
	2. Ajoutez le SPN.
	Utilisez la commande `setspn -s` :
	`setspn -s http/highavail.com hausername`
	Dans cet exemple, highavail.com est le nom d'hôte haute disponibilité de l'appliance et hausername est le nom d'utilisateur créé ou choisi.

Remarque Assurez-vous que l'authentification Keytable est activée dans le domaine Active Directory approprié. Consultez Création d'un domaine Active Directory pour le schéma d'authentification Kerberos, à la page 17. Pour les domaines déjà créés, modifiez le domaine et activez l'authentification Keytable.

Domaines d'authentification

Les domaines d'authentification définissent les détails requis pour communiquer avec les serveurs d'authentification et précisent le schéma d'authentification à utiliser lors de la communication avec les clients. AsyncOS prend en charge plusieurs domaines d'authentification. Les domaines peuvent également être regroupés en séquences d'authentification qui permettent aux utilisateurs ayant des exigences d'authentification différentes d'être gérés par les mêmes politiques.

Basculement de l'authentification

La configuration de domaine actuelle comprend un serveur AD ou LDAP principal et deux serveurs de sauvegarde. Si le premier serveur principal n'est pas accessible, la requête atteint le premier serveur de sauvegarde. Si le premier serveur de sauvegarde n'est pas non plus accessible, la requête atteint le deuxième serveur.

Table 1: Temps de basculement à l'aide de la règle IPFW

Temps de basculement	Temps de basculement de la sauvegarde principale à la sauvegarde secondaire en secondes
Pour interrompre la connexion entre l'AD principal et Secure Web Appliance	75 à 80

Temps de basculement	Temps de basculement de la sauvegarde principale à la sauvegarde secondaire en secondes
Pour interrompre la connexion entre l'AD principal et Secure Web Appliance, ainsi que pour interrompre la connexion entre la première sauvegarde et Secure Web Appliance	180 à 250
Redémarrer l'AD principal	42 s
Mettre l'AD principal hors tension	75 à 80
Mettre l'AD principal et le premier serveur de sauvegarde hors tension	180 à 250

Si plusieurs serveurs sont en panne, Secure Web Appliance réessaye d'établir la connexion jusqu'à ce qu'un contrôleur de domaine soit trouvé.

- Authentification extérieure, on page 16
- Création d'un domaine Active Directory pour le schéma d'authentification Kerberos, on page 17
- Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique), on page 22
- Création d'un domaine d'authentification LDAP, on page 25
- À propos de la suppression de domaines d'authentification, on page 30
- Configuration des paramètres d'authentification globaux, on page 31

Thèmes connexes

- Séquences d'authentification, on page 39
- Authentification des utilisateurs RADIUS

Authentification extérieure

Vous pouvez authentifier les utilisateurs au moyen d'un serveur LDAP ou RADIUS externe.

Configuration de l'authentification extérieure par l'intermédiaire d'un serveur LDAP

Before you begin

Créez un domaine d'authentification LDAP et configurez-le avec une ou plusieurs requêtes d'authentification extérieure. Création d'un domaine d'authentification LDAP, on page 25.

Étape 1 Activez l'authentification extérieure sur l'appliance :

a) Accédez à **System Administration** > **Users** (Administration système > Utilisateurs).
b) Cliquez sur **Enable** (Activer) dans la section External Authentication (Authentification extérieure).
c) Configurez les options :

Option	Description
Activer l'authentification extérieure	—
Type d'authentification	Sélectionnez LDAP.
External Authentication Cache Timeout (Délai d'expiration du cache d'authentification extérieure)	Nombre de secondes pendant lesquelles AsyncOS stocke les informations d'authentification extérieure avant de recontacter le serveur LDAP pour s'authentifier à nouveau. La valeur par défaut est zéro (0).
Requête d'authentification extérieure LDAP	Une requête configurée avec le domaine LDAP.
Délai d'attente d'une réponse valide du serveur	Le nombre de secondes qu'AsyncOS attend une réponse à la requête du serveur.
Mappage de groupe	Pour chaque nom de groupe dans le répertoire, attribuez un rôle.

Étape 2 Envoyez et validez vos modifications.

Activation de l'authentification extérieure RADIUS

Consultez Activation de l'authentification extérieure à l'aide de RADIUS.

Création d'un domaine Active Directory pour le schéma d'authentification Kerberos

Before you begin

- Assurez-vous que l'appliance est configurée en mode standard (et non en mode Cloud Connector).
- Si vous configurez la haute disponibilité, assurez-vous d'avoir également coché la case **Use keytab authentication** (Utiliser l'authentification keytab) dans la section Kerberos High Availability (Haute disponibilité Kerberos) spécifiée à l'**étape 9**.

  Si votre appliance se trouve derrière un périphérique de répartition du trafic HTTP/HTTPS comme un équilibreur de charge, vous devez associer le SPN du périphérique de répartition du trafic dans Active Directory à un compte d'utilisateur et saisir les informations d'authentification de ce compte d'utilisateur dans la section Kerberos High Availability (Haute disponibilité Kerberos). Le SPN du premier périphérique qui redirige le trafic dans la topologie du réseau doit être ajouté. Par exemple, si le trafic réseau sortant des périphériques clients passe par un gestionnaire de trafic, un équilibreur de charge, puis vers Secure Web Appliance, le SPN du gestionnaire de trafic doit être ajouté à un compte d'utilisateur sur Active Directory, et les identifiants de l'utilisateur doivent être saisis dans cette section. En effet, le gestionnaire de trafic est le premier périphérique à rencontrer le trafic des périphériques clients.
- Préparez le serveur Active Directory.
  - Installez Active Directory sur l'un des serveurs suivants : Windows Server 2003, 2008, 2008R2, 2012, 2016 (pour coeus 11.8, 12.0, 12.5, 14.0 et 14.5) ou 2019 (pour coeus 14.5 uniquement).

    Vous pouvez installer le serveur Windows Active Directory 2019 pour coeus 12.5.

- Créez un utilisateur sur le serveur Active Directory :
  - Créez un utilisateur sur le serveur Active Directory qui est membre du groupe des administrateurs de domaine ou des opérateurs de compte.

    Ou

  - Créez un nom d'utilisateur avec les autorisations suivantes :
    - Autorisations Active Directory pour la réinitialisation des mots de passe
    - Écriture validée dans servicePrincipalName
    - Restrictions de compte en écriture
    - Écriture du nom dNShost
    - Écriture dans servicePrincipalName

      Il s'agit des autorisations Active Directory minimales requises par un nom d'utilisateur pour joindre une appliance au domaine et assurer son fonctionnement complet.

- Joignez votre client au domaine. Les clients pris en charge sont Windows XP, Windows 10 et Mac OS 10.5+.
- Utilisez l'outil kerbtray du Kit de ressources Windows pour vérifier le ticket Kerberos sur le client : http://www.microsoft.com/en-us/download/details.aspx?id=17657.
- L'application de visionneuse de tickets sur les clients Mac est disponible dans le menu principal > KeyChain Access (Accès à KeyChain) pour afficher les tickets Kerberos.

- Assurez-vous de disposer des droits et des informations de domaine nécessaires pour joindre le domaine Secure Web Appliance au domaine Active Directory auprès duquel vous souhaitez vous authentifier.
- Comparez l'heure actuelle sur Secure Web Appliance avec l'heure actuelle du serveur Active Directory et vérifiez que la différence n'est pas supérieure à l'heure spécifiée dans l'option « Maximum tolerance for computer clock synchronization » (Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur) sur le serveur Active Directory.
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, soyez prêt à vous assurer que les domaines d'authentification du même nom sur différents Secure Web Appliance ont des propriétés identiques définies sur chaque appliance.
- Configuration de Secure Web Appliance :
  - En mode explicite, le nom d'hôte Secure Web Appliance (commande d'interface de ligne de commande `sethostname`) et le nom de proxy configuré dans le navigateur doivent être identiques.
  - En mode transparent, le nom d'hôte Secure Web Appliance doit être identique au nom d'hôte de redirection (voir Configuration des paramètres d'authentification globaux, on page 31). En outre, le nom d'hôte Secure Web Appliance et le nom d'hôte de redirection doivent être configurés avant la création d'un domaine Keberos.

- Sachez qu'après avoir validé le nouveau domaine, vous ne pouvez pas modifier un protocole d'authentification de domaine.

- Notez que la connexion unique (SSO) doit être configurée sur les navigateurs clients; voir Configuration de la connexion unique, on page 13.
- Pour simplifier l'utilisation des journaux, personnalisez le journal des accès pour utiliser le paramètre de champ personnalisé %m. Consultez Personnalisation des journaux d'accès.

Note Les mots de passe des comptes de service Kerberos à haute disponibilité ne peuvent inclure que des lettres, des chiffres, des espaces et des caractères ~ ! @ # % ^ & () _ - {} ' / [] : ; , | + = * ? <>. Si l'un de ces trois caractères spéciaux « $, ' ou » est utilisé dans le mot de passe du compte de service Kerberos à haute disponibilité, il en résultera un échec lors de la pré-authentification à partir de l'interface utilisateur graphique et de l'interface de ligne de commande. Cependant, l'authentification est réussie pour tous les types de caractères utilisés dans le mot de passe.

Étape 1 Dans l'interface Web de Cisco Secure Web Appliance, sélectionnez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Realm** (Ajouter un domaine).

Étape 3 Attribuez un nom unique au domaine d'authentification en utilisant uniquement des caractères alphanumériques et des espaces.

Étape 4 Sélectionnez **Active Directory** dans le champ Authentication Protocol (Protocole d'authentification).

Étape 5 Entrez jusqu'à trois noms de domaine complets ou adresses IP pour le ou les serveurs Active Directory.

Exemple : `ntlm.exemple.com`.

Une adresse IP n'est requise que si les serveurs DNS configurés sur l'appliance ne peuvent pas résoudre le nom d'hôte du serveur Active Directory.

Si plusieurs serveurs d'authentification sont configurés dans le domaine, l'appliance tente d'autoriser jusqu'à trois serveurs d'authentification avant de ne pas autoriser la transaction dans ce domaine.

Étape 6 Joignez l'appliance au domaine :

a) Configurez le compte Active Directory :

Paramètres	Description
Active Directory Domain (Domaine Active Directory)	Nom de domaine du serveur Active Directory. Également appelé domaine ou domaine DNS.
NetBIOS domain name (Nom de domaine NETBIOS)	Si le réseau utilise NetBIOS, indiquez le nom de domaine. **Tip** Si cette option n'est pas disponible, utilisez la commande de l'interface de ligne de commande `setntlmsecuritymode` pour vérifier que le mode de sécurité NTLM est défini sur « domaine ».

Paramètres	Description
Computer Account (Compte d'ordinateur)	Indiquez un emplacement dans le domaine Active Directory où AsyncOS créera un compte d'ordinateur Active Directory, également appelé « compte approuvé d'ordinateur » pour identifier de manière unique l'ordinateur dans le domaine. Si l'environnement Active Directory supprime automatiquement des objets ordinateur à des intervalles particuliers, spécifiez un emplacement pour le compte d'ordinateur qui se trouve dans un conteneur, protégé contre la suppression automatique.
Enable Trusted Domain Lookup (Activer la recherche dans les domaines approuvés)	L'option **Enable Trusted Domain Lookup** (Activer la recherche dans les domaines approuvés) est ajoutée dans la section **Active Directory Account** [**Network** > **Authentication** > **Add Realm** (Réseau > Authentification > Ajouter un domaine)] afin de contrôler le comportement de la recherche de domaines approuvés pour le domaine. Cette option est activée par défaut.

b) Cliquez sur **Join Domain** (Joindre le domaine).

Note Si vous tentez de rejoindre un domaine que vous avez déjà rejoint (même si vous utilisez les mêmes informations d'authentification), les connexions existantes seront fermées, car Active Directory enverra un nouvel ensemble de clés à tous les clients, y compris ce Secure Web Appliance. Les clients concernés devront se déconnecter et se reconnecter.

Note Le nom d'hôte du Secure Web Appliance déployé sur AWS doit être unique. Vous devez modifier la première chaîne du nom d'hôte pour créer un nom d'hôte unique.

Par exemple, si « mgmt » est ajouté au nom d'hôte comme première chaîne, vous pouvez la modifier comme suit : « mgmt<*wsa_hostname*> ».

c) Indiquez les coordonnées de connexion (nom d'utilisateur et phrase secrète) du compte sur Active Directory, puis cliquez sur Create Account (Créer le compte).

Étape 7 (Facultatif) Configurez une identification transparente de l'utilisateur.

Paramètres	Description
Enable Transparent User Identification using Active Directory agent (Activer l'identification transparente de l'utilisateur à l'aide de l'agent Active Directory)	Entrez le nom de serveur de l'ordinateur sur laquelle l'agent principal Context Directory est installé, ainsi que le secret partagé utilisé pour y accéder. (Facultatif) Saisissez le nom de serveur de l'ordinateur sur lequel un agent Context Directory de secours est installé, ainsi que son secret partagé.

Étape 8 Configurez la sécurité du réseau :

Paramètres	Description
Client Signing Required (Signature du client requise)	Sélectionnez cette option si le serveur Active Directory est configuré pour exiger la signature du client. La sélection de cette option permet la signature SMB : • Pour placer la signature numérique lorsque l'appliance se connecte à Active Directory. • Prévenir les attaques de type homme du milieu.

Étape 9 Si vous comptez utiliser la haute disponibilité, cochez la case **Use keytab authentication** (Utiliser l'authentification keytab) dans la section Kerberos High Availability (Kerberos haute disponibilité).

a) Saisissez le nom d'utilisateur et le mot de passe.

Entrez le nom d'utilisateur Active Directory associé au(x) SPN correspondant à l'adresse IP ou au nom d'hôte de la grappe à haute disponibilité. N'incluez pas le nom de domaine dans le nom d'utilisateur (par exemple, entrez « jeanuntel » plutôt que « DOMAINE\jeanuntel » ou « jeanuntel@domaine »). Consultez Création d'un compte de service dans Windows Active Directory pour l'authentification Kerberos dans les déploiements à haute disponibilité, on page 13 pour obtenir des renseignements précis sur la création d'un compte de service qui sera utilisé pour l'authentification dans les déploiements à haute disponibilité.

b) Répétez cette étape pour tous les périphériques de la grappe à haute disponibilité.

Note Si votre appliance se trouve derrière un périphérique de répartition du trafic HTTP/HTTPS comme un équilibreur de charge, vous devez associer le SPN du périphérique de répartition du trafic dans Active Directory à un compte d'utilisateur et saisir les informations d'authentification de ce compte d'utilisateur dans la section Kerberos High Availability (Kerberos haute disponibilité). Le SPN du premier périphérique qui redirige le trafic dans la topologie du réseau doit être ajouté. Par exemple, si le trafic réseau sortant des périphériques clients passe par un gestionnaire de trafic, un équilibreur de charge, puis vers Secure Web Appliance, le SPN du gestionnaire de trafic doit être ajouté à un compte d'utilisateur sur Active Directory, et les identifiants de l'utilisateur doivent être saisis dans cette section. En effet, le gestionnaire de trafic est le premier périphérique à rencontrer le trafic des périphériques clients.

Étape 10 (Facultatif) Cliquez sur **Start Test** (Commencer le test). Vous pourrez ainsi tester les paramètres que vous avez saisis et vous assurer qu'ils sont corrects avant que les utilisateurs réels ne les utilisent pour s'authentifier. Pour en savoir plus sur les tests réalisés, consultez Utilisation de plusieurs domaines et domaines NTLM, on page 30.

Étape 11 Résolvez les problèmes détectés au cours des tests. Consultez Outils de résolution de problèmes pour les problèmes d'authentification.

Étape 12 Envoyez et validez vos modifications.

What to do next

Créez un profil d'identification qui utilise le schéma d'authentification Kerberos. Classification des utilisateurs et logiciels clients.

Comment créer un domaine d'authentification Active Directory (NTLMSSP et basique)

Conditions préalables à la création d'un domaine d'authentification Active Directory (NTLMSSP et basique)

- Assurez-vous de disposer des droits et des informations de domaine nécessaires pour joindre le domaine Secure Web Appliance au domaine Active Directory auprès duquel vous souhaitez vous authentifier.
- Si vous envisagez d'utiliser « domain » comme mode de sécurité NTLM, utilisez uniquement les groupes Active Directory imbriqués. Si les groupes Active Directory ne sont pas imbriqués, utilisez la valeur par défaut, « ads ». Consultez `setntlmsecuritymode` dans la rubrique Interface de ligne de commande de ce guide.
- Comparez l'heure actuelle sur Secure Web Appliance avec l'heure actuelle du serveur Active Directory et vérifiez que la différence n'est pas supérieure à l'heure spécifiée dans l'option « Maximum tolerance for computer clock synchronization » (Tolérance maximale pour la synchronisation de l'horloge de l'ordinateur) sur le serveur Active Directory.
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, soyez prêt à vous assurer que les domaines d'authentification du même nom sur différents Secure Web Appliance ont des propriétés identiques définies sur chaque appliance.
- Sachez qu'une fois que vous avez validé le nouveau domaine, vous ne pourrez plus modifier le protocole d'authentification de ce domaine.
- Le Secure Web Appliance doit se connecter aux contrôleurs de domaine pour tous les domaines approuvés et aux contrôleurs de domaine configurés dans le domaine NTLM. Pour que l'authentification fonctionne correctement, vous devez ouvrir les ports suivants sur tous les contrôleurs du domaine interne et du domaine externe :
  - LDAP (389 UDP et TCP)
  - Microsoft SMB (445 TCP)
  - Kerberos (88 TCP)
  - Résolution des terminaux : port fixe de mappeur de port (135 TCP) Net Log-on
- Pour NTLMSSP, la connexion unique (SSO) peut être configurée sur les navigateurs clients. Consultez Configuration de la connexion unique, on page 13.

À propos de l'utilisation de plusieurs domaines et domaines NTLM

Les règles suivantes s'appliquent à l'utilisation de plusieurs domaines et domaines NTLM :

- Vous pouvez créer jusqu'à 10 domaines d'authentification NTLM.
- Les adresses IP client d'un domaine NTLM ne doivent pas se chevaucher avec les adresses IP client d'un autre domaine NTLM.
- Chaque domaine NTLM ne peut joindre qu'un seul domaine Active Directory, mais peut authentifier les utilisateurs de tous les domaines approuvés par ce domaine. Cette approbation s'applique par défaut aux autres domaines de la même forêt et aux domaines en dehors de la forêt pour lesquels il existe au moins une approbation unidirectionnelle.

- Créez des domaines NTLM supplémentaires pour authentifier les utilisateurs dans des domaines qui ne sont pas approuvés par les domaines NTLM existants.

Création d'un domaine d'authentification Active Directory (NTLMSSP et basique)

Before you begin

Assurez-vous que les ports de la plage supérieure sur l'appliance (49152 à 65535) sont débloqués dans votre pare-feu. Ces ports sont nécessaires pour effectuer les demandes de recherche de groupe asynchrones. Le blocage de ces ports peut entraîner des défaillances intermittentes de l'authentification.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Realm** (Ajouter un domaine).

Étape 3 Attribuez un nom unique au domaine d'authentification en utilisant uniquement des caractères alphanumériques et des espaces.

Étape 4 Sélectionnez **Active Directory** dans le champ Authentication Protocol and Scheme(s) (Protocole et schéma(s) d'authentification).

Étape 5 Entrez jusqu'à trois noms de domaine complets ou adresses IP pour le ou les serveurs Active Directory.

Exemple : `active.exemple.com`.

Une adresse IP n'est requise que si les serveurs DNS configurés sur l'appliance ne peuvent pas résoudre le nom d'hôte du serveur Active Directory.

Si plusieurs serveurs d'authentification sont configurés dans le domaine, l'appliance tente d'autoriser jusqu'à trois serveurs d'authentification avant de ne pas autoriser la transaction dans ce domaine.

Étape 6 Joignez l'appliance au domaine :

a) Configurez le compte Active Directory :

Paramètres	Description
Active Directory Domain (Domaine Active Directory)	Nom de domaine du serveur Active Directory. Également appelé domaine ou domaine DNS.
NetBIOS domain name (Nom de domaine NETBIOS)	Si le réseau utilise NetBIOS, indiquez le nom de domaine.
Computer Account (Compte d'ordinateur)	Spécifiez un emplacement dans le domaine Active Directory où AsyncOS créera un compte d'ordinateur Active Directory, également appelé « compte approuvé d'ordinateur », pour identifier de manière unique l'ordinateur dans le domaine. Si l'environnement Active Directory supprime automatiquement des objets ordinateur à des intervalles particuliers, spécifiez un emplacement pour le compte d'ordinateur qui se trouve dans un conteneur, protégé contre la suppression automatique.

Paramètres	Description
Enable Trusted Domain Lookup (Activer la recherche dans les domaines approuvés)	L'option **Enable Trusted Domain Lookup** (Activer la recherche dans les domaines approuvés) est ajoutée dans la section **Active Directory Account** [**Network** > **Authentication** > **Add Realm** (Réseau > Authentification > Ajouter un domaine)] afin de contrôler le comportement de la recherche de domaines approuvés pour le domaine. Cette option est activée par défaut.

b) Cliquez sur **Join Domain** (Joindre le domaine).

Note Si vous tentez de rejoindre un domaine que vous avez déjà rejoint (même si vous utilisez les mêmes informations d'authentification), les connexions existantes seront fermées, car Active Directory enverra un nouvel ensemble de clés à tous les clients, y compris ce Secure Web Appliance. Les clients concernés devront se déconnecter et se reconnecter.

Note Le nom d'hôte du Secure Web Appliance déployé sur AWS doit être unique. Vous devez modifier la première chaîne du nom d'hôte pour créer un nom d'hôte unique.

Par exemple, si « mgmt » est ajouté au nom d'hôte comme première chaîne, vous pouvez la modifier comme suit : « mgmt<*wsa_hostname*> ».

c) Entrez le nom d'utilisateur et la phrase secrète sAMAccountName pour un utilisateur Active Directory existant qui possède des droits pour créer des comptes d'ordinateur dans le domaine.

Exemple : « `jazzdoe` » Ne pas utiliser : « `DOMAIN\jazzdoe` » ou « `jazzdoe@domain` »

Ces renseignements sont utilisés une seule fois pour établir le compte d'ordinateur et ne sont pas enregistrés.

d) Cliquez sur **Create Account** (Créer un compte).

Étape 7 (Facultatif) Configurez l'authentification transparente.

Paramètres	Description
Enable Transparent User Identification using Active Directory agent (Activer l'identification transparente de l'utilisateur à l'aide de l'agent Active Directory)	Entrez le nom de serveur de l'ordinateur sur laquelle l'agent principal Context Directory est installé, ainsi que le secret partagé utilisé pour y accéder. (Facultatif) Saisissez le nom de serveur de l'ordinateur sur lequel un agent Context Directory de secours est installé, ainsi que son secret partagé.

Étape 8 Configurez la sécurité du réseau :

Paramètres	Description
Client Signing Required (Signature du client requise)	Sélectionnez cette option si le serveur Active Directory est configuré pour exiger la signature du client. La sélection de cette option permet la signature SMB : • Pour placer la signature numérique lorsque l'appliance se connecte à Active Directory. • Prévenir les attaques de type homme du milieu.

Étape 9 (Facultatif) Cliquez sur **Start Test** (Commencer le test). Cela permettra de tester les paramètres que vous avez saisis, pour s'assurer qu'ils sont corrects avant que les utilisateurs réels ne les utilisent pour s'authentifier.

Étape 10 Envoyez et validez vos modifications.

Création d'un domaine d'authentification LDAP

Before you begin

- Obtenez les informations suivantes sur LDAP au sein de votre organisation :
  - Version LDAP
  - Adresses des serveurs
  - Ports LDAP
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, assurez-vous que les domaines d'authentification du même nom sur différents Secure Web Applianceont des propriétés identiques définies sur chaque appliance.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Realm** (Ajouter un domaine).

Étape 3 Attribuez un nom unique au domaine d'authentification en utilisant uniquement des caractères alphanumériques et des espaces.

Étape 4 Sélectionnez **LDAP** dans le champ Authentication Protocol and Scheme(s) [Protocole et schéma(s) d'authentification].

Étape 5 Saisissez les paramètres d'authentification LDAP :

Paramètres	Description
LDAP Version (Version LDAP)	Choisissez la version de LDAP et indiquez si vous souhaitez utiliser ou non le LDAP sécurisé. L'appliance prend en charge les versions 2 et 3 de LDAP. Le LDAP sécurisé nécessite la version 3 de LDAP. Indiquez si ce serveur LDAP prend en charge ou non Novell eDirectory avec une identification transparente des utilisateurs.

Paramètres	Description
LDAP Server (Serveur LDAP)	Saisissez l'adresse IP du serveur LDAP ou le nom d'hôte et son numéro de port. Vous pouvez définir jusqu'à trois serveurs. Le nom d'hôte doit être un nom de domaine complet. Par exemple, `ldap.exemple.com`. Une adresse IP est requise uniquement si les serveurs DNS configurés sur l'appliance ne peuvent pas résoudre le nom d'hôte du serveur LDAP. Le numéro de port par défaut du LDAP standard est 389. Le numéro par défaut du LDAP sécurisé est 636. Si le serveur LDAP est un serveur Active Directory, entrez le nom d'hôte ou l'adresse IP et le port du contrôleur de domaine ici. Chaque fois que cela est possible, entrez le nom du serveur de catalogue global et utilisez le port 3268. Cependant, vous pouvez souhaiter utiliser un contrôleur de domaine local lorsque le serveur de catalogue global est physiquement éloigné et que vous savez que vous n'avez qu'à authentifier les utilisateurs sur le contrôleur de domaine local. **Remarque :** Lorsque vous configurez plusieurs serveurs d'authentification dans le domaine, l'appliance tente d'autoriser jusqu'à trois serveurs d'authentification avant l'échec de l'authentification de la transaction dans ce domaine. À partir d'AsyncOS version 11.5, vous pouvez spécifier l'interface source pour LDAP/NTLM (communication avec le contrôleur de domaine). Cochez la case **Set Source Interface** (Définir l'interface source), puis sélectionnez l'interface source dans la liste déroulante.
LDAP Persistent Connections (Connexions persistantes LDAP) [sous la section Advanced (Niveau avancé)]	Choisissez l'une des valeurs suivantes : • **Use persistent connections (unlimited)** [Utiliser des connexions persistantes (illimitées)]. Use existing connections (Utiliser des connexions existantes). Si aucune connexion n'est disponible, une nouvelle connexion est ouverte. • **Use persistent connections** (Utiliser des connexions persistantes). Utilisez les connexions existantes pour traiter le nombre de requêtes spécifié. Lorsque le maximum est atteint, établissez une nouvelle connexion au serveur LDAP. • **Do not use persistent connections** (Ne pas utiliser de connexions persistantes). Créez toujours une nouvelle connexion au serveur LDAP.

Paramètres	Description
User Authentication (Authentification de l'utilisateur)	Renseignez les champs suivants : **Base Distinguished Name (Base DN)** [Nom de base distinctif (ND de base)] La base de données LDAP a une structure d'annuaire de type arborescence et l'appliance utilise le ND de base pour accéder à l'emplacement correct dans l'arborescence de l'annuaire LDAP pour commencer une recherche. Une chaîne de filtre de ND de base valide se compose d'un ou de plusieurs composants au format `objet-valeur`. Par exemple , `dc=nomsociété, dc=com`. **Note** Après la mise à niveau vers cette version, vous ne pouvez pas effectuer de test de démarrage pour l'authentification LDAP si ce champ est vide. **User Name Attribute** (Attribut de nom d'utilisateur) Choisissez l'une des valeurs suivantes : • **uid**, **cn** et **sAMAccountName.** Identifiants uniques dans l'annuaire LDAP qui spécifient un nom d'utilisateur. • **custom.** Identifiant personnalisé, tel que `UserAccount`. **User Filter Query** (Requête de filtre utilisateur) La requête de filtre utilisateur est un filtre de recherche LDAP qui localise le ND de base des utilisateurs. Cela est obligatoire si l'annuaire des utilisateurs se trouve dans une hiérarchie inférieure au ND de base ou si le nom de connexion n'est pas inclus dans le composant propre à l'utilisateur du ND de base des utilisateurs. Choisissez l'une des valeurs suivantes : • **none.** Filtre tous les utilisateurs. • **custom.** Filtre un groupe particulier d'utilisateurs.
Query Credentials (Identifiants de requête)	Indiquez si le serveur d'authentification accepte ou non les requêtes anonymes. Si le serveur d'authentification accepte les requêtes anonymes, choisissez **Server Accepts Anonymous Queries** (Le serveur accepte les requêtes anonymes). Si le serveur d'authentification n'accepte pas les requêtes anonymes, choisissez **Use Bind DN** (Utiliser le ND de liaison), puis saisissez les informations suivantes : • **Bind DN** (ND de liaison). Utilisateur sur le serveur LDAP externe autorisé à effectuer une recherche dans l'annuaire LDAP. En règle générale, le ND de liaison doit être autorisé à effectuer une recherche dans tout l'annuaire. • **Passphrase** (Phrase secrète). Phrase secrète associée à l'utilisateur que vous saisissez dans le champ Bind DN (ND de liaison). Le texte suivant répertorie des exemples d'utilisateurs pour le champ Bind DN (ND de liaison) : cn=administrator,cn=Users,dc=domain,dc=com sAMAccountName=jdoe,cn=Users,dc=domain,dc=com. Si le serveur LDAP est un serveur Active Directory, vous pouvez également saisir le nom d'utilisateur du ND de liaison au format « DOMAINE\nom d'utilisateur ».

Étape 6 (Facultatif) Activez l'autorisation de groupe par le biais d'un objet de groupe ou d'un objet utilisateur et définissez les paramètres en conséquence pour l'option choisie :

Paramètre d'objet de groupe	Description
Group Membership Attribute Within Group Object (Attribut d'appartenance au groupe dans l'objet de groupe)	Choisissez l'attribut LDAP qui répertorie tous les utilisateurs appartenant à ce groupe. Choisissez l'une des valeurs suivantes : • **member** et **uniquemember.** Identifiants uniques dans l'annuaire LDAP qui désignent les membres du groupe. • **custom.** Identifiant personnalisé, tel que `UserInGroup`.
Attribute that Contains the Group Name (Attribut qui contient le nom du groupe)	Choisissez l'attribut LDAP qui désigne le nom de groupe pouvant être utilisé dans la configuration de groupe de politiques. Choisissez l'une des valeurs suivantes : • **cn.** Identifiant unique dans l'annuaire LDAP qui spécifie le nom d'un groupe. • **custom.** Identifiant personnalisé, tel que `FinanceGroup`.
Query String to Determine if Object is a Group (Chaîne de requête déterminant si l'objet est un groupe)	Choisissez un filtre de recherche LDAP qui détermine si un objet LDAP représente un groupe d'utilisateurs. Choisissez l'une des valeurs suivantes : • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.** Filtre personnalisé, tel que `objectclass=person`. **Remarque :** La requête définit l'ensemble de groupes d'authentification qui peuvent être utilisés dans les groupes de politiques.

Paramètre de l'objet utilisateur	Description
Group Membership Attribute Within User Object (Attribut de membre du groupe dans l'objet utilisateur)	Choisissez l'attribut répertoriant tous les groupes auxquels cet utilisateur appartient. Choisissez l'une des valeurs suivantes : • **memberOf.** Identifiants uniques dans l'annuaire LDAP qui désignent les membres utilisateurs. • **custom.** Identifiant personnalisé, tel que `UserInGroup`.
Group Membership Attribute is a DN (L'attribut d'appartenance au groupe est un ND)	Indiquez si l'attribut d'appartenance à un groupe est un nom distinctif (ND) qui fait référence à un objet LDAP. Activez cette option pour les serveurs Active Directory. Lorsque cette option est activée, vous devez configurer les paramètres suivants.

Paramètre de l'objet utilisateur	Description
Attribute that Contains the Group Name (Attribut qui contient le nom du groupe)	Lorsque l'attribut d'appartenance à un groupe est un ND, cela spécifie l'attribut qui peut être utilisé comme nom de groupe dans les configurations de groupe de politiques. Choisissez l'une des valeurs suivantes : • **cn.** Identifiant unique dans l'annuaire LDAP qui spécifie le nom d'un groupe. • **custom.** Identifiant personnalisé, tel que `FinanceGroup`.
Query String to Determine if Object is a Group (Chaîne de requête déterminant si l'objet est un groupe)	Choisissez un filtre de recherche LDAP qui détermine si un objet LDAP représente un groupe d'utilisateurs. Choisissez l'une des valeurs suivantes : • **objectclass=groupofnames** • **objectclass=groupofuniquenames** • **objectclass=group** • **custom.** Filtre personnalisé, tel que `objectclass=person`. **Remarque :** La requête définit l'ensemble des groupes d'authentification qui peuvent être utilisés dans les politiques Web Security Manager.

Étape 7 (Facultatif) Configurez l'authentification LDAP externe pour les utilisateurs.

a) Sélectionnez **External Authentication Queries** (Requêtes d'authentification extérieure).

b) Déterminez les comptes d'utilisateur :

Nom unique de base	ND de base permettant d'accéder à l'emplacement correct dans l'arborescence de l'annuaire LDAP pour commencer une recherche.

Query String (Chaîne de requête)	Requête permettant de renvoyer l'ensemble des groupes d'authentification, par exemple :
	`(&(objectClass=posixAccount)(uid={u}))`
	ou
	`(&(objectClass=user)(sAMAccountName={u}))`

Attribute containing the user's full name (Attribut contenant le nom complet de l'utilisateur)	Attribut LDAP, par exemple displayName ou gecos .

c) (Facultatif) Refusez la connexion aux comptes expirés en fonction des attributs LDAP d'expiration du compte RFC 2307.

d) Fournissez une requête permettant de récupérer les informations de groupe des utilisateurs.

Si un utilisateur appartient à plusieurs groupes LDAP avec des rôles utilisateur différents, AsyncOS accorde à l'utilisateur les autorisations correspondants au rôle le plus restrictif.

Nom unique de base	ND de base permettant d'accéder à l'emplacement correct dans l'arborescence de l'annuaire LDAP pour commencer une recherche.
Query String (Chaîne de requête)	`(&(objectClass=posixAccount)(uid={u}))`
Attribute containing the user's full name (Attribut contenant le nom complet de l'utilisateur)	`gecos`

Étape 8 (Facultatif) Cliquez sur **Start Test** (Commencer le test). Vous pourrez ainsi tester les paramètres que vous avez saisis et vous assurer qu'ils sont corrects avant que les utilisateurs réels ne les utilisent pour s'authentifier. Pour en savoir plus sur les tests réalisés, consultez Utilisation de plusieurs domaines et domaines NTLM, on page 30.

Note Une fois que vous avez envoyé et validé vos modifications, vous ne pourrez plus modifier le protocole d'authentification d'un domaine par la suite.

Étape 9 Envoyez et validez vos modifications.

What to do next

Créez un profil d'identification qui utilise le schéma d'authentification Kerberos. Consultez Classification des utilisateurs et logiciels clients.

Thèmes connexes

- Authentification extérieure, on page 16

Utilisation de plusieurs domaines et domaines NTLM

Les règles suivantes s'appliquent à l'utilisation de plusieurs domaines et domaines NTLM :

- Vous pouvez créer jusqu'à 10 domaines d'authentification NTLM.
- Les adresses IP client d'un domaine NTLM ne doivent pas se chevaucher avec les adresses IP client d'un autre domaine NTLM.
- Chaque domaine NTLM ne peut joindre qu'un seul domaine Active Directory, mais peut authentifier les utilisateurs de tous les domaines approuvés par ce domaine. Cette approbation s'applique par défaut aux autres domaines de la même forêt et aux domaines en dehors de la forêt pour lesquels il existe au moins une approbation unidirectionnelle.
- Créez des domaines NTLM supplémentaires pour authentifier les utilisateurs dans des domaines qui ne sont pas approuvés par les domaines NTLM existants.

À propos de la suppression de domaines d'authentification

La suppression d'un domaine d'authentification désactive les identités associées, ce qui supprime ces identités des politiques associées.

La suppression d'un domaine d'authentification le supprime des séquences.

Configuration des paramètres d'authentification globaux

Configurez les paramètres d'authentification globaux pour appliquer des paramètres à tous les domaines d'authentification, indépendamment de leurs protocoles d'authentification.

Le mode de déploiement du proxy Web affecte les paramètres d'authentification globaux que vous pouvez configurer. Des paramètres supplémentaires sont disponibles en cas de déploiement en mode transparent par rapport au mode de transfert explicite.

Before you begin

Familiarisez-vous avec les concepts suivants :

- Échec de l'authentification, on page 41
- Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes, on page 45

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

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

Étape 3 Modifiez les paramètres dans la section Global Authentication Settings (Paramètres d'authentification globaux) :

Paramètres	Description
Action if Authentication Service Unavailable (Action si le service d'authentification n'est pas disponible)	Choisissez l'une des valeurs suivantes : • **Permit traffic to proceed without authentication** (Autoriser la poursuite du trafic sans authentification). Le traitement se poursuit comme si l'utilisateur était authentifié. • **Block all traffic if user authentication fails** (Bloquer l'intégralité du trafic en cas d'échec de l'authentification de l'utilisateur). Le traitement est interrompu et l'intégralité du trafic est bloquée.
Failed Authentication Handling (Échec de la gestion de l'authentification)	Lorsque vous accordez aux utilisateurs un accès invité dans une politique de profil d'identification, ce paramètre détermine comment le proxy Web identifie et connecte l'utilisateur en tant qu'invité dans les journaux d'accès. Pour en savoir plus sur l'octroi d'un accès invité aux utilisateurs, consultez Octroi d'un accès invité après échec de l'authentification, on page 44.

Paramètres	Description
Re-authentication (Réauthentification) (Activer l'invite de réauthentification si l'utilisateur final est bloqué par la catégorie d'URL ou la restriction de session de l'utilisateur)	Ce paramètre permet aux utilisateurs de s'authentifier à nouveau si l'accès à un site Web de l'utilisateur est interdit en raison d'une politique de filtrage d'URL restrictive ou de l'interdiction de se connecter à une autre adresse IP. L'utilisateur voit une page de blocage qui comprend un lien qui lui permet d'entrer de nouveaux identifiants d'authentification. Si l'utilisateur saisit des identifiants qui permettent un accès plus étendu, la page demandée s'affiche dans le navigateur. **Remarque :** Ce paramètre s'applique uniquement aux utilisateurs authentifiés qui sont bloqués en raison de politiques de filtrage d'URL restrictives ou de restrictions de session utilisateur. Il ne s'applique pas aux transactions bloquées par sous-réseau sans authentification. Pour en savoir plus, consultez Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes, on page 45.
Basic Authentication Token TTL (Durée de vie du jeton d'authentification de base)	Contrôle la durée pendant laquelle les informations d'authentification de l'utilisateur sont stockées dans le cache avant de les revalider auprès du serveur d'authentification. Ces informations incluent le nom d'utilisateur et la phrase secrète, ainsi que les groupes d'annuaires associés à l'utilisateur. La valeur par défaut est le paramètre recommandé. Lorsque le paramètre Surrogate Timeout (Délai d'expiration de substitution) est configuré et est supérieur à la durée de vie du jeton d'authentification de base, la valeur du délai d'expiration de substitution est prioritaire et le proxy Web contacte le serveur d'authentification après l'expiration du délai de substitution.

Les autres paramètres d'authentification que vous pouvez configurer dépendent du déploiement du proxy Web, en mode de transfert transparent ou explicite.

Étape 4 Si le proxy Web est déployé en mode transparent, modifiez les paramètres comme suit :

Paramètres	Description
Credential Encryption (Chiffrement des informations d'authentification)	Ce paramètre spécifie si le client envoie ou non les coordonnées de connexion au proxy Web au moyen d'une connexion HTTPS chiffrée. Ce paramètre s'applique aux schémas d'authentification de base et NTLMSSP, mais il est particulièrement utile pour le schéma d'authentification de base, car les informations d'authentification de l'utilisateur sont envoyées en texte brut. Pour en savoir plus, consultez Échec de l'authentification, on page 41.
HTTPS Redirect Port (Port de redirection HTTPS)	Indiquez un port TCP à utiliser pour la redirection des demandes d'authentification des utilisateurs sur une connexion HTTPS. Ce paramètre spécifie le port que le client ouvrira une connexion au proxy Web à l'aide de HTTPS. Cela se produit lorsque le chiffrement des informations d'authentification est activé ou lors de l'utilisation du contrôle d'accès et que les utilisateurs sont invités à s'authentifier.

Paramètres	Description
Redirect Hostname (Nom d'hôte de redirection)	Entrez le nom d'hôte court de l'interface réseau sur laquelle le proxy Web écoute les connexions entrantes. Lorsque vous configurez l'authentification sur une appliance déployée en mode transparent, le proxy Web utilise ce nom d'hôte dans l'URL de redirection envoyée aux clients pour authentifier les utilisateurs. Vous pouvez saisir les valeurs suivantes : • **Single word hostname** (Nom d'hôte en un seul mot). Vous pouvez entrer le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Cela permet aux clients de réaliser une véritable connexion unique avec Internet Explorer sans configuration supplémentaire côté navigateur. Assurez-vous d'entrer le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Par exemple, si vos clients se trouvent dans le domaine monentreprise.com et que l'interface sur laquelle le proxy Web écoute a le nom d'hôte complet **`proxy.monentreprise.com`**, vous devez saisir **`proxy`** dans ce champ. Les clients effectuent une recherche sur le proxy et devraient être en mesure de résoudre **`proxy.monentreprise.com`**. • **Nom de domaine complet** [Nom de domaine complet (FQDN).] Vous pouvez également saisir le nom de domaine complet (FQDN) ou l'adresse IP dans ce champ. Toutefois, si vous faites cela et que vous souhaitez une véritable connexion unique pour les navigateurs Internet Explorer et Firefox, vous devez vous assurer que le nom de domaine complet (FQDN) ou l'adresse IP est ajouté à la liste des sites approuvés du client dans les navigateurs client. La valeur par défaut est le nom de domaine complet (FQDN) de l'interface M1 ou P1, selon l'interface utilisée pour le trafic du proxy.
Options du cache des informations d'authentification : Surrogate Timeout (Délai d'expiration de la substitution)	Ce paramètre indique combien de temps le proxy Web attend avant de demander à nouveau au client ses identifiants d'authentification. Jusqu'à ce que le proxy Web demande à nouveau les informations d'authentification, il utilise la valeur stockée dans la substitution (adresse IP ou témoin). Il est courant que les agents utilisateurs, tels que les navigateurs, mettent en cache les informations d'authentification afin que l'utilisateur ne soit pas invité à saisir ses informations d'authentification à chaque fois.
Options du cache des informations d'authentification : Client IP Idle Timeout (Délai d'expiration pour inactivité du client)	Lorsque l'adresse IP est utilisée comme substitution d'authentification, ce paramètre indique la durée d'attente du proxy Web avant de demander à nouveau au client des informations d'authentification lorsque le client est inactif. Si cette valeur est supérieure au délai d'expiration de substitution, ce paramètre n'a aucun effet et les clients sont invités à s'authentifier une fois le délai d'expiration de substitution atteint. Vous pourriez souhaiter utiliser ce paramètre pour réduire la vulnérabilité des utilisateurs qui quittent leur ordinateur.

Paramètres	Description
User Session Restrictions (Restrictions des sessions utilisateur)	Ce paramètre indique si les utilisateurs authentifiés sont autorisés à accéder à Internet à partir de plusieurs adresses IP simultanément. Vous pouvez souhaiter restreindre l'accès à un appareil pour empêcher les utilisateurs de partager leurs identifiants d'authentification avec des utilisateurs non autorisés. Si un utilisateur ne peut pas se connecter sur un autre appareil, une page de notification à l'utilisateur final s'affiche. Vous pouvez choisir si les utilisateurs peuvent ou non cliquer sur un bouton pour se connecter avec un nom d'utilisateur différent à l'aide du paramètre de réauthentification sur cette page. Lorsque vous activez ce paramètre, saisissez la valeur du délai d'expiration de restriction, qui détermine le temps que les utilisateurs doivent attendre avant de pouvoir se connecter à un appareil avec une adresse IP différente. La valeur du délai d'expiration de la restriction doit être supérieure à la valeur du délai d'expiration de la substitution. Vous pouvez supprimer un utilisateur en particulier ou tous les utilisateurs du cache d'authentification à l'aide de la commande de l'interface de ligne de commande `authcache`.

Paramètres	Description
Header Based Authentication (Authentification basée sur l'en-tête)	Ce paramètre vous permet de configurer le schéma d'authentification basée sur l'en-tête pour un annuaire Active Directory. Les paramètres du cache pour l'authentification basée sur l'en-tête : • Le cache d'authentification est activé par défaut. • Le délai d'expiration du cache d'authentification est identique au délai d'expiration de substitution. • Le cache stocke le nom d'utilisateur et les groupes d'utilisateurs. **Note** Effacez le cache d'authentification si vous mettez à jour la configuration du groupe d'utilisateurs. Cochez la case **Standard Header** (En-tête standard) avec ASCII comme encodage de texte et No encoding (Aucun encodage) pour Binary (Binaire) qui sont les paramètres par défaut. Cochez la case **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** (Utiliser les groupes dans l'en-tête X-Authenticate-Groups/en-tête personnalisé pour les politiques d'accès correspondantes) afin de prendre en compte l'en-tête des groupes entrants. Utilisez l'option **Custom Header Name** (Nom d'en-tête personnalisé) si vous souhaitez configurer les noms d'en-tête personnalisés. **Note** Si vous cochez la case **Use Groups in X-Authenticate-Groups Header/Personal Header for matching Policies** (Utiliser des groupes dans l'en-tête X-Authenticate-Groups/l'en-tête personnel pour les politiques correspondantes) et qu'aucun en-tête X-Authenticated-Groups n'est fourni, la correspondance pourrait échouer pour les politiques d'accès. Si elle n'est pas activée, les groupes extraits d'Active Directory seront mis en correspondance avec les politiques d'accès. Cochez la case **Retain Authentication Details on Egress** (Conserver les détails d'authentification à la sortie) pour conserver les en-têtes (en-têtes d'utilisateur et de groupe) à la sortie.
Advanced (Niveau avancé)	Lorsque vous utilisez le chiffrement des identifiants ou le contrôle d'accès, vous pouvez choisir si l'appliance utilise le certificat numérique et la clé livrés avec l'appliance (certificat de démonstration de l'appliance Cisco pour la sécurité du Web) ou un certificat numérique et la clé que vous chargez ici.

Étape 5 Si le proxy Web est déployé en mode de transfert explicite, modifiez les paramètres comme suit :

Paramètres	Description
Credential Encryption (Chiffrement des informations d'authentification)	Ce paramètre spécifie si le client envoie ou non les coordonnées de connexion au proxy Web au moyen d'une connexion HTTPS chiffrée. Pour activer le chiffrement des informations d'identification, choisissez « HTTPS Redirect (Secure) » [Redirection HTTPS (sécurisée)]. Lorsque vous activez le chiffrement des informations d'authentification, des champs supplémentaires apparaissent pour permettre la configuration de la redirection des clients vers le proxy Web pour l'authentification. Ce paramètre s'applique aux schémas d'authentification de base et NTLMSSP, mais il est particulièrement utile pour le schéma d'authentification de base, car les informations d'authentification de l'utilisateur sont envoyées en texte brut. Pour en savoir plus, consultez Échec de l'authentification, on page 41.
HTTPS Redirect Port (Port de redirection HTTPS)	Indiquez un port TCP à utiliser pour la redirection des demandes d'authentification des utilisateurs sur une connexion HTTPS. Ce paramètre spécifie le port que le client ouvrira une connexion au proxy Web à l'aide de HTTPS. Cela se produit lorsque le chiffrement des informations d'authentification est activé ou lors de l'utilisation du contrôle d'accès et que les utilisateurs sont invités à s'authentifier.
Redirect Hostname (Nom d'hôte de redirection)	Entrez le nom d'hôte abrégé de l'interface réseau sur laquelle le proxy Web écoute les connexions entrantes. Lorsque vous activez le mode d'authentification ci-dessus, le proxy Web utilise ce nom d'hôte dans l'URL de redirection envoyée aux clients pour authentifier les utilisateurs. Vous pouvez saisir les valeurs suivantes : • **Single word hostname** (Nom d'hôte en un seul mot). Vous pouvez saisir le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Cela permet aux clients de réaliser une véritable connexion unique avec Internet Explorer sans configuration supplémentaire côté navigateur. Assurez-vous d'entrer le nom d'hôte en un seul mot qui est résolu par DNS par le client et Secure Web Appliance. Par exemple, si vos clients se trouvent dans le domaine monentreprise.com et que l'interface sur laquelle le proxy Web écoute a le nom d'hôte complet `proxy.monentreprise.com`, vous devez saisir `proxy` dans ce champ. Les clients effectuent une recherche sur le proxy et devraient être en mesure de résoudre `proxy.monentreprise.com`. • **Nom de domaine complet** [Nom de domaine complet (FQDN).] Vous pouvez également saisir le nom de domaine complet (FQDN) ou l'adresse IP dans ce champ. Toutefois, si vous faites cela et que vous souhaitez une véritable connexion unique pour les navigateurs Internet Explorer et Firefox, vous devez vous assurer que le nom de domaine complet (FQDN) ou l'adresse IP est ajouté à la liste des sites approuvés du client dans les navigateurs client. La valeur par défaut est le nom de domaine complet (FQDN) de l'interface M1 ou P1, selon l'interface utilisée pour le trafic du proxy.

Paramètres	Description
Options du cache des informations d'authentification : Surrogate Timeout (Délai d'expiration de la substitution)	Ce paramètre indique combien de temps le proxy Web attend avant de demander à nouveau au client ses identifiants d'authentification. Jusqu'à ce que le proxy Web demande à nouveau les informations d'authentification, il utilise la valeur stockée dans la substitution (adresse IP ou témoin). Notez qu'il est courant pour les agents utilisateurs, comme les navigateurs, de mettre en cache les identifiants d'authentification afin que l'utilisateur ne soit pas invité à saisir ses identifiants à chaque fois.
Options du cache des informations d'authentification : Client IP Idle Timeout (Délai d'expiration pour inactivité du client)	Lorsque l'adresse IP est utilisée comme substitution d'authentification, ce paramètre indique la durée d'attente du proxy Web avant de demander à nouveau au client des informations d'authentification lorsque le client est inactif. Si cette valeur est supérieure au délai d'expiration de substitution, ce paramètre n'a aucun effet et les clients sont invités à s'authentifier une fois le délai d'expiration de substitution atteint. Vous pourriez souhaiter utiliser ce paramètre pour réduire la vulnérabilité des utilisateurs qui quittent leur ordinateur.
User Session Restrictions (Restrictions des sessions utilisateur)	Ce paramètre indique si les utilisateurs authentifiés sont autorisés à accéder à Internet à partir de plusieurs adresses IP simultanément. Vous pouvez souhaiter restreindre l'accès à un appareil pour empêcher les utilisateurs de partager leurs identifiants d'authentification avec des utilisateurs non autorisés. Lorsqu'un utilisateur ne peut pas se connecter sur un autre appareil, une page de notification à l'utilisateur final s'affiche. Vous pouvez choisir si les utilisateurs peuvent ou non cliquer sur un bouton pour se connecter avec un nom d'utilisateur différent à l'aide du paramètre de réauthentification sur cette page. Lorsque vous activez ce paramètre, saisissez la valeur du délai d'expiration de restriction, qui détermine le temps que les utilisateurs doivent attendre avant de pouvoir se connecter à un appareil avec une adresse IP différente. La valeur du délai d'expiration de la restriction doit être supérieure à la valeur du délai d'expiration de la substitution. Vous pouvez supprimer un utilisateur en particulier ou tous les utilisateurs du cache d'authentification à l'aide de la commande de l'interface de ligne de commande `authcache`.

Paramètres	Description
Header Based Authentication (Authentification basée sur l'en-tête)	Ce paramètre vous permet de configurer le schéma d'authentification basée sur l'en-tête pour un annuaire Active Directory. Les paramètres du cache pour l'authentification basée sur l'en-tête : • Le cache d'authentification est activé par défaut. • Le délai d'expiration du cache d'authentification est identique au délai d'expiration de substitution. • Le cache stocke le nom d'utilisateur et les groupes d'utilisateurs. **Note** Effacez le cache d'authentification si vous mettez à jour la configuration du groupe d'utilisateurs. Cochez la case **Standard Header** (En-tête standard) avec ASCII comme encodage de texte et No encoding (Aucun encodage) pour Binary (Binaire) qui sont les paramètres par défaut. Cochez la case **Use Groups in X-Authenticate-Groups Header/Custom Header for matching Access Policies** (Utiliser les groupes dans l'en-tête X-Authenticate-Groups/en-tête personnalisé pour les politiques d'accès correspondantes) afin de prendre en compte l'en-tête des groupes entrants. Utilisez l'option **Custom Header Name** (Nom d'en-tête personnalisé) si vous souhaitez configurer les noms d'en-tête personnalisés. **Note** Si vous cochez la case **Use Groups in X-Authenticate-Groups Header/Personal Header for matching Policies** (Utiliser des groupes dans l'en-tête X-Authenticate-Groups/l'en-tête personnel pour les politiques correspondantes) et qu'aucun en-tête X-Authenticated-Groups n'est fourni, la correspondance pourrait échouer pour les politiques d'accès. Si elle n'est pas activée, les groupes extraits d'Active Directory seront mis en correspondance avec les politiques d'accès. Cochez la case **Retain Authentication Details on Egress** (Conserver les détails d'authentification à la sortie) pour conserver les en-têtes (en-têtes d'utilisateur et de groupe) à la sortie.
Advanced (Niveau avancé)	Lorsque vous utilisez le chiffrement des identifiants ou le contrôle d'accès, vous pouvez choisir si l'appliance utilise le certificat numérique et la clé livrés avec l'appliance (certificat de démonstration de l'appliance Cisco pour la sécurité du Web) ou un certificat numérique et la clé que vous chargez ici. Pour charger un certificat numérique et une clé, cliquez sur **Browse** (Parcourir) et accédez au fichier nécessaire sur votre ordinateur local. Cliquez ensuite sur **Upload Files** (Charger des fichiers) après avoir sélectionné les fichiers souhaités.

Étape 6 Envoyez et validez vos modifications.

Séquences d'authentification

À propos des séquences d'authentification

Utilisez des séquences d'authentification pour permettre l'authentification des utilisateurs avec des identités uniques au moyen de différents serveurs ou protocoles d'authentification. Les séquences d'authentification sont également utiles pour fournir des options de secours au cas où les options d'authentification principales étaient indisponibles.

Les séquences d'authentification sont des ensembles composés d'au moins deux domaines d'authentification. Les domaines utilisés peuvent avoir différents serveurs d'authentification et différents protocoles d'authentification. Pour en savoir plus sur les domaines d'authentification, consultez Domaines d'authentification, on page 15.

Une fois que vous avez créé un deuxième domaine d'authentification, l'appliance affiche automatiquement une section Realm Sequences (Séquences de domaines) sous Network > Authentication (Réseau > Authentification) et inclut une séquence d'authentification par défaut nommée All Realms (Tous les domaines). La séquence All Realms (Tous les domaines) comprend automatiquement chaque domaine que vous définissez. Vous pouvez modifier l'ordre des domaines dans la séquence All Realms (Tous les domaines), mais vous ne pouvez pas supprimer la séquence All Realms (Tous les domaines) ni en supprimer le moindre domaine.

Si plusieurs domaines d'authentification NTLM sont définis, Secure Web Appliance utilise le schéma d'authentification NTLMSSP avec un seul domaine d'authentification NTLM par séquence. Vous pouvez choisir le domaine d'authentification NTLM à utiliser pour NTLMSSP dans chaque séquence, notamment la séquence All Realms (Tous les domaines). Pour utiliser NTLMSSP avec plusieurs domaines NTLM, configurez un seul profil d'identification pour deux domaines d'authentification en veillant à ce qu'une seule identité soit utilisée pour All Realms (Tous les domaines). Les domaines doivent entretenir une confiance mutuelle.

Les domaines d'authentification utilisés lors de l'authentification dans une séquence dépendent des éléments suivants :

- Le schéma d'authentification utilisé. Cela est généralement dicté par le type d'informations d'authentification saisies sur le client.
- L'ordre dans lequel les domaines sont répertoriés dans la séquence (pour les domaines Basic (De base) uniquement, car un seul domaine NTLMSSP est possible).

Tip Pour des performances optimales, authentifiez les clients sur le même sous-réseau à l'aide d'un seul domaine.

Création de séquences d'authentification

Before you begin

- Créez deux domaines d'authentification ou plus (voir Domaines d'authentification, on page 15).
- Si le Secure Web Appliance est géré par une appliance de gestion de la sécurité, assurez-vous que les domaines d'authentification du même nom sur différents Secure Web Applianceont des propriétés identiques définies sur chaque appliance.
- Sachez qu'AsyncOS utilisera les domaines pour traiter l'authentification de manière successive, en commençant par le premier domaine de la liste.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur **Add Sequence** (Ajouter une séquence).

Étape 3 Saisissez un nom unique pour la séquence en utilisant des caractères alphanumériques et des espaces.

Étape 4 Dans la première ligne de la zone Realm Sequence for Basic System (Séquence de domaine pour le schéma de base), choisissez le premier domaine d'authentification que vous souhaitez inclure dans la séquence.

Étape 5 Dans la deuxième ligne de la zone Realm Sequence for Basic System (Séquence de domaine pour le schéma de base), choisissez le domaine suivant à inclure dans la séquence.

Étape 6 (Facultatif) Cliquez sur **Add Row** (Ajouter une ligne) pour inclure un autre domaine qui utilise les informations d'authentification de base.

Étape 7 Si un domaine NTLM est défini, choisissez-en un dans le champ Realm (Domaine) pour le schéma NTLMSSP.

Le proxy Web utilise ce domaine NTLM lorsque le client envoie les informations d'authentification NTLMSSP.

Étape 8 Envoyez et validez vos modifications.

Modification et réorganisation des séquences d'authentification

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur le nom de la séquence que vous souhaitez modifier ou réorganiser.

Étape 3 Choisissez un nom de domaine dans la liste déroulante Realms (Domaines) sur la ligne correspondant au numéro de position que vous souhaitez que le domaine occupe dans la séquence.

Note Pour la séquence All Realms (Tous les domaines), vous pouvez uniquement modifier l'ordre de ses domaines, vous ne pouvez pas modifier les domaines eux-mêmes. Pour modifier l'ordre des domaines dans la séquence All Realms (Tous les domaines), cliquez sur les flèches dans la colonne Order (Organiser) pour repositionner les domaines correspondants.

Étape 4 Répétez l'**étape 3** jusqu'à ce que tous les domaines soient répertoriés et organisés comme requis, en vous assurant que chaque nom de domaine s'affiche sur une seule ligne.

Étape 5 Envoyez et validez vos modifications.

Suppression de séquences d'authentification

Before you begin

Sachez que la suppression d'une séquence d'authentification désactive également les identités associées, qui à leur tour suppriment ces identités des politiques associées.

Étape 1 Choisissez **Network** > **Authentication** (Réseau > Authentification).

Étape 2 Cliquez sur l'icône de corbeille en regard du nom de la séquence.

Étape 3 Cliquez sur **Delete** (Supprimer) pour confirmer la suppression de la séquence.

Étape 4 Validez vos modifications.

Échec de l'authentification

À propos de l'échec de l'authentification

L'accès au Web des utilisateurs peut être bloqué en raison d'un échec d'authentification pour les raisons suivantes :

- **Limites du client/agent utilisateur.** Certaines applications clientes peuvent ne pas prendre en charge correctement l'authentification. Vous pouvez contourner l'authentification pour ces clients en configurant des profils d'identification qui ne nécessitent pas d'autorisation et en fondant leurs critères sur les clients (et, éventuellement, sur les URL auxquels ils doivent accéder).
- **Le service d'authentification n'est pas disponible.** Un service d'authentification peut ne pas être disponible en raison de problèmes de réseau ou de serveur. Vous pouvez choisir d'autoriser le trafic non authentifié dans ces circonstances.
- **informations d'authentification non valides.** Certains utilisateurs peuvent ne pas être en mesure de fournir des identifiants valides pour une authentification correcte (par exemple, les visiteurs ou les utilisateurs en attente d'identifiants). Vous pouvez choisir d'accorder à ces utilisateurs un accès limité à Internet.

Thèmes connexes

- Contournement de l'authentification avec des agents utilisateur problématiques , on page 42
- Contournement de l'authentification, on page 43
- Autorisation du trafic non authentifié lorsque le service d'authentification n'est pas disponible, on page 44

• Octroi d'un accès invité après échec de l'authentification, on page 44

Contournementdel'authentificationavecdesagentsutilisateurproblématiques

Certains agents utilisateur sont connus pour avoir des problèmes d'authentification qui peuvent avoir une incidence sur leurs opérations normales.

Vous devez contourner l'authentification par les agents utilisateur suivants :

- Windows-Update-Agent
- MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT
- Microsoft BITS
- SLSSoapClient
- Akamai NetSession Interface
- Microsoft-CryptoAPI
- NCSI
- MSDW
- Gnotify
- msde
- Mise à jour Google

Note Les politiques d'accès continuent de filtrer (en fonction des catégories d'URL) et d'analyser le trafic (McAfee, Webroot) selon la configuration des politiques d'accès.

Étape 1 Configurez le profil d'identification pour contourner l'authentification avec les agents utilisateur indiqués :

a) Sélectionnez **Web Security Manager > Identification Profile** (Web Security Manager > Profil d'identification).
b) Cliquez sur **Add Identification Profile** (Ajouter un profil d'identification).
c) Saisissez les informations :

Option	Valeur
Name (Nom)	User Agent AuthExempt Identification Profile (Profil d'identification Authexempt d'agent utilisateur)
Insert Above (Insérer au-dessus)	Définir sur le premier profil dans l'ordre de traitement
Define Members by Subnet (Définir les membres par sous-réseau)	Laissez le champ vide.
Define Members by Authentication (Définir les membres par authentification)	Aucune authentication requise.

d) Cliquez sur **Advanced > User Agents** (Avancé > Agents utilisateur).
e) Cliquez sur **None Selected** (Aucune sélection).
f) Sous Custom user Agents (Agents utilisateur personnalisés), indiquez les chaînes d'agents utilisateur problématiques.

Étape 2 Configurez la politique d'accès :

a) Choisissez **Web Security Manager > Access Policies** (Web Security Manager > Politiques d'accès).
b) Cliquez sur **Add Policy** (Ajouter une politique).
c) Saisissez les informations :

Option	Valeur
Policy Name (nom de la politique)	Auth Exemption for User Agents (Dispense d'autorisation pour les agents utilisateur)
Insert Above Policy (Insérer au-dessus de la politique)	Définissez la première politique dans l'ordre de traitement.
Identification Profile Policy (Politique de profil d'identification)	User Agent AuthExempt Identification Profile (Profil d'identification Authexempt d'agent utilisateur)
Advanced (Niveau avancé)	Aucun

Étape 3 Envoyez et validez vos modifications.

Contournement de l'authentification

	Étape	Autres renseignements
1	Créez une catégorie d'URL personnalisée qui contient les sites Web concernés en configurant les propriétés avancées.	Création et modification de catégories d'URL personnalisées
2	Créez un profil d'identification ayant les caractéristiques suivantes : • Placé au-dessus de toutes les identités nécessitant une authentification. • Comprend la catégorie d'URL personnalisée. • Comprend les applications clientes concernées. • Ne requiert pas d'authentification.	Classification des utilisateurs et logiciels clients
3	Créez une politique pour le profil d'identification.	Création d'une politique

Thèmes connexes

- Contourner le proxy Web

Autorisation du trafic non authentifié lorsque le service d'authentification n'est pas disponible

Note Cette configuration s'applique uniquement lorsqu'un service d'authentification n'est pas disponible. Elle ne contournera pas l'authentification de façon permanente. Pour d'autres options, consultez À propos de l'échec de l'authentification, on page 41

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

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

Étape 3 Cliquez sur **Permit Traffic To Proceed Without Authentication** (Permettre au trafic de poursuivre sans authentification) dans le champ Action If Authentication Service Unavailable (Action en cas d'indisponibilité du service d'authentification).

Étape 4 Envoyez et validez vos modifications.

Octroi d'un accès invité après échec de l'authentification

Pour accorder l'accès invité, vous devez exécuter les procédures suivantes :

1. Définir un profil d'identification qui prend en charge l'accès invité, on page 44
2. Utiliser un profil d'identification qui prend en charge l'accès invité dans une politique, on page 45
3. (Facultatif) Configurer la façon dont les détails de l'utilisateur invité sont journalisés, on page 45

Note Si un profil d'identification permet l'accès invité et qu'aucune politique définie par l'utilisateur n'utilise ce profil d'identification, les utilisateurs qui échouent à l'authentification correspondent à la politique globale du type de politique applicable. Par exemple, si MyIdentificationProfile permet l'accès en tant qu'invité et qu'aucune politique d'accès définie par l'utilisateur n'utilise MyIdentificationProfile, les utilisateurs qui échouent à l'authentification correspondent à la politique d'accès globale. Si vous ne souhaitez pas que les utilisateurs invités correspondent à une politique globale, créez une politique supérieure à la politique globale qui s'applique aux utilisateurs invités et bloque tous les accès.

Définir un profil d'identification qui prend en charge l'accès invité

Étape 1 Choisissez **Web Security Manager > Identification Profiles** (Web Security Manager > Profils d'identification).

Étape 2 Cliquez sur **Add Identification Profile** (Ajouter un profil d'identification) pour ajouter une nouvelle identité, ou cliquez sur le nom de l'identité existante que vous souhaitez utiliser.

Étape 3 Cochez la case **Support Guest Privileges** (Prise en charge des privilèges invité).

Étape 4 Envoyez et validez vos modifications.

Utiliser un profil d'identification qui prend en charge l'accès invité dans une politique

Étape 1 Choisissez un type de politique dans le menu Web Security Manager.

Étape 2 Cliquez sur un nom de politique dans le tableau des politiques.

Étape 3 Choisissez **Select One Or More Identification Profiles** (Sélectionner un ou plusieurs profils d'identification) dans la liste déroulante Identification Profiles And Users (Profils d'identification et utilisateurs) (si ce n'est déjà fait).

Étape 4 Choisissez un **profil** qui prend en charge l'accès invité dans la liste déroulante de la colonne Identification Profile (Profil d'identification).

Étape 5 Cliquez sur le bouton radio **Guest (Users Failing Authentication)** [Invités (Utilisateurs dont l'authentification a échoué)].

Note Si cette option n'est pas disponible, cela signifie que le **profil** que vous avez choisi n'est pas configuré pour prendre en charge l'accès invité. Revenez à l'étape 4 et choisissez-en un autre, ou consultez Définir un profil d'identification qui prend en charge l'accès invité, on page 44 pour en définir un nouveau.

Étape 6 Envoyez et validez vos modifications.

Configurer la façon dont les détails de l'utilisateur invité sont journalisés

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

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

Étape 3 Cliquez sur un bouton radio Log Guest User By (Consigner l'utilisateur invité par), décrit ci-dessous, dans le champ Failed Authentication Handling (Échec de la gestion de l'authentification).

Bouton radio	Description
IP Address (Adresse IP)	L'adresse IP du client de l'utilisateur invité est consignée dans les journaux d'accès.
User Name As Entered By End-User (Nom d'utilisateur tel qu'il a été saisi par l'utilisateur final)	Le nom d'utilisateur dont l'authentification a initialement échoué est consigné dans les journaux d'accès.

Étape 4 Envoyez et validez vos modifications.

Échec de l'autorisation : autorisation de réauthentification avec des informations d'authentification différentes

À propos de l'autorisation de réauthentification avec des informations d'authentification différentes

Utilisez la nouvelle authentification pour permettre aux utilisateurs de s'authentifier à nouveau, en utilisant des informations d'authentification différentes, si les informations d'authentification qu'ils ont précédemment utilisées ont échoué à l'autorisation. Un utilisateur peut s'authentifier avec succès, mais ne pas pouvoir accéder à une ressource Web s'il n'est pas autorisé à le faire. En effet, l'authentification identifie simplement les utilisateurs dans le but de transmettre leurs informations d'authentification vérifiées aux politiques, mais ce sont les politiques qui autorisent ou non ces utilisateurs à accéder aux ressources.

Un utilisateur doit s'être authentifié avec succès pour être autorisé à s'authentifier de nouveau.

- Pour utiliser la fonctionnalité de réauthentification avec les pages de notification à l'utilisateur final définies par l'utilisateur, le script CGI qui analyse l'URL de redirection doit analyser et utiliser le paramètre Reauth_URL.

Autorisation de réauthentification avec des informations d'authentification différentes

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

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

Étape 3 Cochez la case **Re-Authentication Prompt If End User Blocked by URL Category Or User Session Restriction** (Invite de réauthentification si l'utilisateur final est bloqué par la catégorie d'URL ou la restriction de session de l'utilisateur).

Étape 4 Cliquez sur **Submit** (Soumettre).

Suivi des utilisateurs identifiés

Note Lorsque l'appliance est configurée pour utiliser des substitutions d'authentification basées sur les témoins, elle ne reçoit pas les informations sur les témoins des clients pour les demandes HTTPS et FTP sur HTTP. Par conséquent, elle ne peut pas obtenir le nom d'utilisateur à partir du témoin.

Substituts d'authentification pris en charge pour les demandes explicites

Types de substitution	Chiffrement des informations d'authentification désactivé			Chiffrement des informations d'authentification activé		
Protocole :	HTTP	HTTPS et FTP sur HTTP	FTP natif	HTTP	HTTPS et FTP sur HTTP	FTP natif
Aucun modèle de substitution	Oui	Oui	Oui	S.O.	S.O.	S.O.
Basé sur IP	Oui	Oui	Oui	Oui	Oui	Oui
Basés sur les témoins	Oui	Oui***	Oui***	Oui	Non/Oui**	Oui***

Substituts d'authentification pris en charge pour les demandes transparentes

Note Consultez également la description des options de substitution d'authentification dans Classification des utilisateurs et logiciels clients.

Types de substitution	Chiffrement des informations d'authentification désactivé			Chiffrement des informations d'authentification activé		
Protocole :	HTTP	HTTPS	FTP natif	HTTP	HTTPS	FTP natif
Aucun modèle de substitution	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
Basé sur IP	Oui	Non/Oui*	Non/Oui*	Oui	Non/Oui*	Non/Oui*
Basés sur les témoins	Oui	Non/Oui**	Non/Oui**	Oui	Non/Oui**	Non/Oui**

* Fonctionne après que le client a envoyé une demande à un site HTTP et qu'il est authentifié. Avant que cela ne se produise, le comportement dépend du type de transaction :

- **Transactions FTP natives.** Contournement de l'authentification des transactions.
- **Transactions HTTPS.** Les transactions sont abandonnées. Cependant, vous pouvez configurer le proxy HTTPS pour déchiffrer la première requête HTTPS à des fins d'authentification.

** Lorsque l'authentification basée sur les témoins est utilisée, le proxy Web ne peut pas authentifier l'utilisateur pour les transactions HTTPS, FTP natif et FTP sur HTTP. En raison de cette limitation, toutes les demandes HTTPS, FTP natives et FTP sur HTTP contournent l'authentification, donc l'authentification n'est pas demandée du tout.

*** Aucune substitution n'est utilisée dans ce cas, même si la substitution basée sur les témoins est configurée.

Thèmes connexes

- Profils d'identification et authentification

Suivi des utilisateurs réauthentifiés

Avec la réauthentification, si un utilisateur plus privilégié s'authentifie et est autorisé, le proxy Web met en cache l'identité de cet utilisateur pendant différentes durées selon les substitutions d'authentification configurées :

- **Session cookie** (Témoin de session). L'identité de l'utilisateur privilégié est utilisée jusqu'à ce que le navigateur soit fermé ou que la session expire.
- **Persistent cookie** (Témoin persistant). L'identité de l'utilisateur privilégié est utilisée jusqu'à ce que la substitution expire.
- **IP address** (Adresse IP). L'identité de l'utilisateur privilégié est utilisée jusqu'à ce que la substitution expire.

- **No surrogate** (Aucune substitution). Par défaut, le proxy Web demande l'authentification à chaque nouvelle connexion, mais lorsque la réauthentification est activée, le proxy Web demande l'authentification à chaque nouvelle demande, ce qui entraîne une charge accrue du serveur d'authentification lors de l'utilisation de NTLMSSP. Cependant, il est possible que l'augmentation de l'activité d'authentification ne soit pas visible pour un utilisateur, car la plupart des navigateurs mettent en cache les informations d'authentification de l'utilisateur privilégié et s'authentifient sans invite jusqu'à la fermeture du navigateur. En outre, lorsque le proxy Web est déployé en mode transparent et que l'option « Apply same surrogate settings to explicit forward requests » (Appliquer les mêmes paramètres de substitution aux demandes de transfert explicites) n'est pas activée, aucune substitution d'authentification n'est utilisée pour les demandes de transfert explicites et la réauthentification se produira.

Note Si Secure Web Appliance utilise des témoins pour les substitutions d'authentification, Cisco recommande d'activer le chiffrement des identifiants.

Informations d'authentification

Les informations d'authentification des utilisateurs peuvent être obtenues auprès des utilisateurs en étant invités à les saisir dans leur navigateur ou dans une autre application cliente, ou en obtenant les identifiants de manière transparente d'une autre source.

Suivi des informations d'authentification pour leur réutilisation au cours d'une session

Grâce aux substitutions d'authentification, après l'authentification d'un utilisateur au cours d'une session, vous pouvez suivre les informations d'authentification en vue de les réutiliser tout au long de la session plutôt que de demander à l'utilisateur de s'authentifier à chaque nouvelle demande. Les substitutions d'authentification peuvent être basées sur l'adresse IP du poste de travail de l'utilisateur ou sur un témoin affecté à la session.

Pour Internet Explorer, assurez-vous que le nom d'hôte de redirection est le nom d'hôte court (ne contenant pas de points) ou le nom NetBIOS plutôt qu'un domaine qualifié complet. Vous pouvez également ajouter le nom d'hôte de l'appliance à la zone intranet local d'Internet Explorer [Tools > Internet options > Security tab (Outils > options Internet > onglet Sécurité)]. Cependant, cela sera requis sur chaque client. Pour plus d'informations à ce sujet, consultez Comment puis-je configurer correctement NTLM avec SSO (les informations d'authentification envoyées de manière transparente)?

Avec les navigateurs Firefox et d'autres navigateurs autres que Microsoft, les paramètres **network.negotiate-auth.delegation-uris**, **network.negotiate-auth.trusted-uris** et **network.automatic-ntlm-auth.trusted-uris** doivent être définis sur le nom d'hôte de redirection en mode transparent. Vous pouvez également vous reporter à Firefox n'envoie pas les informations d'authentification de manière transparente (SSO). Cet article fournit des informations générales sur la modification des paramètres de Firefox.

Pour en savoir plus sur le nom d'hôte de redirection, consultez Configuration des paramètres d'authentification globaux, on page 31 ou la commande d'interface de ligne de commande `sethostname`.

Échecs d'authentification et d'autorisation

Si l'authentification échoue pour des raisons acceptées, comme des applications client incompatibles, vous pouvez accorder l'accès en tant qu'invité.

Si l'authentification réussit, mais que l'autorisation échoue, il est possible d'autoriser la nouvelle authentification en utilisant un autre ensemble d'identifiants qui peuvent être autorisés à accéder à la ressource demandée.

Thèmes connexes

- Octroi d'un accès invité après échec de l'authentification, on page 44
- Autorisation de réauthentification avec des informations d'authentification différentes, on page 46

Format des informations d'authentification

Schéma d'authentification	Format des informations d'authentification
NTLMSSP	**`MonDomaine\jdupont`**
Basic (niveau de base)	**`jdupont`** **`MonDomaine\jdupont`** **Note** Si l'utilisateur ne saisit pas le domaine Windows, le proxy Web ajoute le domaine Windows par défaut au début.

Chiffrement des informations d'authentification pour l'authentification de base

À propos du chiffrement des informations d'authentification pour l'authentification de base

Activez le chiffrement des informations d'identification pour transmettre les informations d'authentification sur HTTPS sous forme chiffrée. Cela augmente la sécurité du processus d'authentification de base.

Le Secure Web Appliance utilise ses propres certificat et clé privée par défaut pour créer une connexion HTTPS avec le client à des fins d'authentification sécurisée. La plupart des navigateurs avertissent cependant les utilisateurs que ce certificat n'est pas valide. Pour empêcher les utilisateurs de voir le message de certificat non valide, vous pouvez télécharger un certificat valide et une paire de clés que votre organisation utilise.

Configuration du chiffrement des informations d'authentification

Before you begin

- Configurez l'appliance pour utiliser les substitutions d'adresses IP.
- (Facultatif) Obtenez un certificat et une clé privée non chiffrée. Le certificat et la clé configurés ici sont également utilisés par le contrôle d'accès.

Étape 1 Choisissez **Network > Authentication** (Réseau > Authentification).

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

Étape 3 Cochez la case **Use Encrypted HTTPS Connection For Authentication** (Utiliser la connexion HTTPS chiffrée pour l'authentification) dans le champ Credential Encryption (Chiffrement des informations d'authentification).

Étape 4 (Facultatif) Modifiez le numéro de port par défaut (443) dans le champ HTTPS Redirect Port (Port de redirection HTTPS) pour les connexions HTTP du client lors de l'authentification.

Étape 5 (Facultatif) Charger le certificat et la clé :

a) Développez la section Advanced (Niveau avancé).
b) Cliquez sur **Browse** (Parcourir) dans le champ Certificat (Certificate) et trouvez le fichier de certificat que vous souhaitez télécharger.
c) Cliquez sur **Browse** (Parcourir) dans le champ Key (Clé) et trouvez le fichier de clé privée que vous souhaitez télécharger.
d) Cliquez sur **Upload Files** (Charger des fichiers).

Étape 6 Envoyez et validez vos modifications.

What to do next

Thèmes connexes

- Certificate Management.

Résolution de problèmes liés à l'authentification

- Échec d'authentification de l'utilisateur LDAP en raison du protocole NTLMSSP
- Échec de l'authentification LDAP en raison du renvoi au protocole LDAP
- Échec de l'authentification de base
- Utilisateurs invités par erreur à fournir des informations d'authentification
- Les demandes HTTPS et FTP via HTTP correspondent uniquement aux politiques d'accès qui ne nécessitent pas d'authentification
- Impossible d'accéder aux URL qui ne prennent pas en charge l'authentification
- Échec des demandes du client au proxy en amont

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.