

Comment est-ce que j'installe correctement NTLM avec SSO (qualifications envoyées d'une manière transparente) ?

Contenu

Question :

Symptômes : Le navigateur incite pour des qualifications quand l'authentification NTLM est utilisée.

Environnement : Appliance de sécurité Web de Cisco (WSA), toutes les versions d'AsyncOS

Plusieurs facteurs pourraient affecter si le client envoie ses qualifications automatiquement (SSO - simple connectez-vous), ou incitent l'utilisateur final à entrer dans manuellement leurs qualifications.

Vérifiez les articles suivants en tentant d'implémenter NTLM avec SSO :

Configuration d'authentification WSA :

Vérifiez que le WSA n'est installé pour utiliser NTLMSSP et pas NTLM de base seulement

Cette configuration peut être trouvée sur le GUI sous la page de **gestionnaire > d'identités de sécurité Web**. Éditez l'identité appropriée et puis vérifiez les **membres de définir par l'établissement d'authentification > de modèles d'authentification**.

Sélectionnez une des options suivantes :

NTLMSSP permet à la fonctionnalité pour que le client envoie les qualifications sécurisé et d'une manière transparente au proxy de Web.

NTLM de base permet au client pour envoyer le nom d'utilisateur et mot de passe en texte brut une fois incité pour les qualifications.

Le client choisit la meilleure méthode disponible quand l'**utilisation de base** ou l'option **NTLMSSP** est (recommandé) sélectionné. Si le client prend en charge NTLMSSP, il utilisera cette méthode, et tous autres navigateurs utiliseront de base. Ceci tient compte de la compatibilité maximum.

Confiance de client :

Si le client ne fait pas confiance au WSA, il ne l'enverra pas est des qualifications d'une manière

transparente. Ce qui suit sont des instructions à aider à dépanner des environnements où le client ne fait pas confiance au WSA.

Le client ne fait pas confiance à l'URL de redirection d'authentification (les déploiements transparents seulement)

Dans un déploiement transparent, le WSA doit réorienter le client à lui-même afin d'exécuter l'authentification. Le client peut ou peut ne pas faire confiance à cet emplacement réorienté.

Par défaut, les redirect to WSA le FQDN du P1 (ou l'interface M1 si elle est utilisée pour des données de proxy). Puisque c'est un FQDN, l'Internet Explorer ne lui fera pas confiance, comme il croit que c'est une ressource en dehors de son réseau.

Il y a deux manières d'inciter l'Internet Explorer à faire confiance au WSA :