Guide de démarrage rapide – Authentification

INTRODUCTION

WebTitan Web Filter permet de définir comment les utilisateurs s'authentifient avant d'accéder à des sites Web externes.

Par défaut, l'authentification est désactivée. Cela signifie que n'importe quel utilisateur est accepté par l'appliance WebTitan Web Filter sans authentification. Si l'authentification est nécessaire, il est possible de l'activer via Paramètres système-> onglet Authentification, comme illustré ci-dessous. La méthode d'authentification peut être sélectionnée dans la liste déroulante « Type de politique ». WebTitan Web Filter propose les différentes méthodes d'authentification de l'utilisateur suivantes :

- authentification basée sur l'IP,
- authentification basée sur LDAP,
- authentification basée sur NTLM,
- authentification basée sur l'IP et LDAP,
- authentification basée sur l'IP et NTLM,
- authentification NTLM en mode transparent via WADA (WebTitan Web Filter Active Directory Agent).

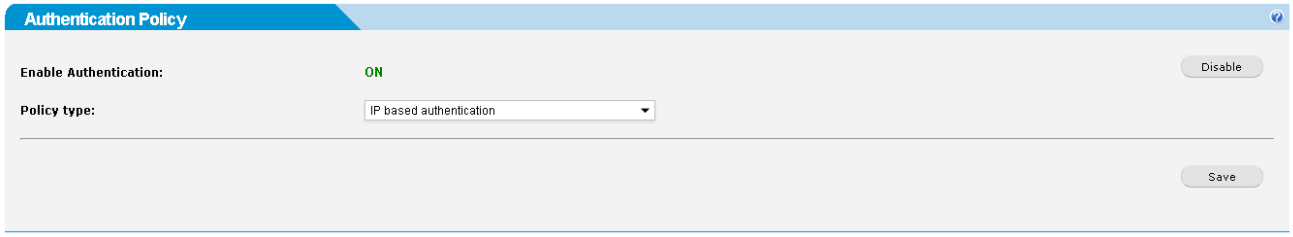

Illustration 1 : Paramètres d'authentification

L'authentification par l'adresse IP et l'authentification NTLM sont transparentes pour l'utilisateur alors que l'authentification LDAP nécessitera que l'utilisateur saisisse ses références d'authentification (nom d'utilisateur/mot de passe) LDAP avant de commencer à naviguer sur le Web. Ces informations ne lui seront demandées qu'une seule fois.

AUTHENTIFICATION IP

L'authentification IP ne convient que lorsque les utilisateurs ont des adresses IP statiques. Il est également recommandé d'utiliser l'authentification LDAP ou NTLM lorsque des serveurs LDAP sont utilisés pour gérer les utilisateurs et les groupes dans WebTitan Web Filter. Pour faciliter l'authentification IP dans WebTitan Web Filter, il est nécessaire de procéder comme suit :

- Il est nécessaire d'activer l'authentification IP via Paramètres système > onglet Authentification.
- Des adresses IP doivent être assignées aux utilisateurs via Utilisateurs et groupes > onglet Utilisateurs. Une adresse IP peut être assignée lors de la création de l'utilisateur ou en modifiant un utilisateur existant. La figure 2 ci-dessous montre que l'on peut assigner aux utilisateurs une seule adresse IP et une série d'adresses IP.

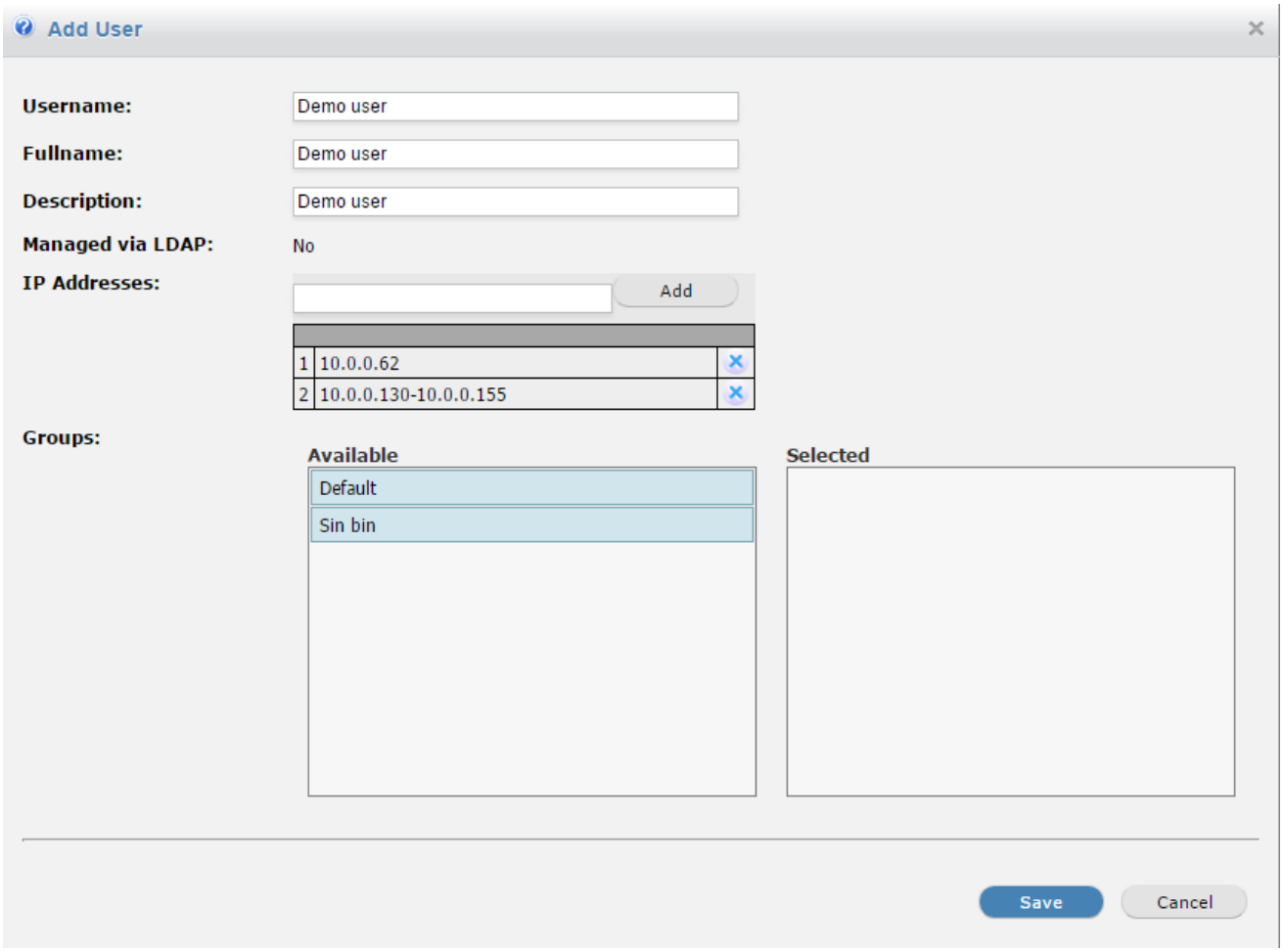

Illustration 2 : Boîte de dialogue Ajouter des utilisateurs

Points relatifs à l'authentification IP

- L'authentification IP est transparente pour l'utilisateur final.
- L'authentification IP doit être utilisée uniquement pour les adresses IP statiques.

AUTHENTIFICATION LDAP

L'authentification LDAP convient lorsque les utilisateurs et les groupes sont gérés par un serveur LDAP et que l'on préfère que l'utilisateur saisisse ses références d'authentification (nom d'utilisateur/mot de passe) LDAP avant de commencer sa navigation sur le Web.

Pour faciliter l'authentification LDAP dans WebTitan Web Filter, il est nécessaire de procéder comme suit :

- Il est nécessaire d'activer l'authentification LDAP via Paramètres système > onglet Authentification.
- Au moins un serveur LDAP doit être spécifié dans Utilisateurs et groupes > onglet Utilisateurs*.

- Les utilisateurs associés au serveur LDAP d'authentification doivent être importés dans WebTitan Web Filter.

L'illustration 3 est une capture d'écran de l'authentification LDAP activée dans WebTitan Web Filter. La figure suivante montre une capture de l'invite demandant à l'utilisateur ses identifiants LDAP. Ces identifiants ne doivent être saisies qu'une seule fois.

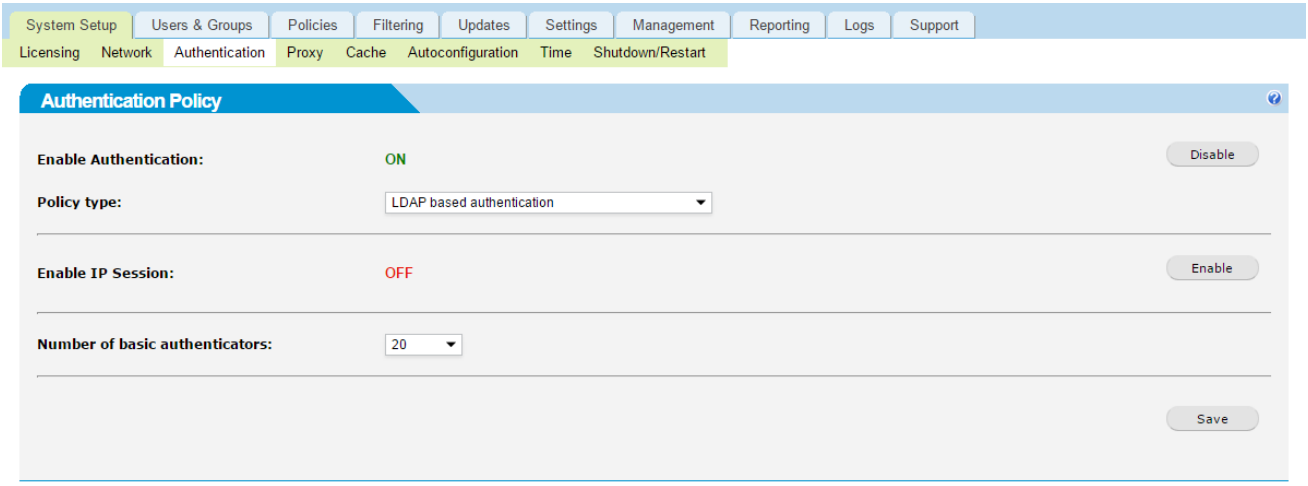

Illustration 3 : Paramètres d'authentification LDAP

* Veuillez consulter le « Guide de démarrage rapide – Configuration LDAP » pour plus d'informations sur comment se connecter à un serveur LDAP dans WebTitan Web Filter et comment importer des utilisateurs LDAP.

Illustration 4 : Fenêtre contextuelle d'authentification LDAP d'Internet Explorer

Si l'utilisateur Web entre un nom d'utilisateur ou un mot de passe incorrect, il reçoit la page Web suivante :


Access Denied

You have attempted to access the following web page:

http://helpdesk.webtitan.com/index.php/tickets

Access has been blocked because:

Authentication failed - username or password incorrect

Management have deemed that access to this web page is inappropriate at this time. Please contact your supervisor if you feel that this is incorrect.

Generated on Mon, 23 Nov 2009 15:29:05 +0000

Illustration 5 : Page d'échec d'authentification

Points relatifs à l'authentification LDAP

- L'authentification LDAP exige que l'utilisateur saisisse ses identifiants LDAP.

AUTHENTIFICATION NTLM

Si votre réseau utilise l'authentification NTLM, alors les utilisateurs peuvent être authentifiés de manière transparente par WebTitan Web Filter à l'aide de leurs identifiants Microsoft Windows.

Pour faciliter l'authentification NTLM dans WebTitan Web Filter, il est nécessaire de procéder comme suit :

- Il est nécessaire d'activer l'authentification NTLM via Paramètres système > onglet Authentification.

- Les utilisateurs doivent naviguer à l'aide d'Internet Explorer ou de Mozilla Firefox.

La figure 6 ci-dessous montre un exemple de paramètres d'un serveur NTLM. La vérification des paramètres est effectuée automatiquement une fois que vous avez cliqué sur le bouton «Enregistrer ».

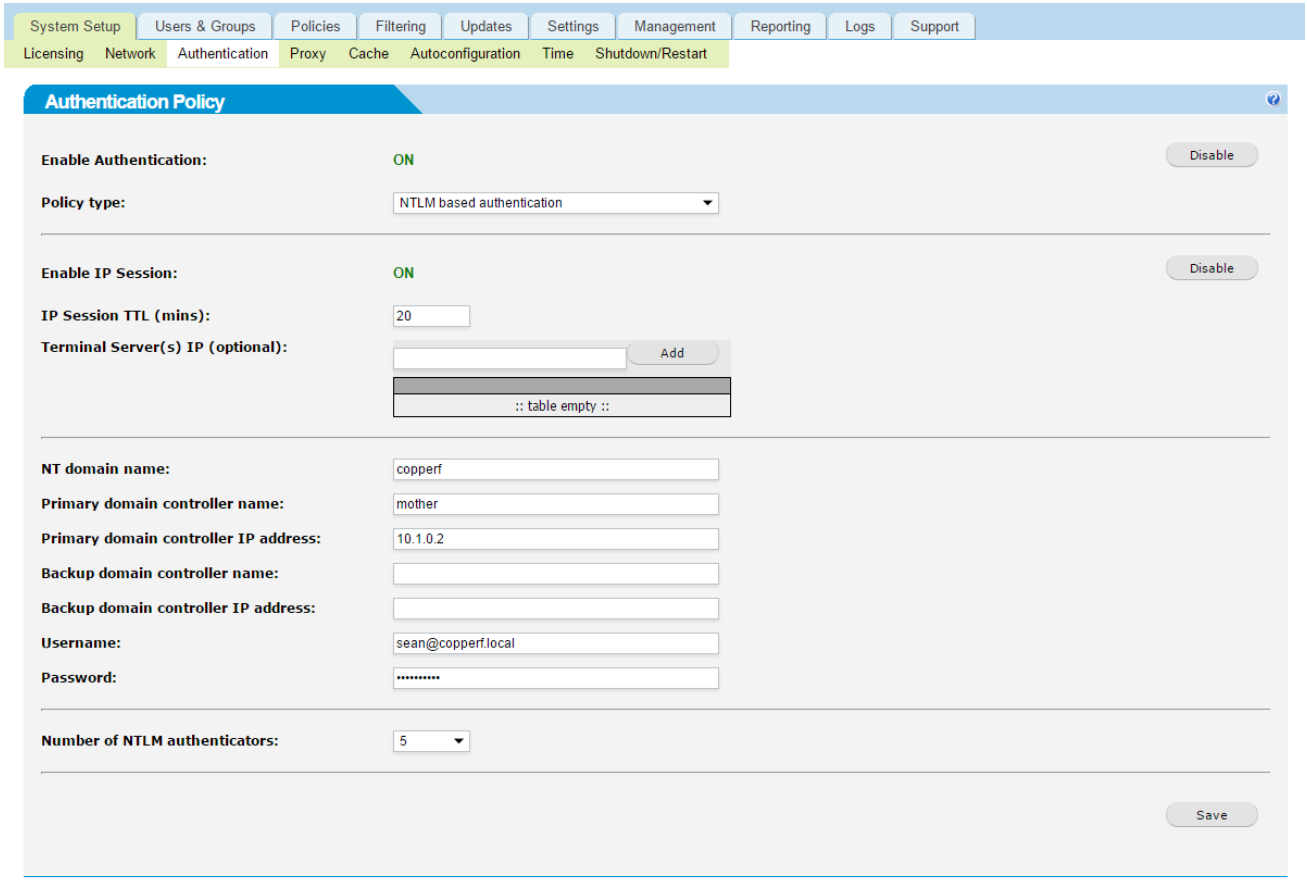

Illustration 6 : Paramètres d'authentification NTLM

Si votre serveur NTLM ne parvient pas à vous authentifier, les codes d'erreur suivants renvoyés par WebTitan Web Filter peuvent vous être utiles.

Code d'erreur	Explication
- 1	L'authentification NTLM n'est pas activée.
- 2	Le nom d'utilisateur ou le mot de passe est incorrect.
- 3	Impossible de se connecter aux contrôleurs de domaine.
- 4	La commande /usr/local/bin/net join a échoué pour une autre raison.
- 5	winbindd ne fonctionne pas (wbinfo -p).
- 6	winbindd ne fonctionne pas correctement (wbinfo -t).

Points relatifs à l'authentification NTLM

- L'authentification NTLM est transparente pour l'utilisateur final.
- L'authentification NTLM ne fonctionne qu'avec Internet Explorer et Mozilla Firefox.
- Les utilisateurs ne correspondant à aucun compte d'utilisateur NTLM sont automatiquement contrôlés par la politique « Par défaut » et apparaissent dans les rapports en tant qu'utilisateur « GDefault ».

WEBTITAN WEB FILTER ACTIVE DIRECTORY AGENT (WADA)

WebTitan Web Filter Active Directory Agent (WADA) est un service de Windows qui dresse une liste des sessions de connexion actives et mappe une adresse IP à un nom d'utilisateur. Ces informations sont ensuite transmises à WebTitan Web Filter pour permettre d'utiliser des règles de filtrage des utilisateurs appliquées en fonction des paramètres des politiques relatives aux utilisateurs connectés.

Ces informations sont récoltées à partir de 3 sources différentes existant sur le réseau Windows :

- LDAP,
- Journal des événements,
- sessions réseau.

Le mécanisme LDAP collecte une liste d'ordinateurs dans le domaine et, en fonction du paramètre lastLogon (Dernière connexion), contacte chaque ordinateur en utilisant le protocole WMI afin de vérifier les sessions de connexion actives et, finalement, obtient le nom d'utilisateur. Tous les ordinateurs ne sont pas contrôlés ; seuls ceux dont le champ lastLogon se trouve dans la plage définie dans la configuration (1 an par défaut).

Le mécanisme Journal des événements écoute l'enregistreur d'événements et recherche certains événements qui contiennent des informations sur le nom d'utilisateur et l'IP.

En outre, les sessions réseau sont comptées (toutes les 10 secondes par défaut) pour découvrir les sessions actives. Cette méthode est importante, notamment lorsqu'il y a des utilisateurs sur le réseau qui n'éteignent pas leur ordinateur pendant longtemps et que, pour une raison quelconque, leur ordinateur n'est pas accessible avec WMI.

Les résultats de toutes ces méthodes sont ensuite fusionnés en une liste et transmis à WebTitan Web Filter.

INSTALLATION DE WADA

Installez-le sur le serveur Active Directory ou sur un autre serveur du domaine. L'installation est simple et utilise le kit MSI WADA comme illustré ci-dessous.

Illustration 7 : Installation de WADA

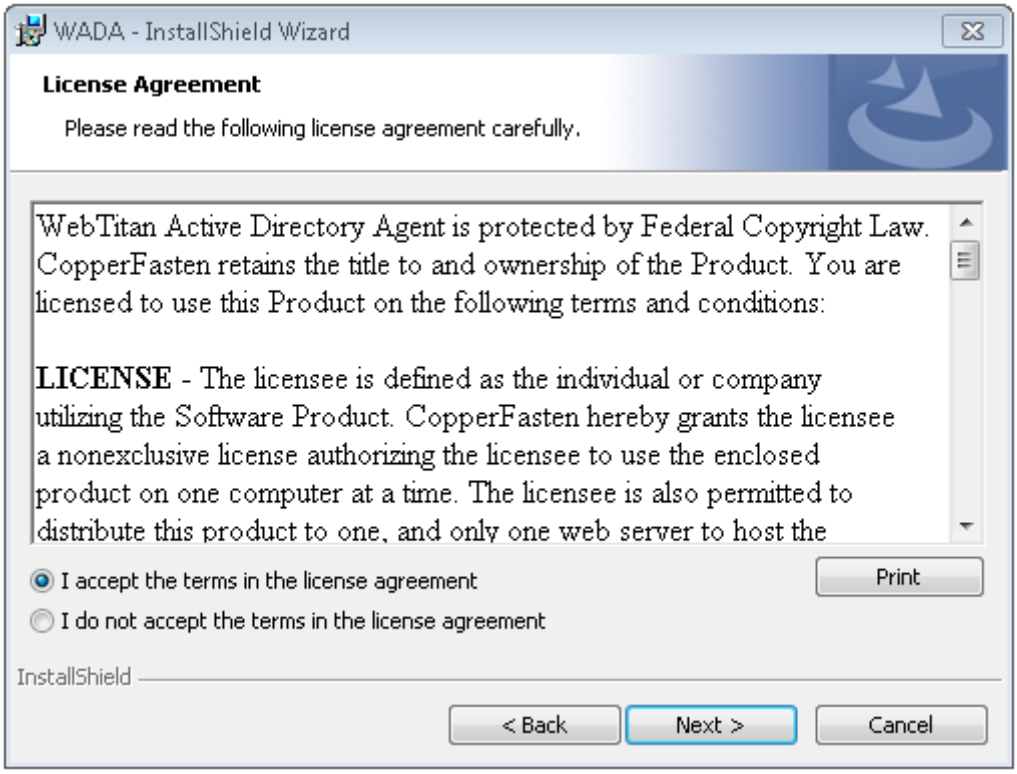

Illustration 8 : Installation de WADA – Acceptation de la licence

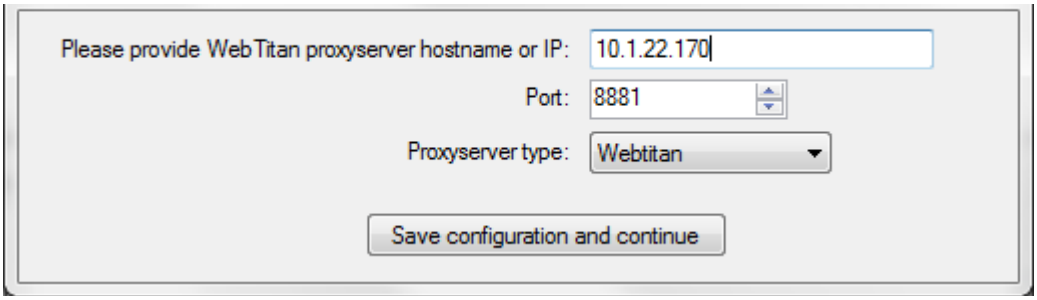

Illustration 9 : Installation de WADA – Paramètres de serveur d'WebTitan Web Filter

Saisissez l'adresse IP d'WebTitan Web Filter.
REMARQUE : Indiquez le port du proxy sur lequel WebTitan Web Filter est à l'écoute des requêtes HTTP. Par défaut : 8881.

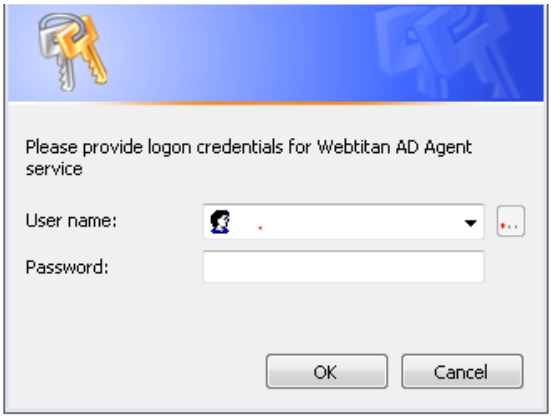

Illustration 10 : Installation de WADA – Références d'authentification AD

Enfin, saisissez vos identifiants de domaine pour votre Active Directory, par exemple: copperf\admin / mot de passe.

ÉTAPES SUIVANTES

Pour mettre en place l'identification des utilisateurs en mode transparent (figure 11), vous devez avoir importé vos utilisateurs depuis Active Directory sur Utilisateurs et groupes -> page Utilisateurs et configurer l'appliance WebTitan Web Filter afin qu'elle fonctionne en mode transparent.

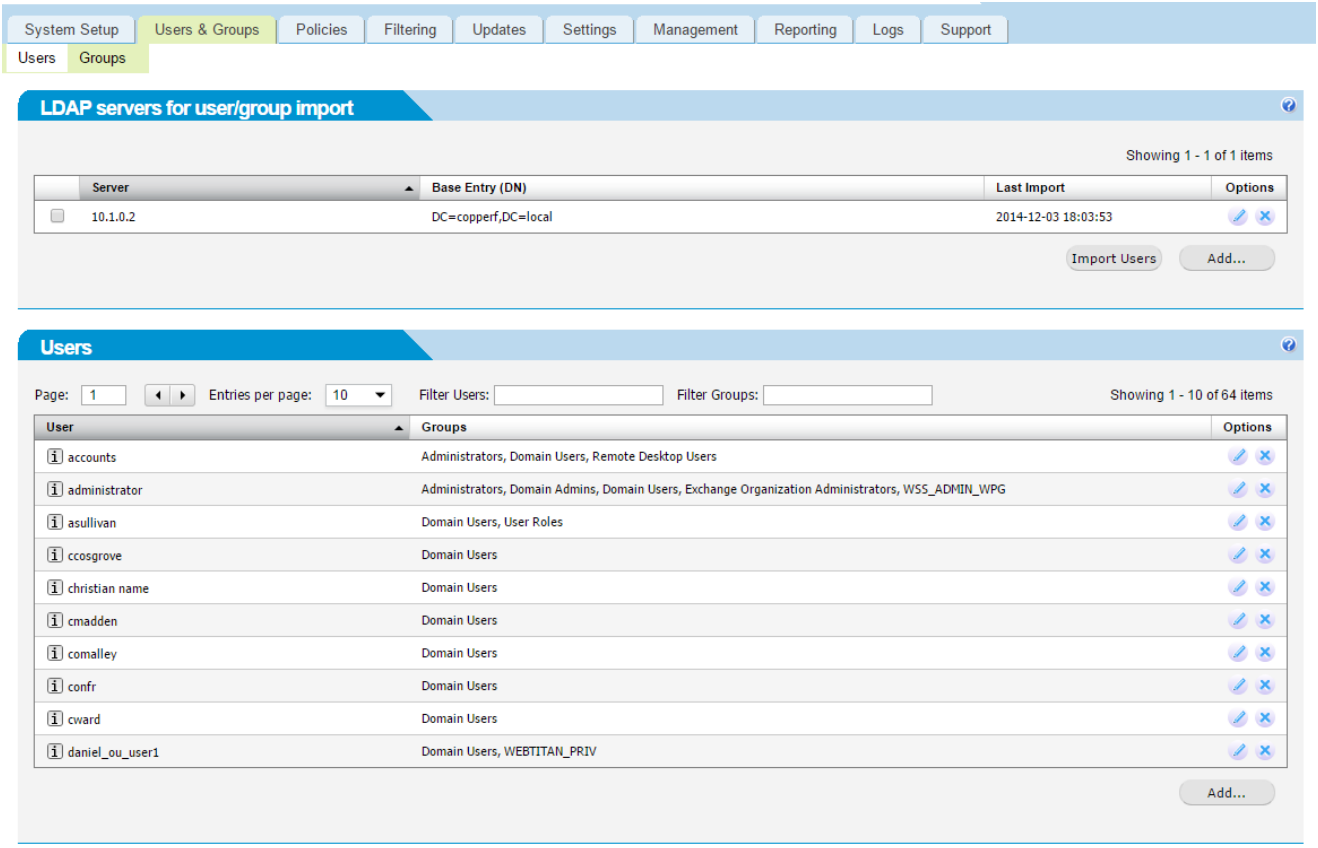

Illustration 11 : Importation d'utilisateurs depuis Active Directory

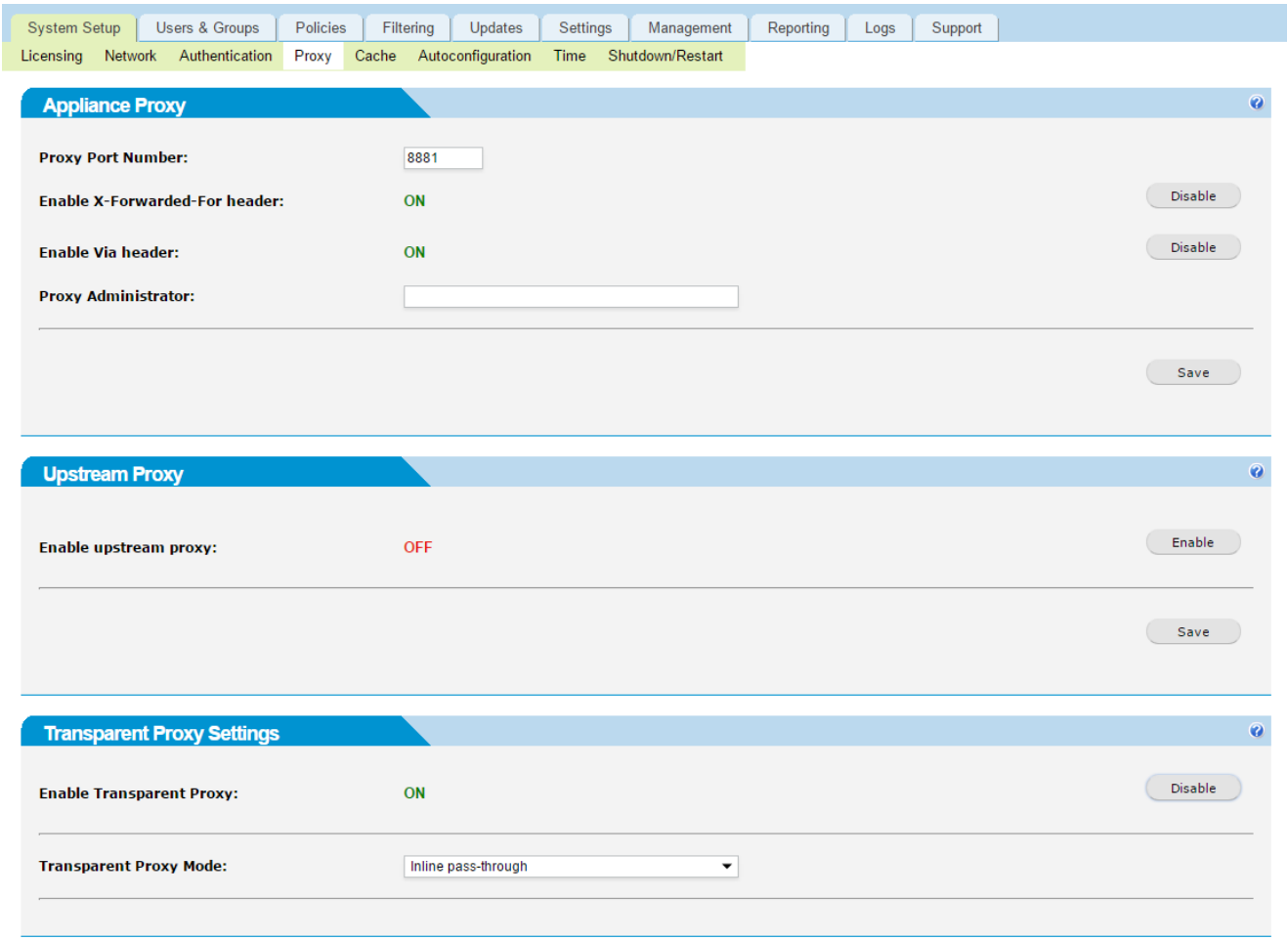

Illustration 12 : Proxy en mode transparent

Sous Configuration du système -> page Authentification, il suffit de choisir l'authentification IP.