VXPERT SYSTEMES

CITRIX NETSCALER 10.1
et
SMS PASSCODE 6.2

Guide d'installation et de configuration pour Xenapp 6.5 avec SMS PASSCODE 6.2

Pour
VXPERT.fr et FGAGNE.COM

François Gagné
fgagne@vxpert.fr

1. Présentation

Cette documentation vous permettra d'installer et de configurer une Appliance Citrix NetScaler en mode proxy (Netscaler Gateway) sécurisée avec SMSPASSCODE.

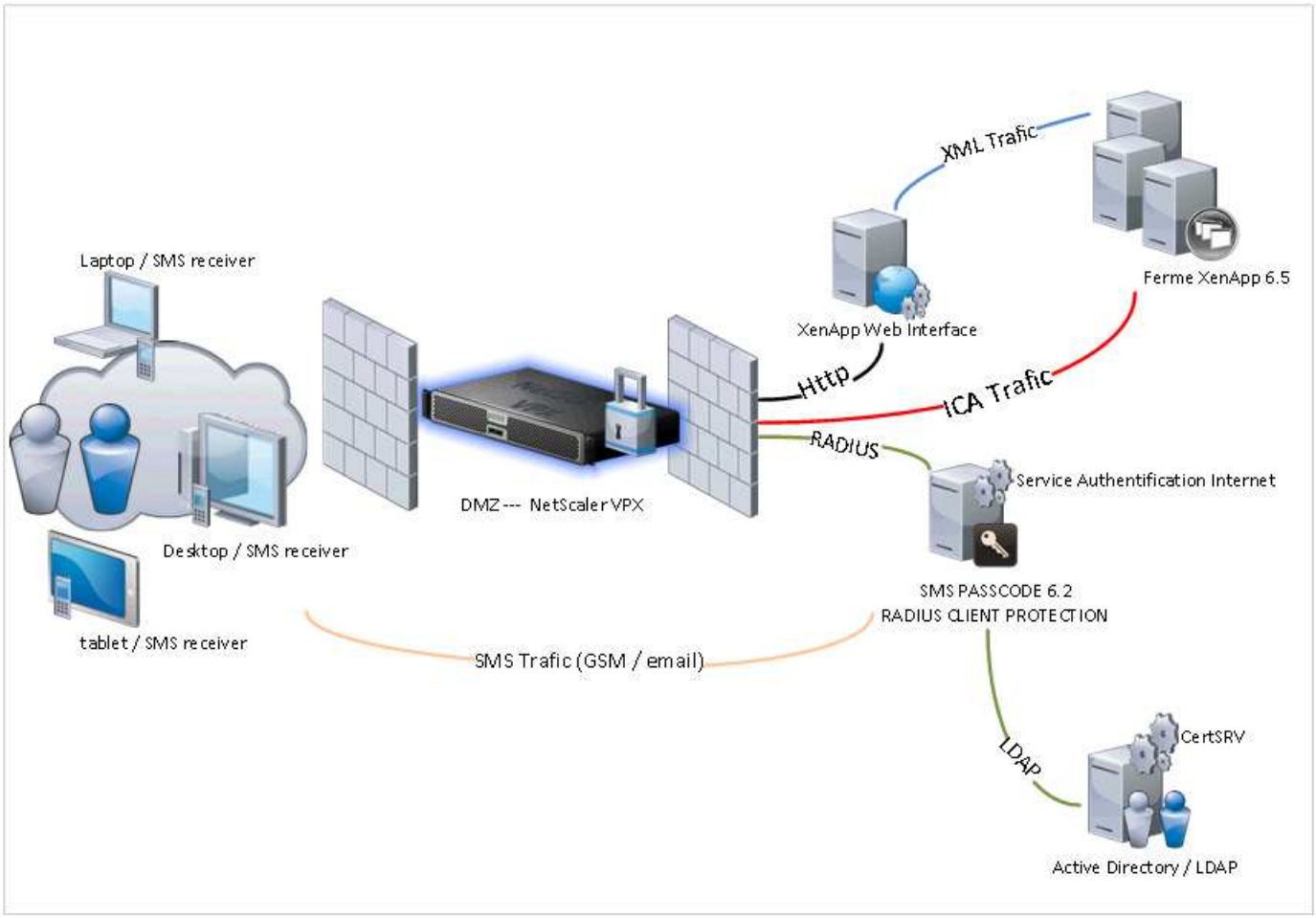
Certains éléments de l'infrastructure ne seront pas abordés dans cette documentation, notamment :

L'installation d'un Active Directory
L'installation de Xenapp 6.5
L'installation de la Web interface Citrix 5.4
L'installation de base de SMSPASSCODE 6.2

Seront traités :
L'installation et la configuration du NetScaler.
La configuration de la partie RADIUS de SMSPASSCODE.
L'installation et la configuration du service d'authentification Internet de Windows 2003.
La customisation de l'interface Web de Citrix.

2. Schéma d’architecture

Ce schéma présente les éléments de l’installation.



3. Installation Netscaler 10.1

Télécharger puis déployer la machine virtuelle NetScaler VPX sur un serveur Vsphere, hyper-v ou Xenserver.

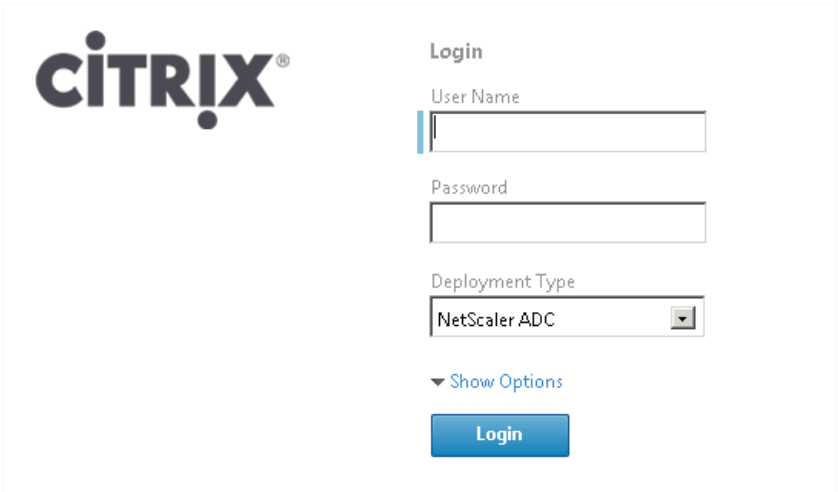
Sous Vpshere, faire **fichier**, **déployer modèle OVF**…

(sinon http://lmgtfy.com/?q=d%C3%A9ployer+un+modele+ovf+sous+vphere)

Démarrer la VM et configurer la partie réseaux.

```
Enter NetScaler's IPv4 address []:



Enter NetScaler's IPv4 address []: 192.168.1.240
Enter Netmask []: 255.255.255.0
Enter Gateway IPv4 address []: 192.168.1.1

------------------------------------------------------------------------------
Netscaler Virtual Appliance Initial Network Address Configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.

After the network changes are saved, you may either login as nsroot and
use the Netscaler command line interface, or use a web browser to
http://192.168.1.240 to complete or change the Netscaler configuration.
------------------------------------------------------------------------------
    1. NetScaler's IPv4 address [192.168.1.240]
    2. Netmask [255.255.255.0]
    3. Gateway IPv4 address [192.168.1.1]
    4. Save and quit
Select item (1-4) [4]:
```

Le reste se fait à partir d'un navigateur internet.

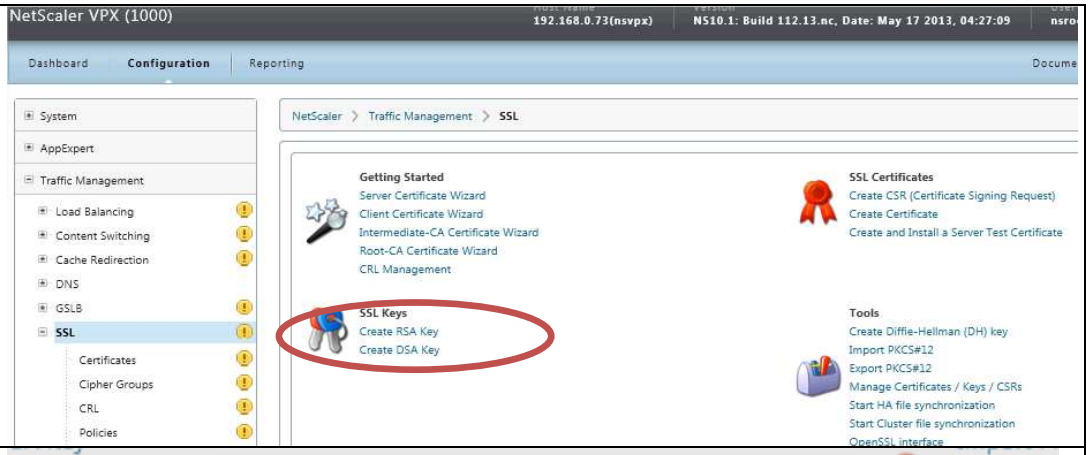


4. Génération du certificat SSL du NetScaler

Pré-requis : avoir installé une licence valide sur le NetScaler.

Lancer la page web de configuration du **NetScaler** et cliquer sur **Traffic Management/SSL** sur la zone de gauche.

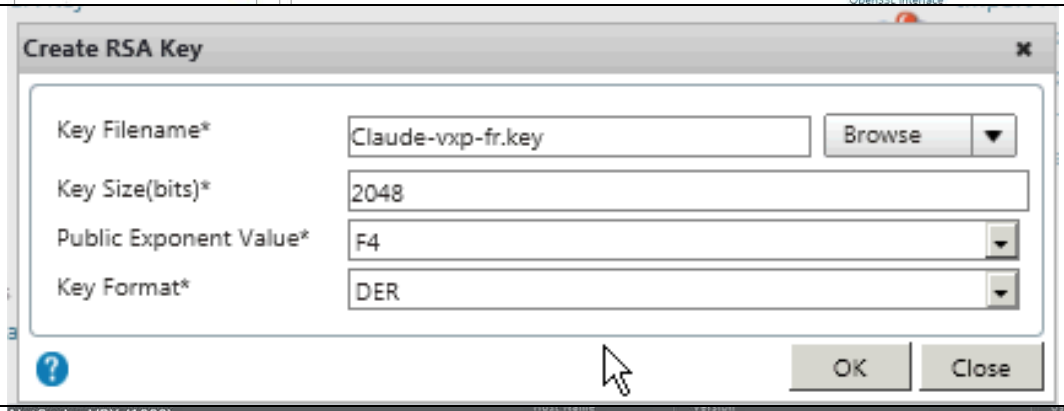
Cliquer sur **Create RSA Key**.



Entrer un nom de fichier en rapport avec votre installation.

Entrer **2048** en tant que key size et choisir le format **DER**.

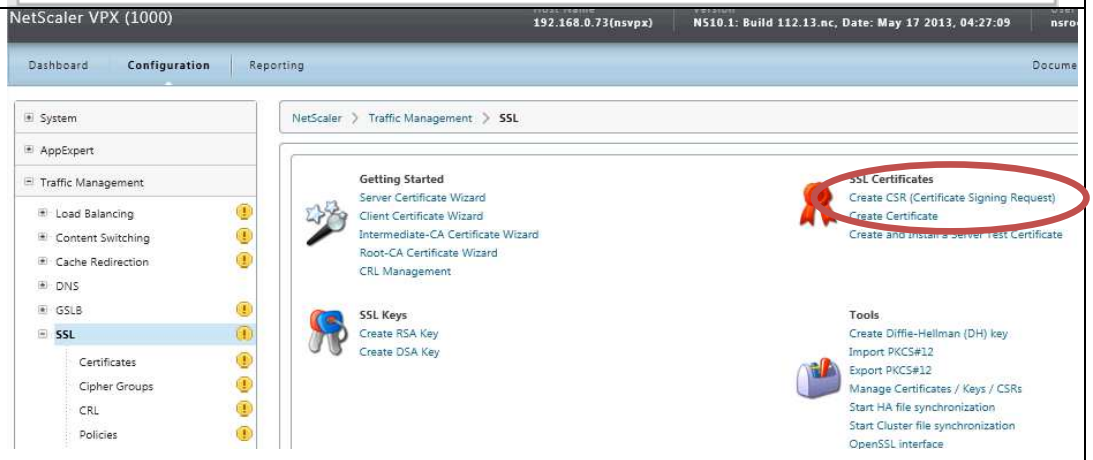
Cliquer sur OK.



Cliquer sur **Create CSR**.

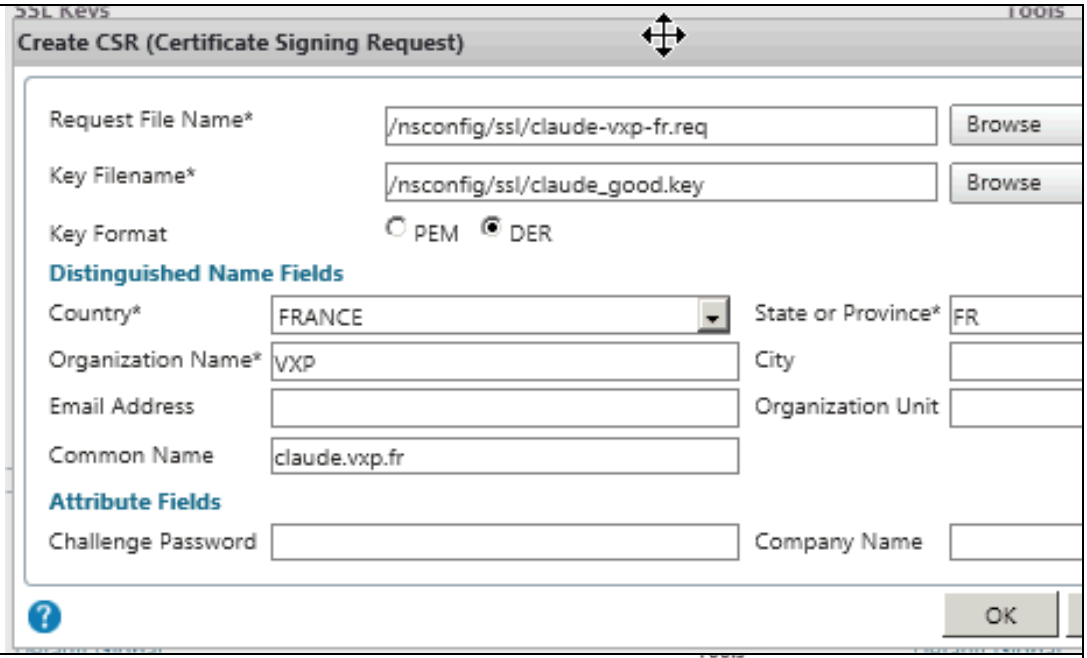
Entrer un nom de fichier pour la demande de certificat (nous vous suggérons une extension req).
Puis rechercher le fichier "clé privée" que vous venez de créer.

Choisir DER en format.



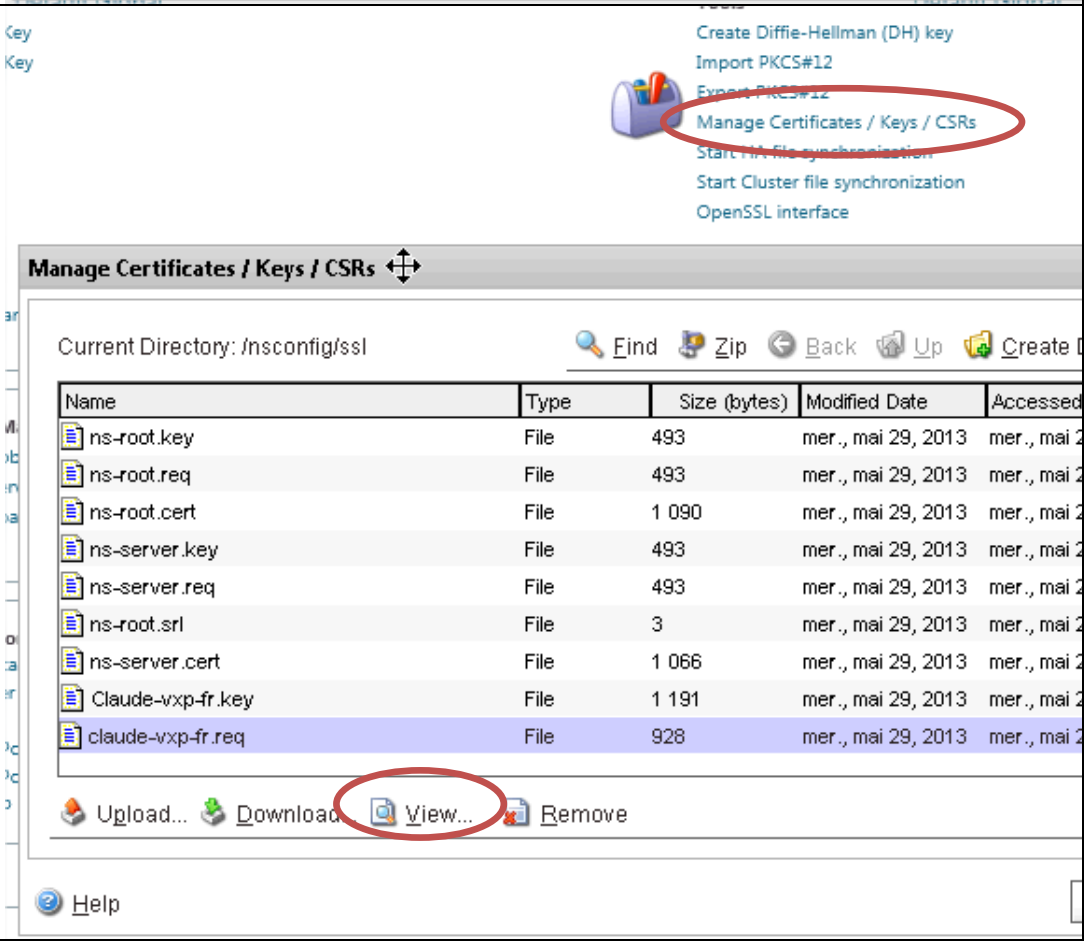
Le champ **Common Name** est très important. Il correspond au **FQDN** final.
Le reste est informatif si une autorité de certification privée (interne à l'entreprise) est utilisée.

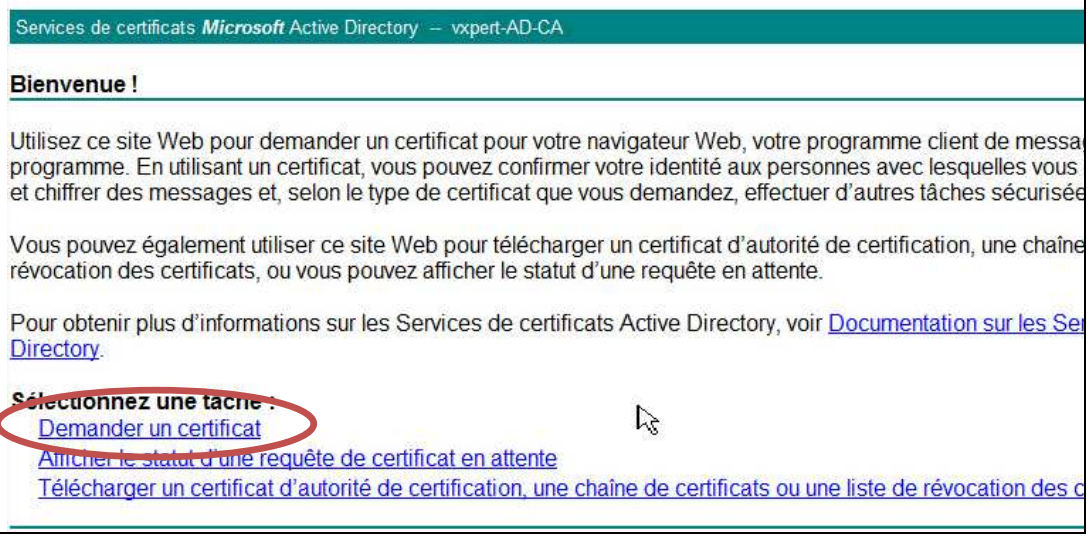
Ensuite cliquer sur **OK**.

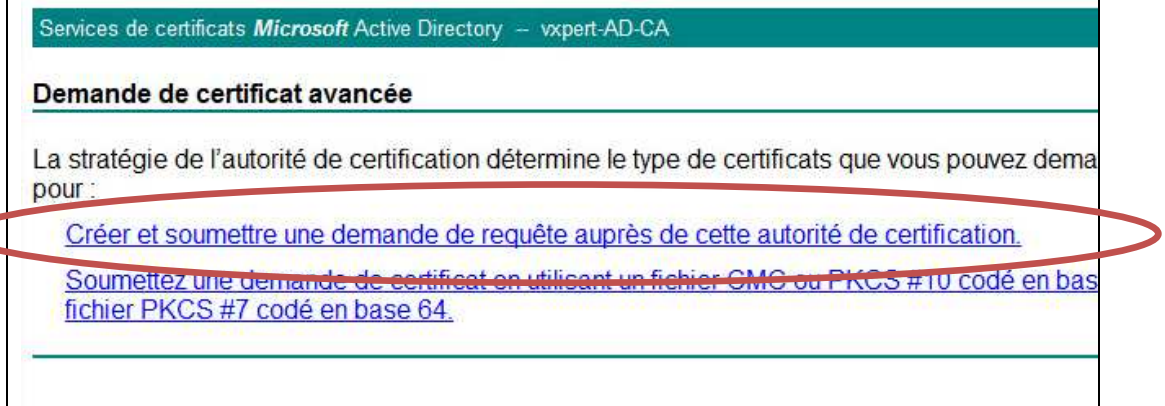


Retourner sur la page SSL.
Cliquer sur **Manage Certificates**.

Naviguer vers le fichier REQ et cliquer sur **View**.



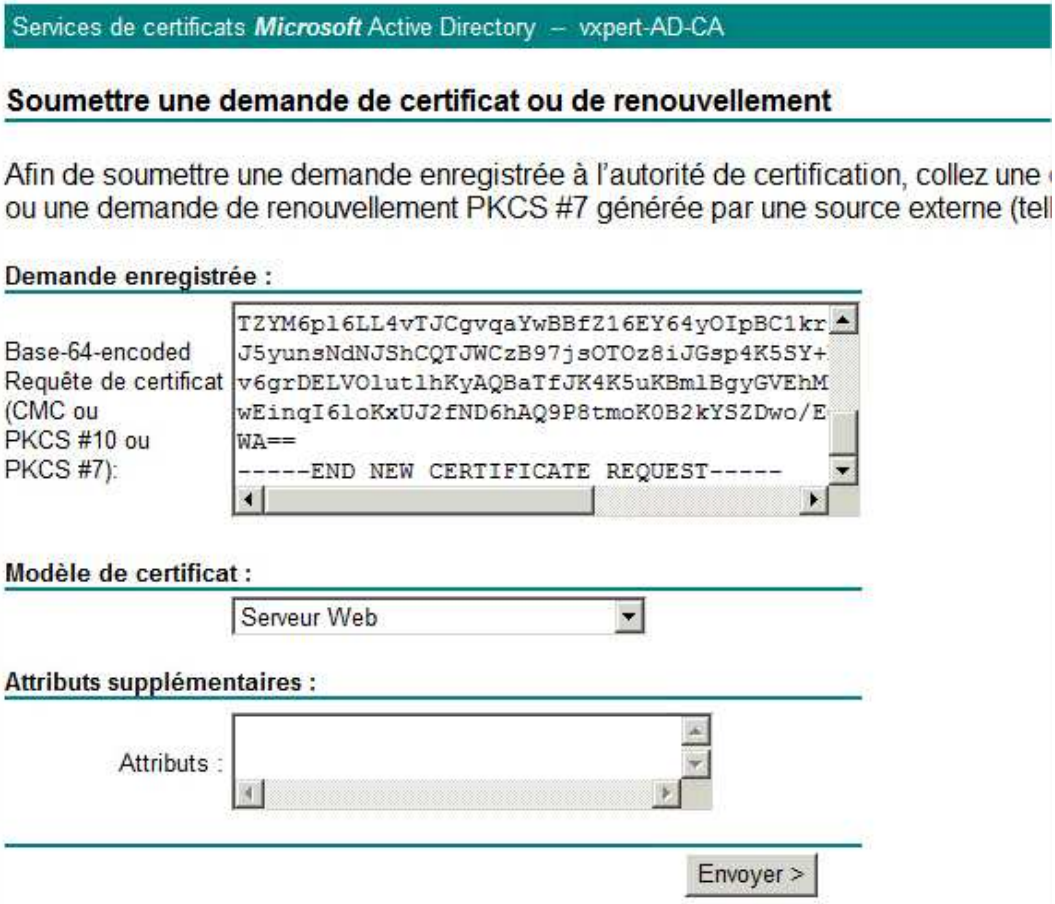
Copier le contenu du fichier dans le presse-papier et fermer la fenêtre.	
Les étapes suivantes sont à effectuer depuis l'interface web de votre serveur d'autorité de certification privée (interne) : Ici, un service de certificats Microsoft Windows 2003. http://%SERVNEAME/certsrv Cliquer sur **Request a certificate**.	

Choisir **Advanced certificate request**.	
Choisir **Submit a certificate request by using a base-64-encoded**…	

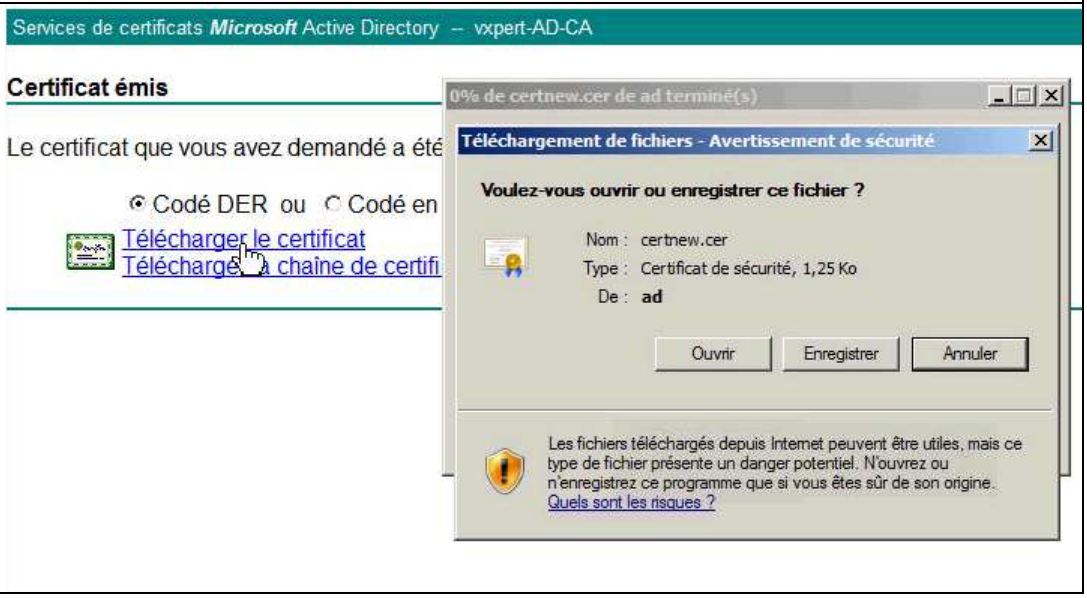
Coller le contenu de votre fichier .req dans la zone demande.

Choisir **Serveur Web** en tant que modèle.

Puis cliquer sur **Envoyer**.

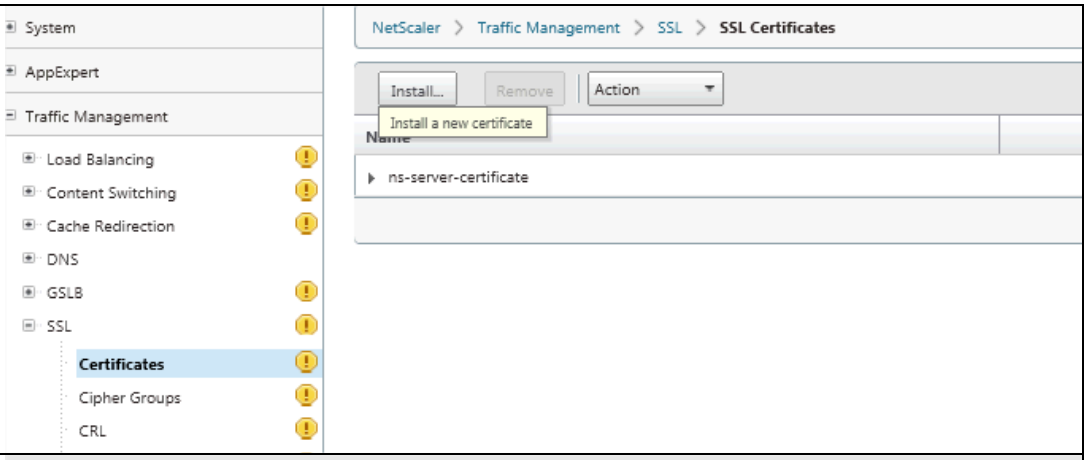


Ensuite, télécharger le certificat au **format DER**.



Retourner sur la console web NetScaler dans la partie **Traffic Management/SSL** puis **SSL Certificates**.

Cliquer sur le bouton **Install…**.

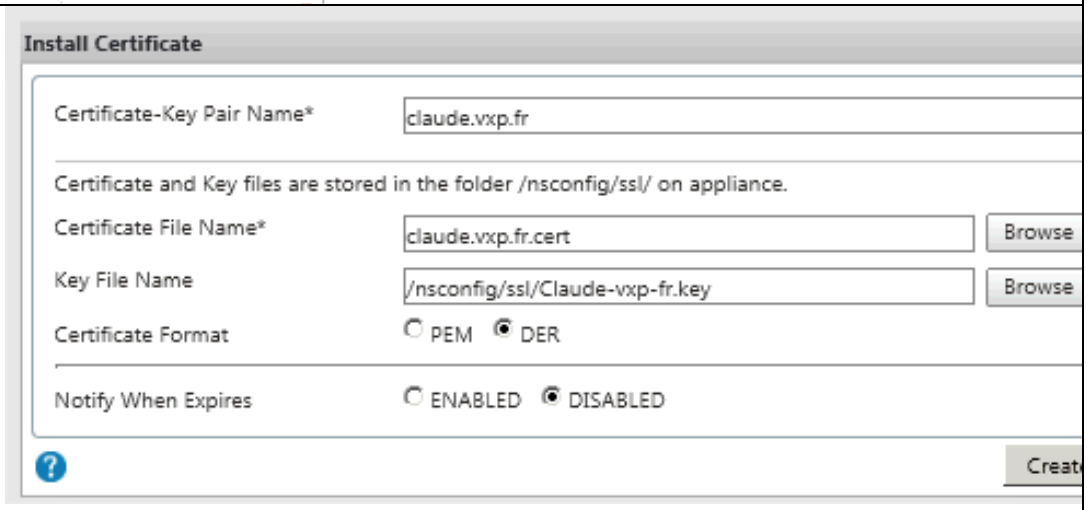


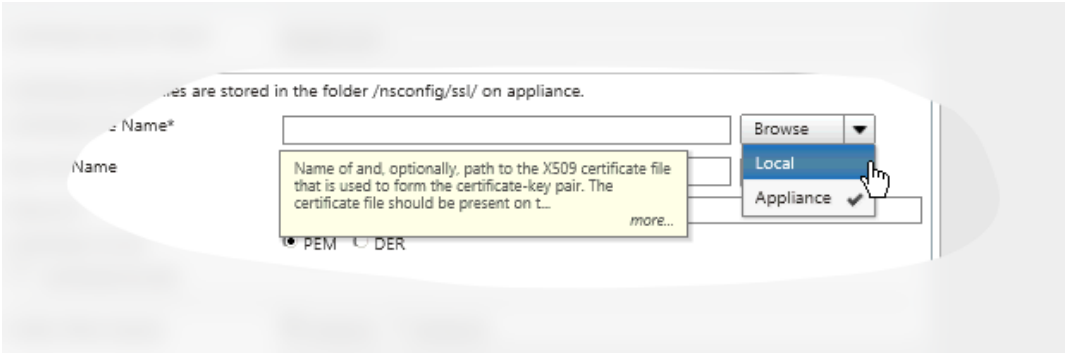
Entrer le "FQDN" dans le champ **Pair Name**.

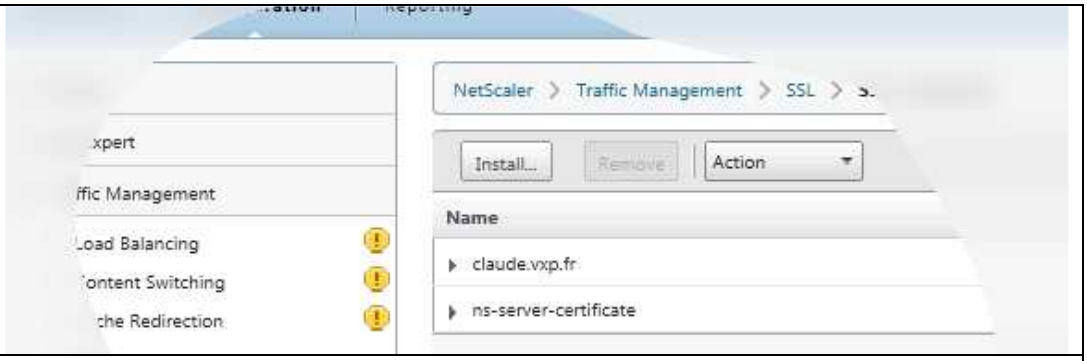
Sélectionner votre fichier cert depuis votre poste de travail (pour cela, cliquer sur Browse et choisir Local),

puis naviguer sur le NetScaler pour la clé privée (fichier .key), et enfin changer le format du certificat en DER.

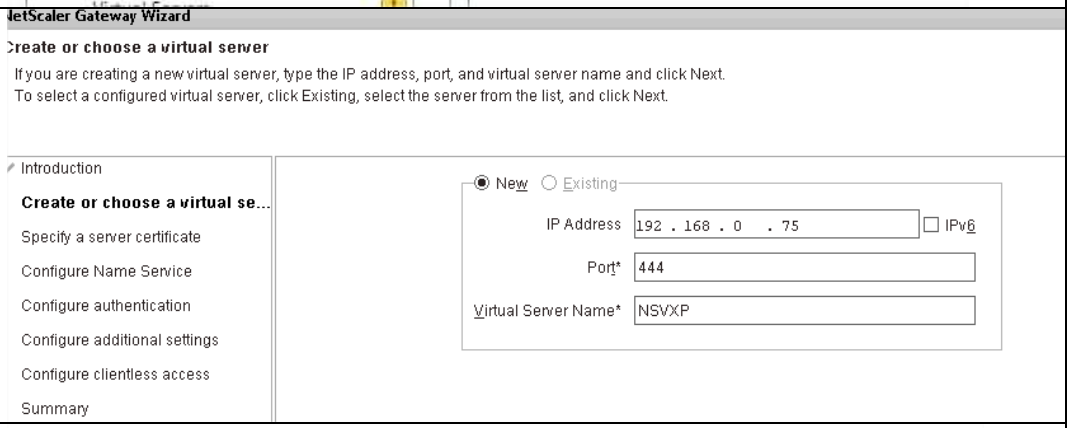
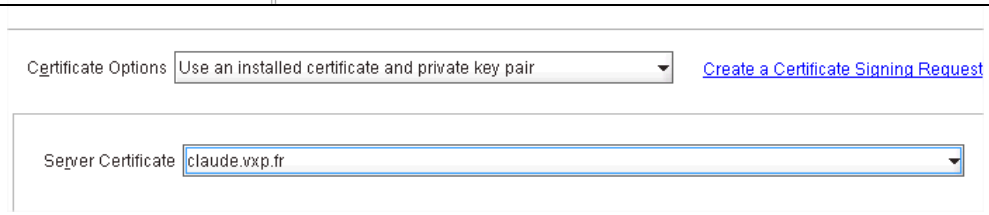
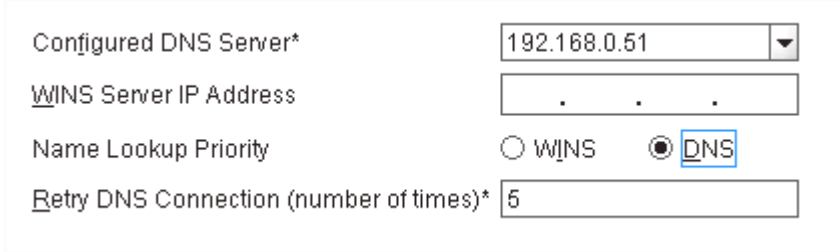
Cliquer sur **Create** puis **Close**.

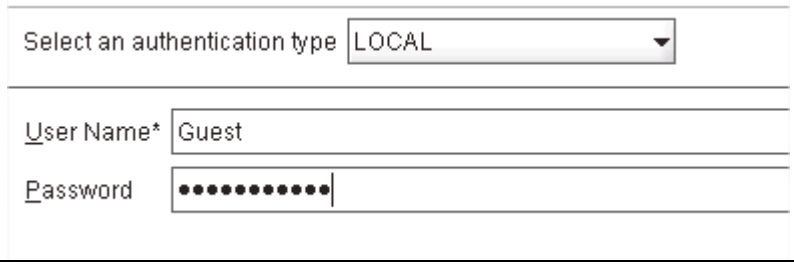
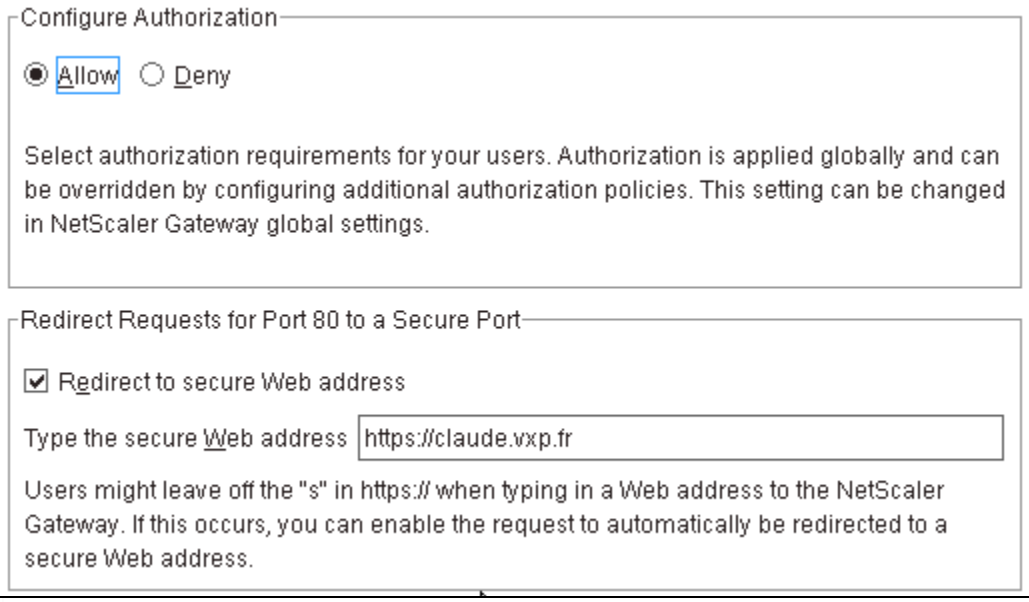
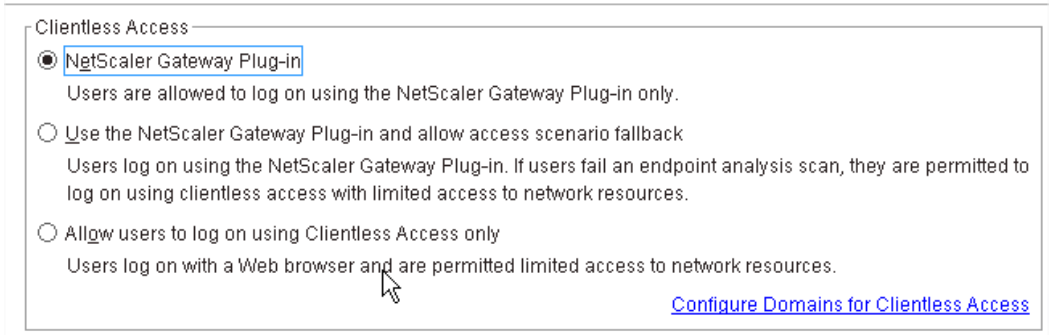
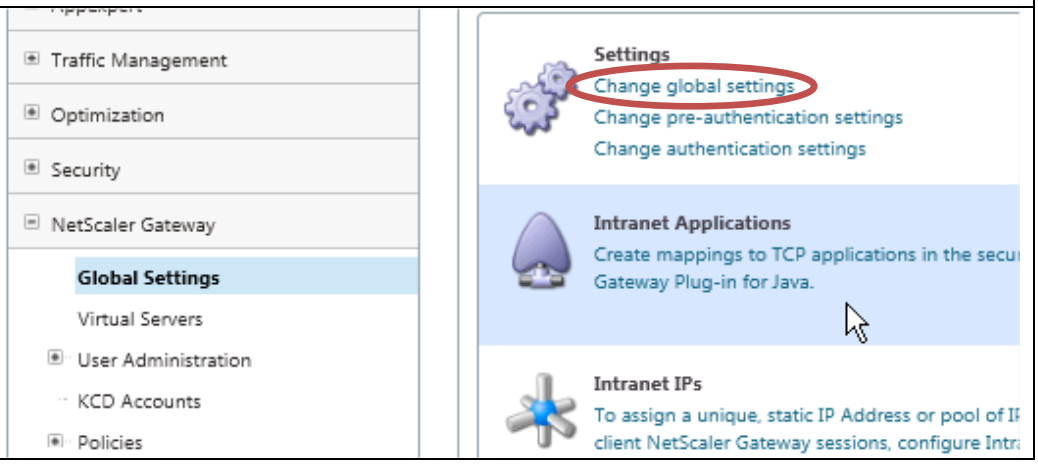


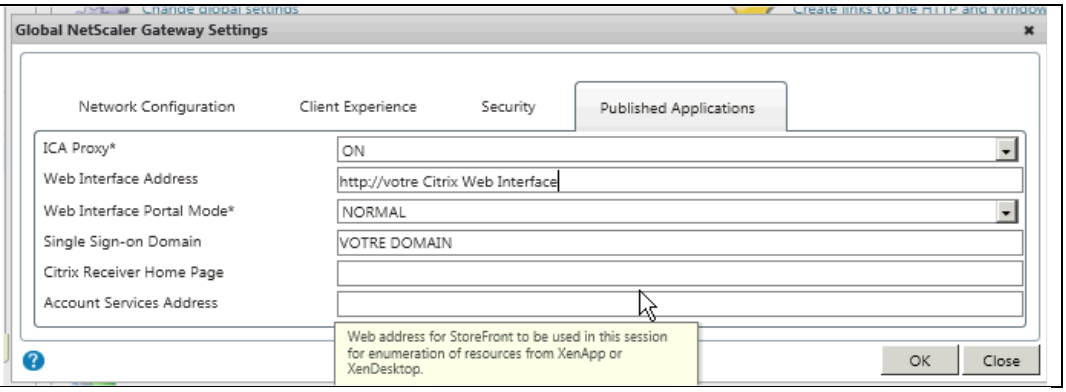


Le certificat devrait apparaitre dans la liste.	
Si ce message d'erreur est obtenu, c'est qu'il n'y a pas de licence Netscape installée correctement.	

5. Configuration de la fonction NetScaler Gateway

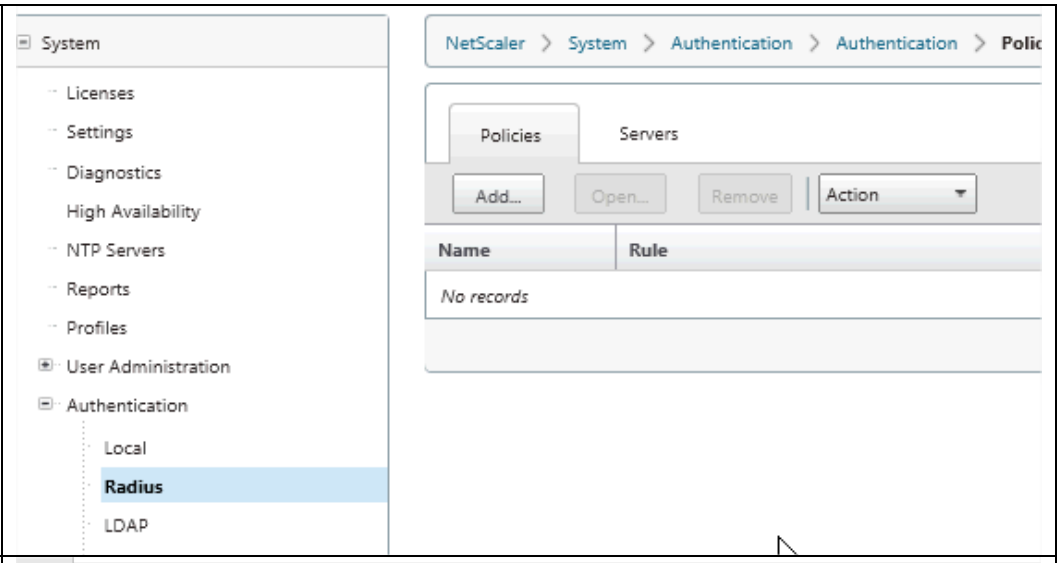
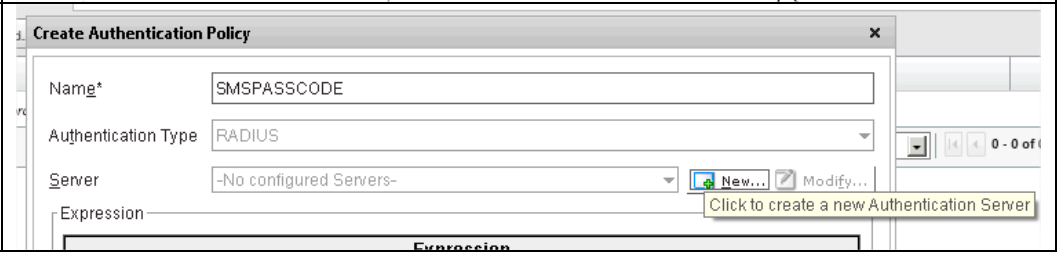
Cliquer sur le lien **NetScaler Gateway wizzard** et cliquer sur **Next**.	
Entrer une adresse Virtual IP et un port 443 par defaut. Dans ce lab, le port 444 est utilisé pour des raisons pratiques. Cliquer sur **Next**.	
Choisir l'option **Use an installed certificate and private key pair**. Choisir le certificat SSL précédemment crée. Cliquer sur **Next**.	
Entrer le DNS de votre réseau. Cliquer sur **Next**.	

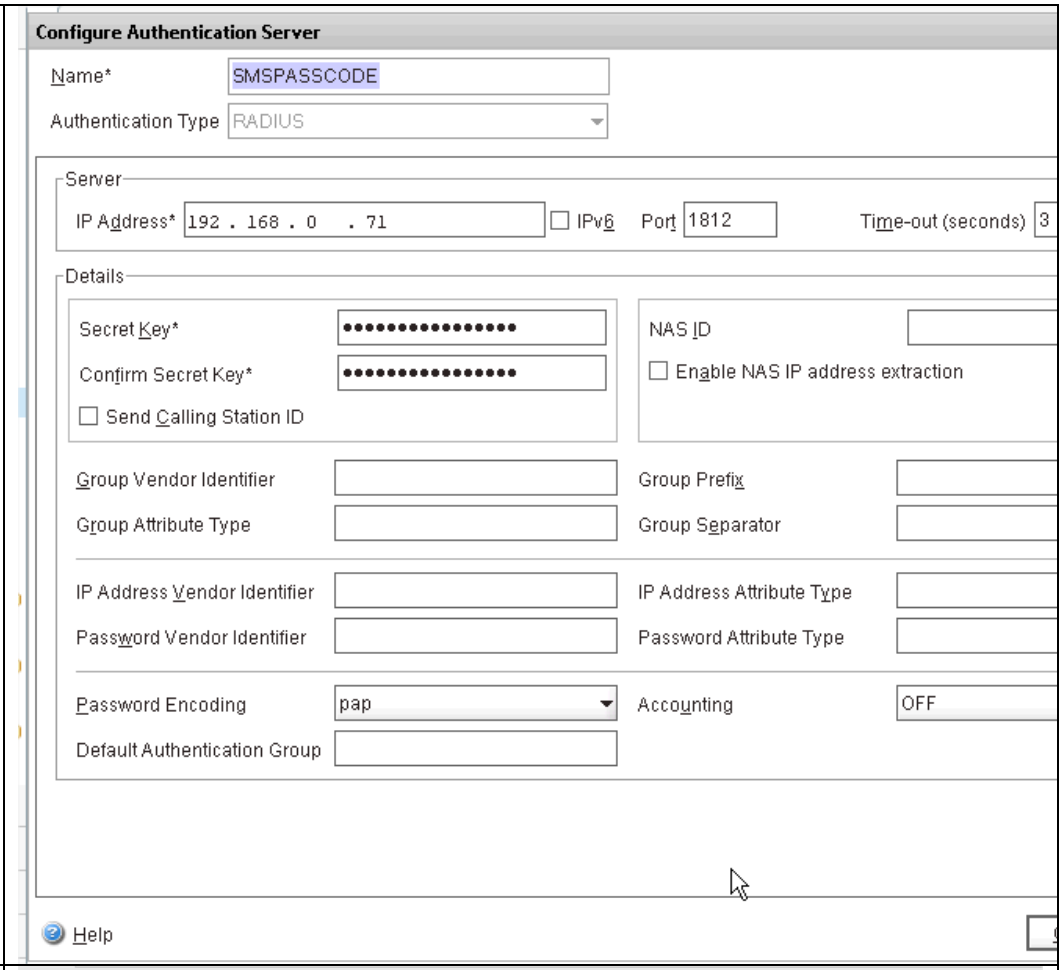
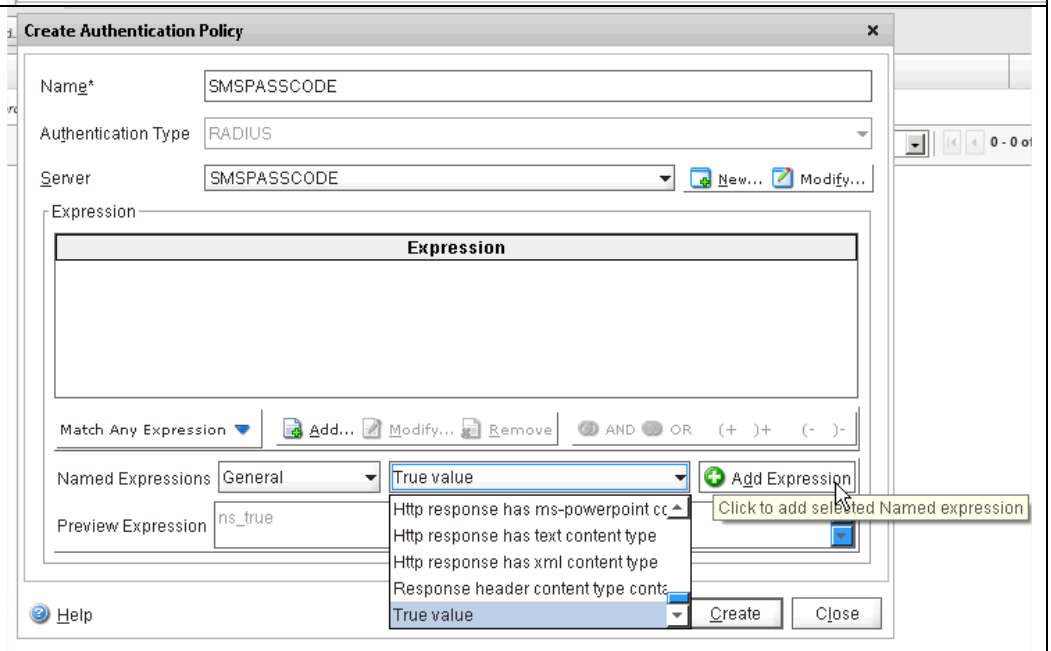
Pour le moment, choisir LOCAL. Nous reviendrons plus tard sur la partie authentification.	
Choisir **Allow**. Optionnel : s'il est choisi de laisser le NetScaler, répondre sur le port 80 (avec le port 80 du firewall ouvert) et cocher la case pour rediriger le trafic sur l'url SSL.	
Choisir **NetScaler Gateway Plug-in**. Cliquer sur **Next**, **Finish**, et **Exit**.	
Dans la section **NetScaler Gateway**, puis **Global Settings,** cliquer sur **Change global settings**.	

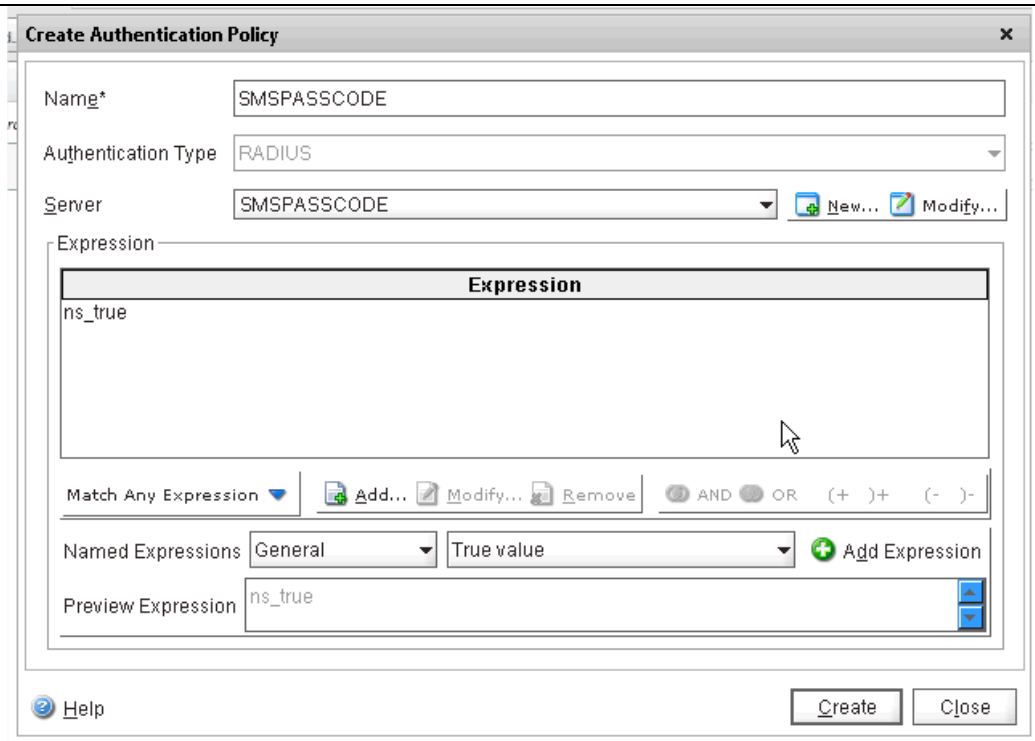
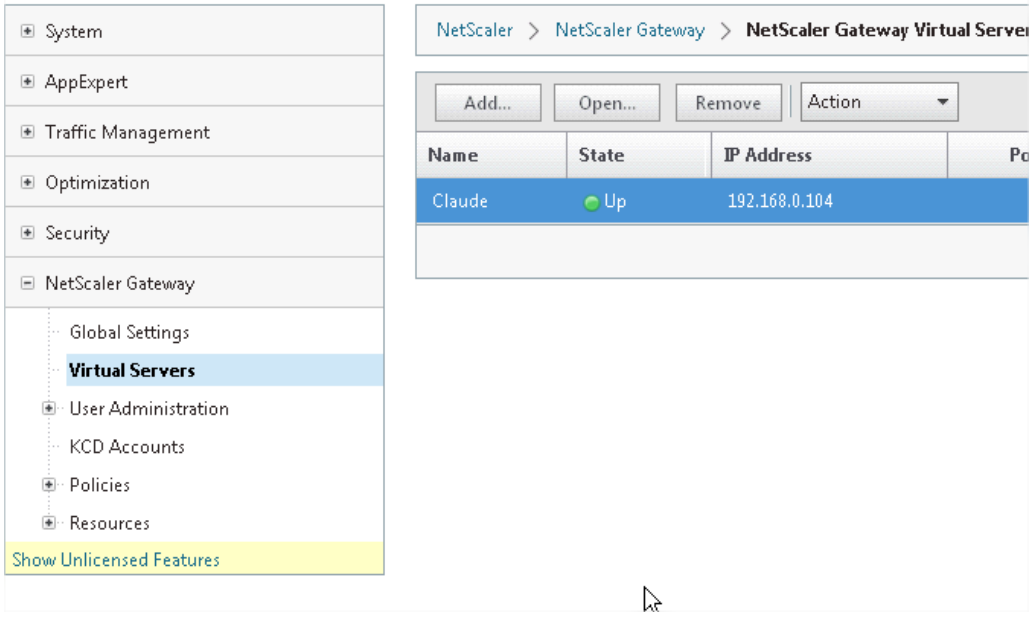
Passer le ICA proxy sur **ON**. Ajouter l'url de votre Citrix Web Interface ainsi que le domaine dans le champ **SSO Domain**. Cliquer sur **OK**.	

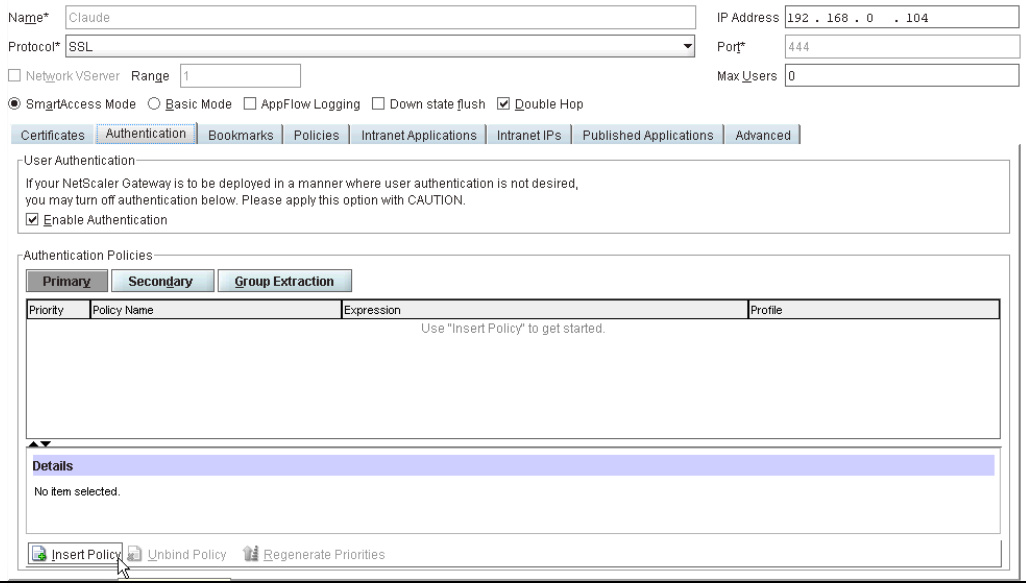
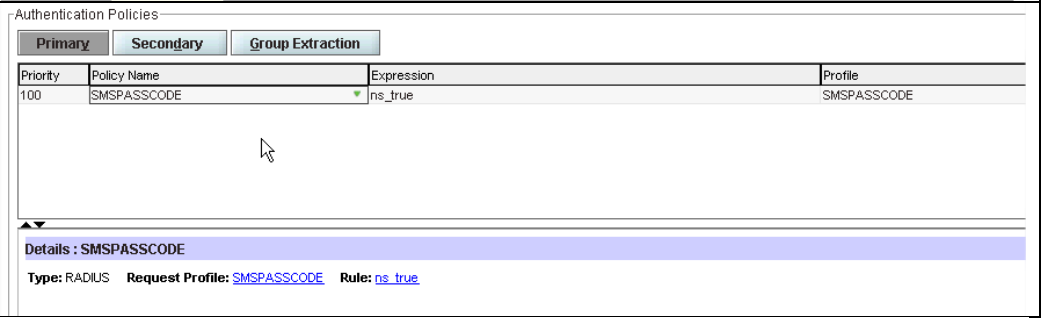
6. Configuration de l'authentification RADIUS pour SMSPASSCODE

Retour sur la page de configuration web de l'Appliance Netscaler Gateway.

Dans la partie **System**, puis **Authentification**, puis **Radius** : cliquer sur **Add**.	
Entrer un nom et cliquer sur le bouton **New**.	

Entrer les informations comme sur la capture d'écran. Choisir un mot de passe comme Secret Key. Ce mot de passe devra être entré lors de la configuration de la partie RADIUS sur le serveur SMSPASSCODE. Cliquer sur le bouton **Create**.	
Ajouter l'expression ns_true.	

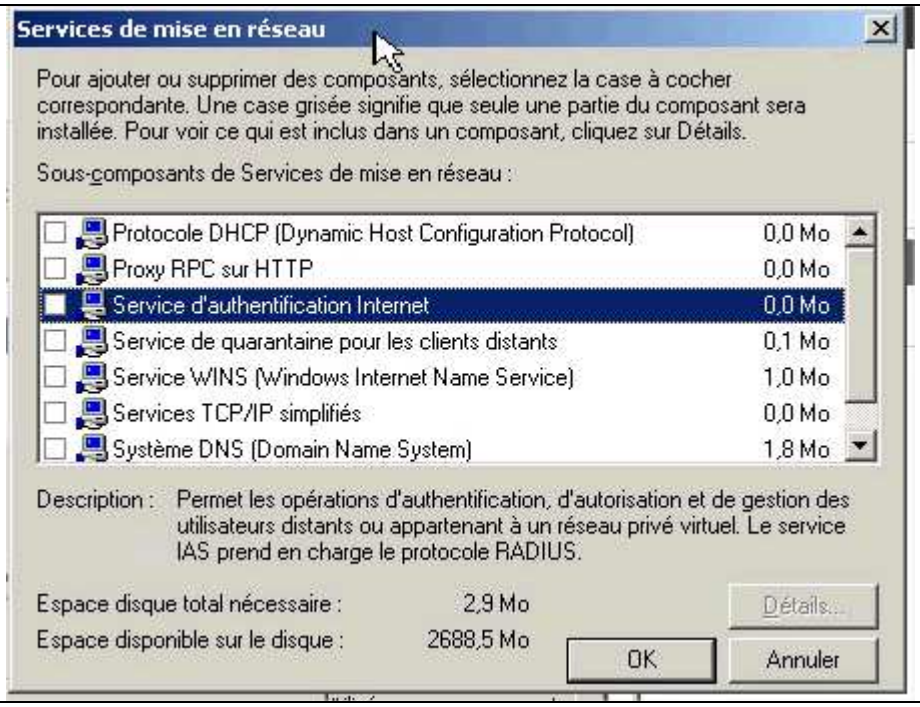
Cliquer sur **Create**.	
Ensuite le Virtual Server NetScaler Gateway va être "linké". Aller dans la section **NetScaler Gateway**, puis **Virtual Servers**. Cliquer sur la VIP Gateway puis sur **Open**.	

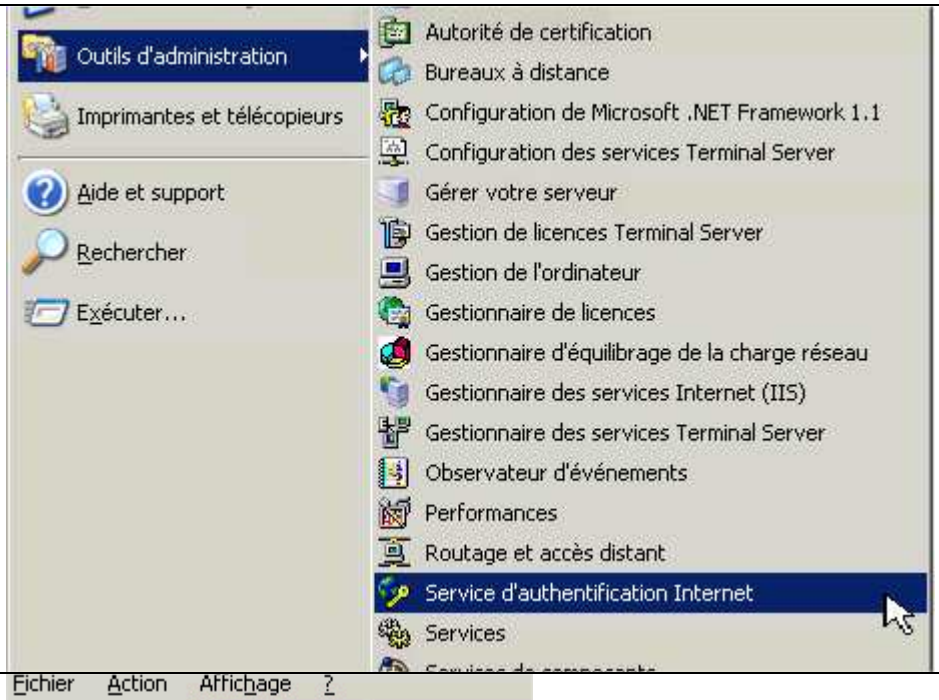
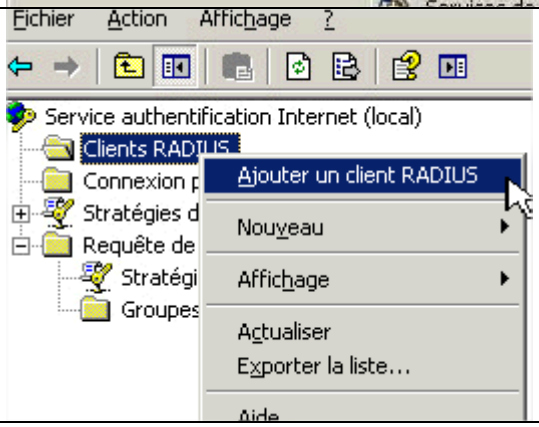
Cliquer sur l'onglet **Authentification** et sur le bouton **Insert Policy**.	
Sélectionner la policy **SMSPASSCODE** précédemment créée, puis cliquer sur **OK**.	

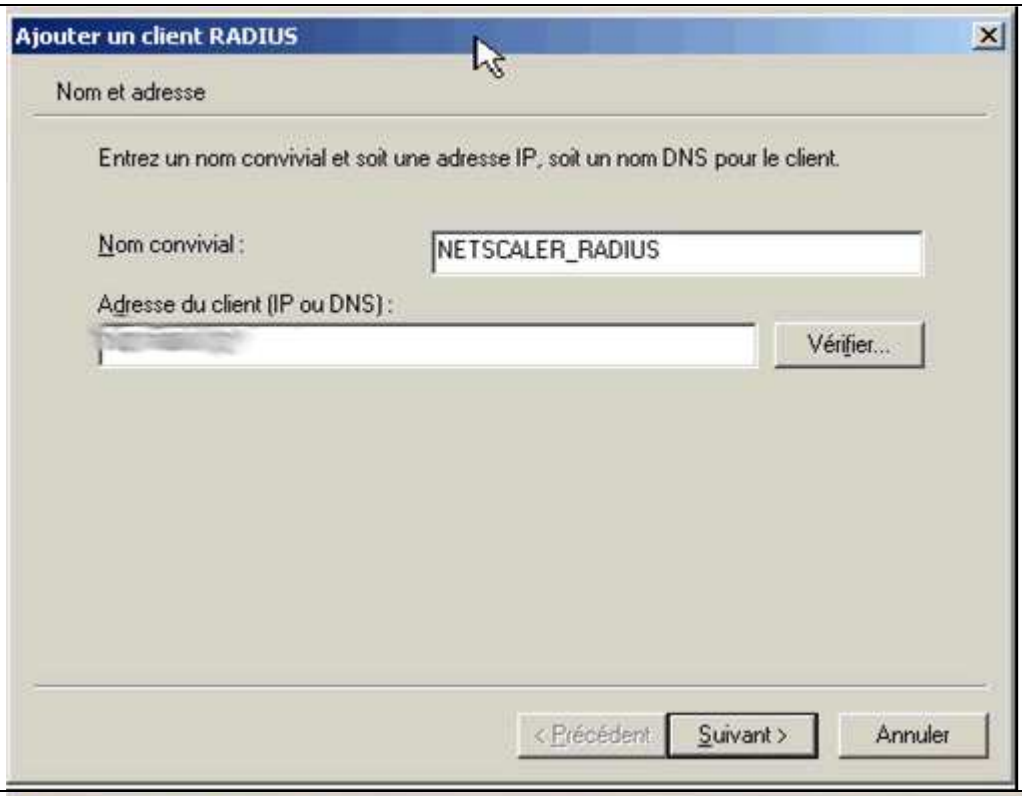
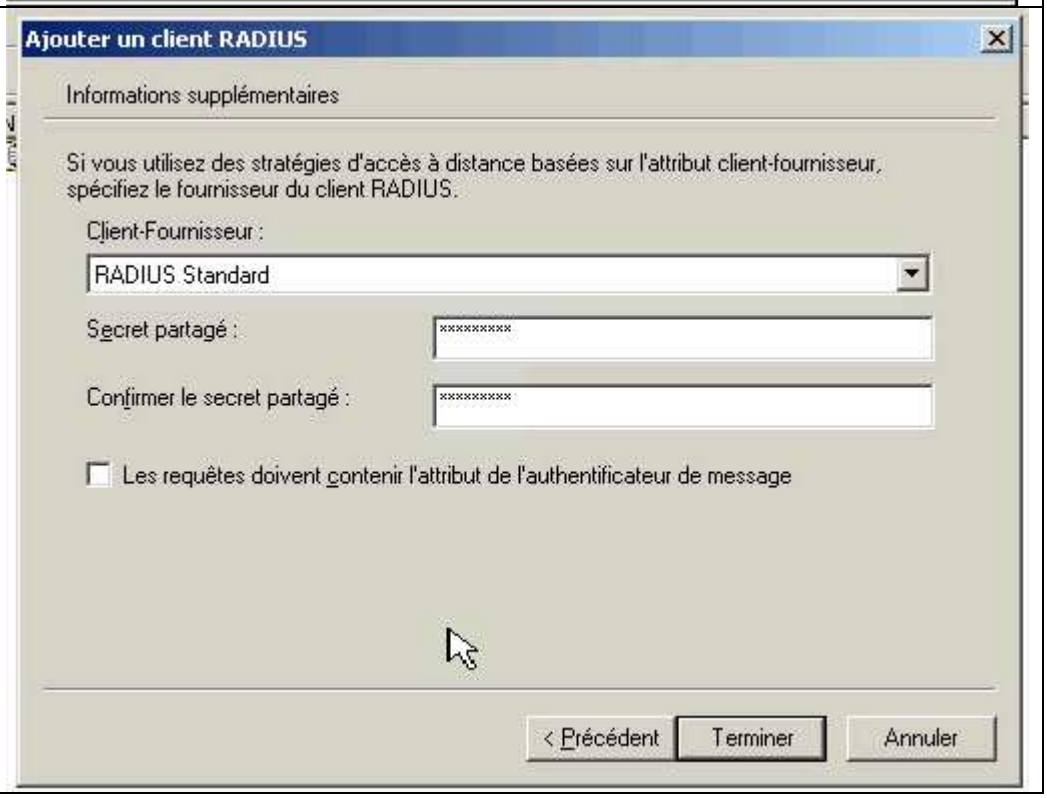
7. Configuration de l’authentification RADIUS pour SMS PASSCODE

Pour faire fonctionner l’authentification SMS PASSCODE avec NetScaler, il est nécessaire d’installer le composant "Service d’authentification Internet". Ce service peut être installé sur le serveur ou est installé SMSPASSCODE.

Sur un Windows 2003 :

Ajouter le composant "Service d’authentification Internet".	

Lancer ensuite la console depuis les outils d'administration : **Service d'authentification Internet**	
Dans la zone Client RADIUS, cliquer sur **Ajouter un client RADIUS**.	

Ajouter les informations IP de l'Appliance NetScaler Gateway. Ne pas mettre la VIP Gateway.	
Entrer les informations suivantes : RADIUS standard et choisir un mot de passe.	


Service authentification Internet (local)
Clients RADIUS
Connexion par accès distant
Stratégies d'accès distant
Requête de connexion en cours de traitement
Stratégies de demande de connexion
Nom convivial
Adresse
Protocole
Client-Fournisseur
Netscaler_Radius
RADIUS
RADIUS Standard

8. Configuration SMSPASSECODE

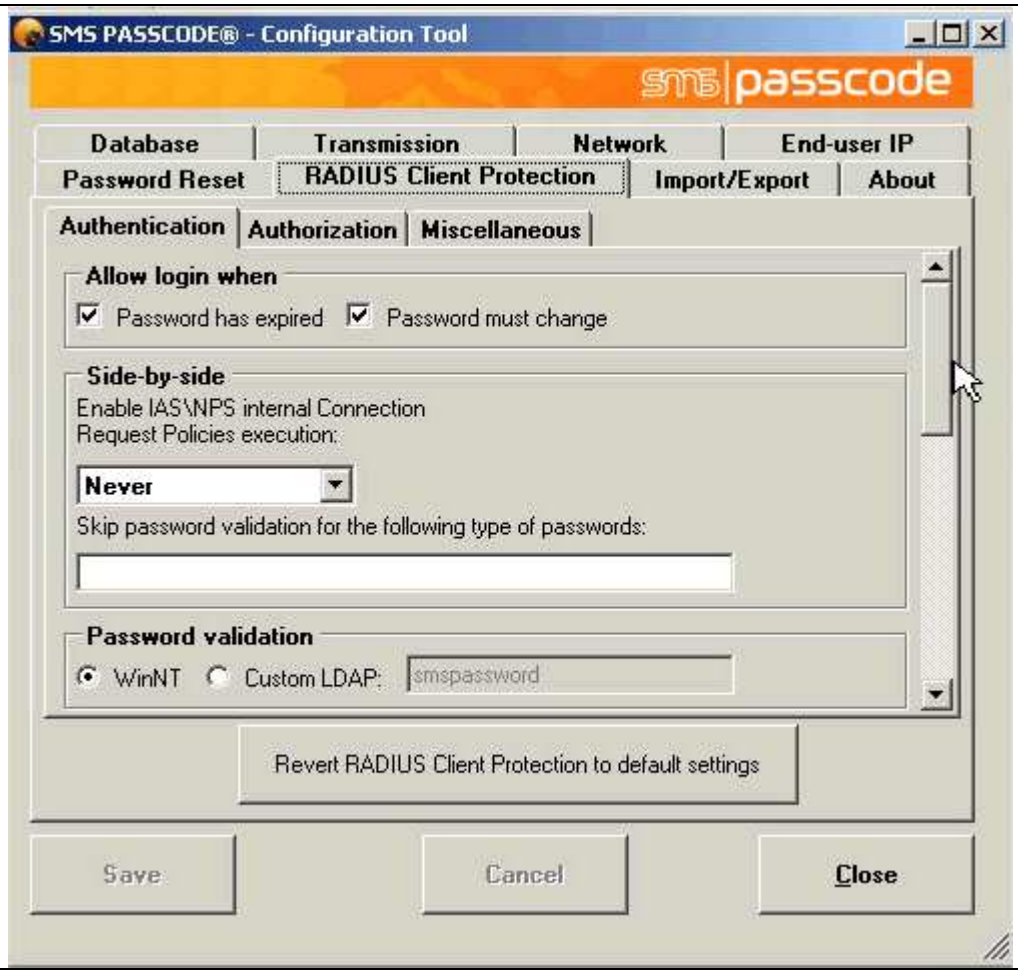
Lancer le setup de SMS PASSCODE sur le serveur SMS PASSCODE.

Ajouter le composant RADIUS Client Protection	

Un nouvel onglet apparait dans l'interface de Configuration SMS PASSCODE.

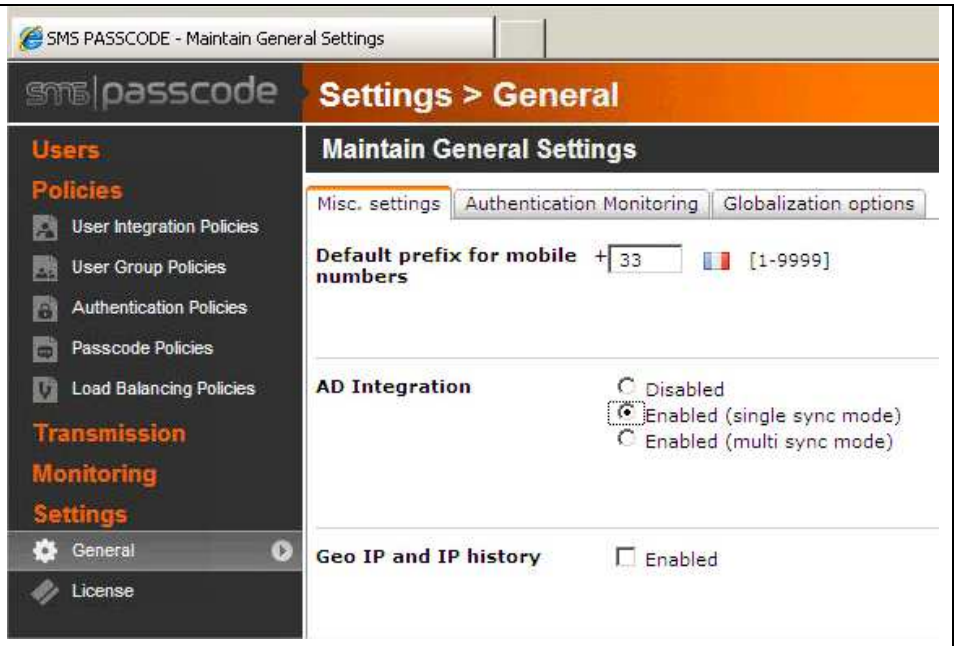
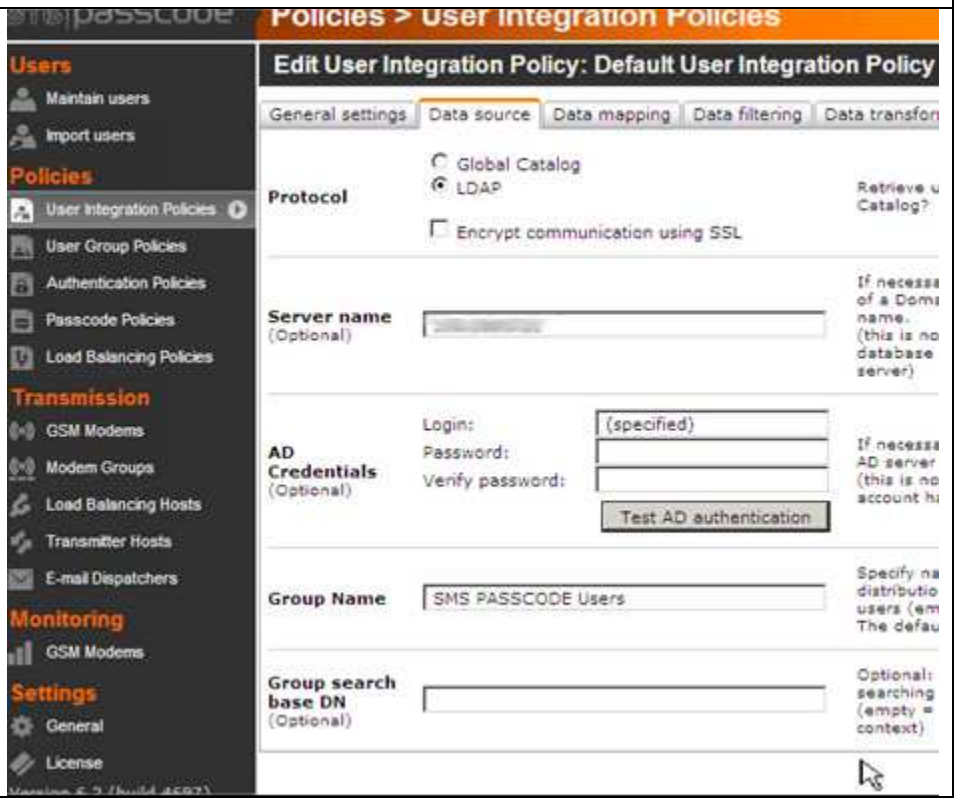
Vérifiez les paramètres.
Ici, votre politique interne de sécurité doit s'appliquer.

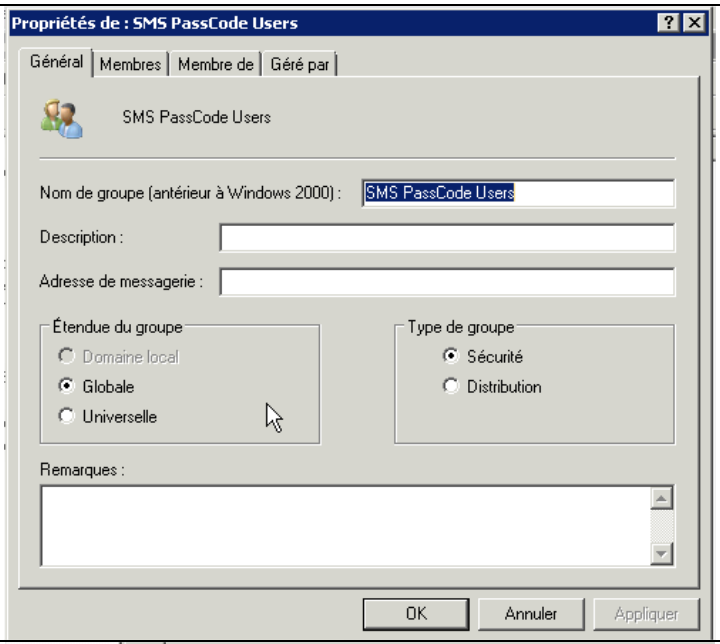
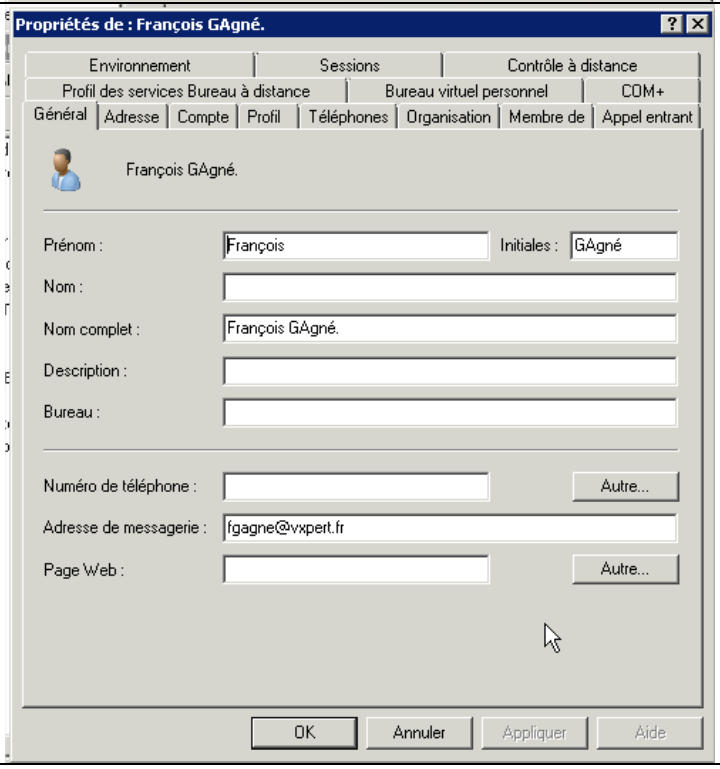
Cliquez sur SAVE si besoin.

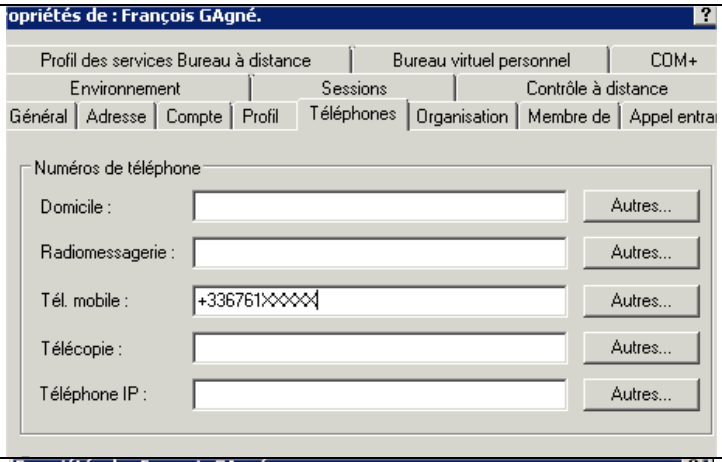
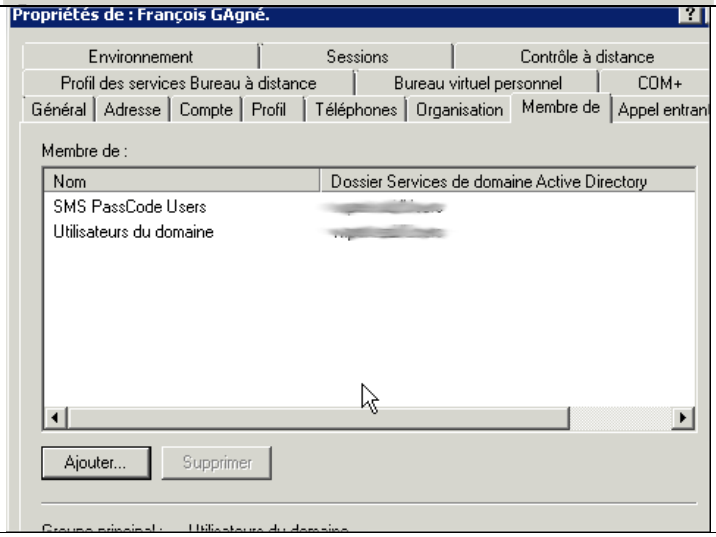


9. Activation de l'intégration AD avec SMS PASSCODE

Dans l'interface Web de SMS PASSECODE, il faut activer l'intégration avec l'active directory et ensuite configurer les comptes AD.

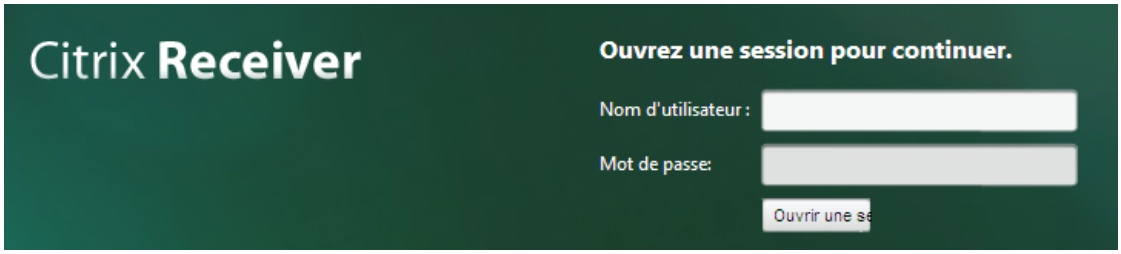
Dans la zone **Settings > General** Cocher la case **Enabled** dans la zone **AD intégration**.	
Ensuite dans la zone **Policies > User Integration Policies** onglet **Data source**, choisissez **LDAP** (il est préférable de cocher la case **Encrypt Communication using SSL** si **LDAPS** a été activé sur votre Active directory Pour ce lab, nous resterons en LDAP. Entrer le nom de votre contrôleur de domaine ou son IP/ le login Admin AD et son mot de passe.	

Créer le Groupe utilisateur "SMS PassCode Users" dans votre domaine Active Directory. Ce groupe doit contenir tous les utilisateurs qui devront être synchronisés dans la base SMS PASSCODE.	
Vérifier les champs Adresse de messagerie. Il est important d'y entrer une adresse personnelle. Cette adresse permettra d'envoyer le passcode dans le cas ou les SMS sont inutilisables (PB de réseaux GSM…).	

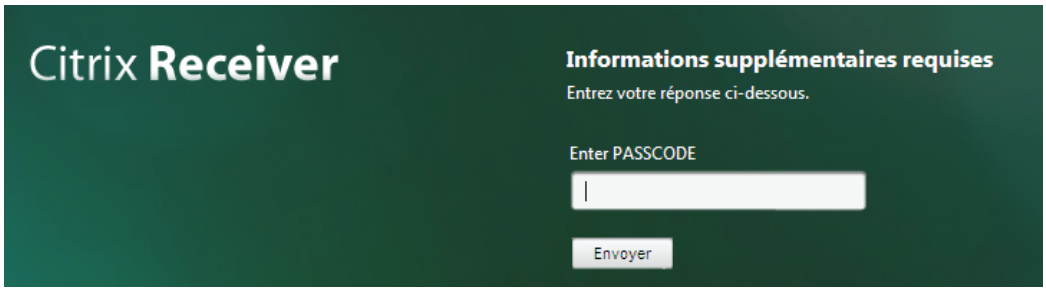
Vérifier les champs Tél. mobile.	
Et vérifier l'appartenance de l'utilisateur au groupe SMS PassCode Users.	

Ensuite forcer une synchro depuis la zone **Maintain users** de la console Web SMS PASSCODE.

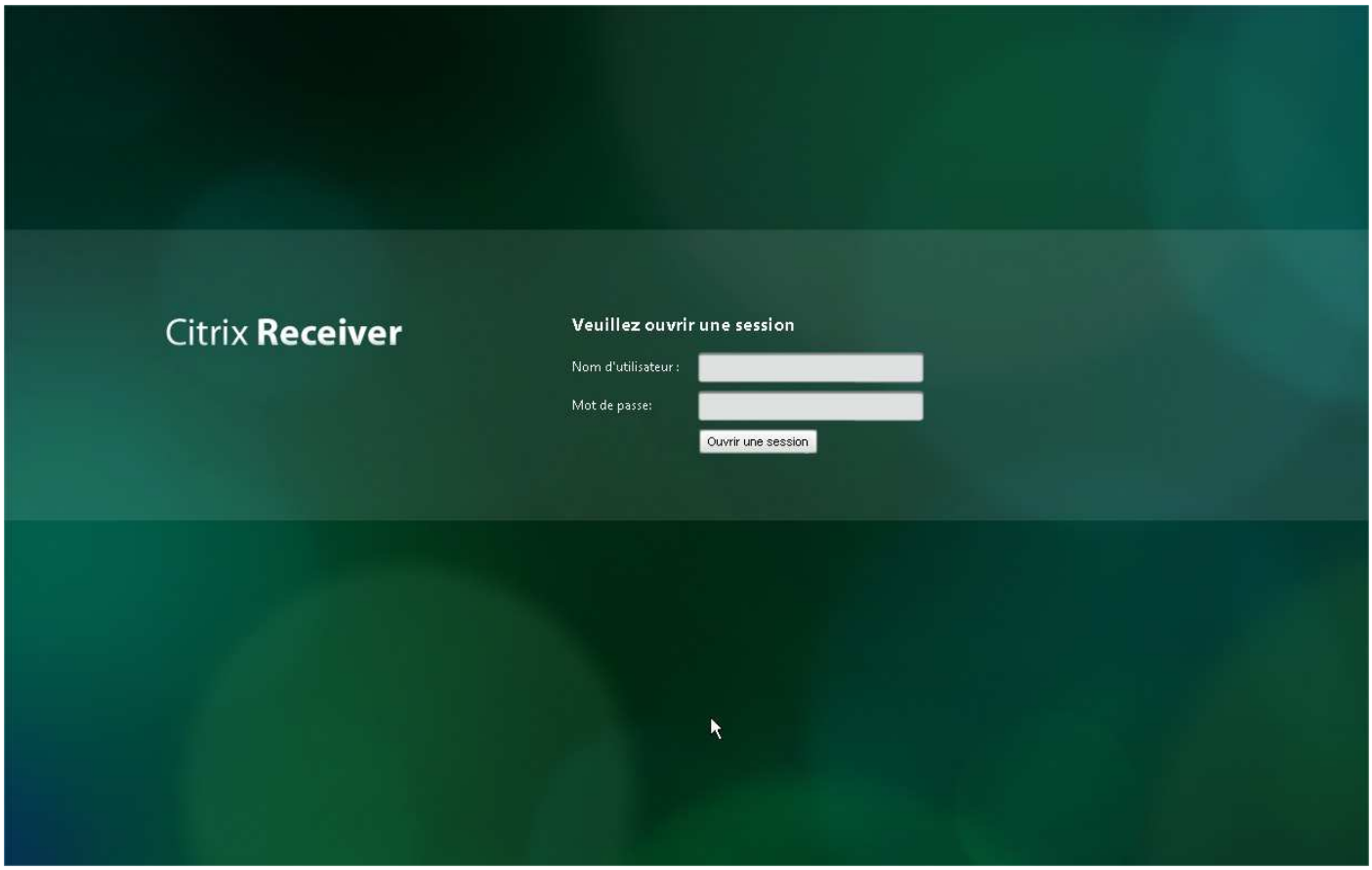
Voici le résultat lors du login sur le NetScaler.



Puis la demande du Passcode.



10. Installation du thème GREEN BUBBLE sur le NetScaler



Télécharger le script d'installation automatique depuis le site Citrix à l'adresse suivante :
http://cdn.ws.citrix.com/wp-content/uploads/2012/04/GreenBubble.txt

Copier le fichier GreenBubble.txt en GreenBubble1.sh avec Winscp (ou autre) directement sur le NetScaler : exemple répertoire /tmp.

Exécuter ensuite les commandes suivantes :

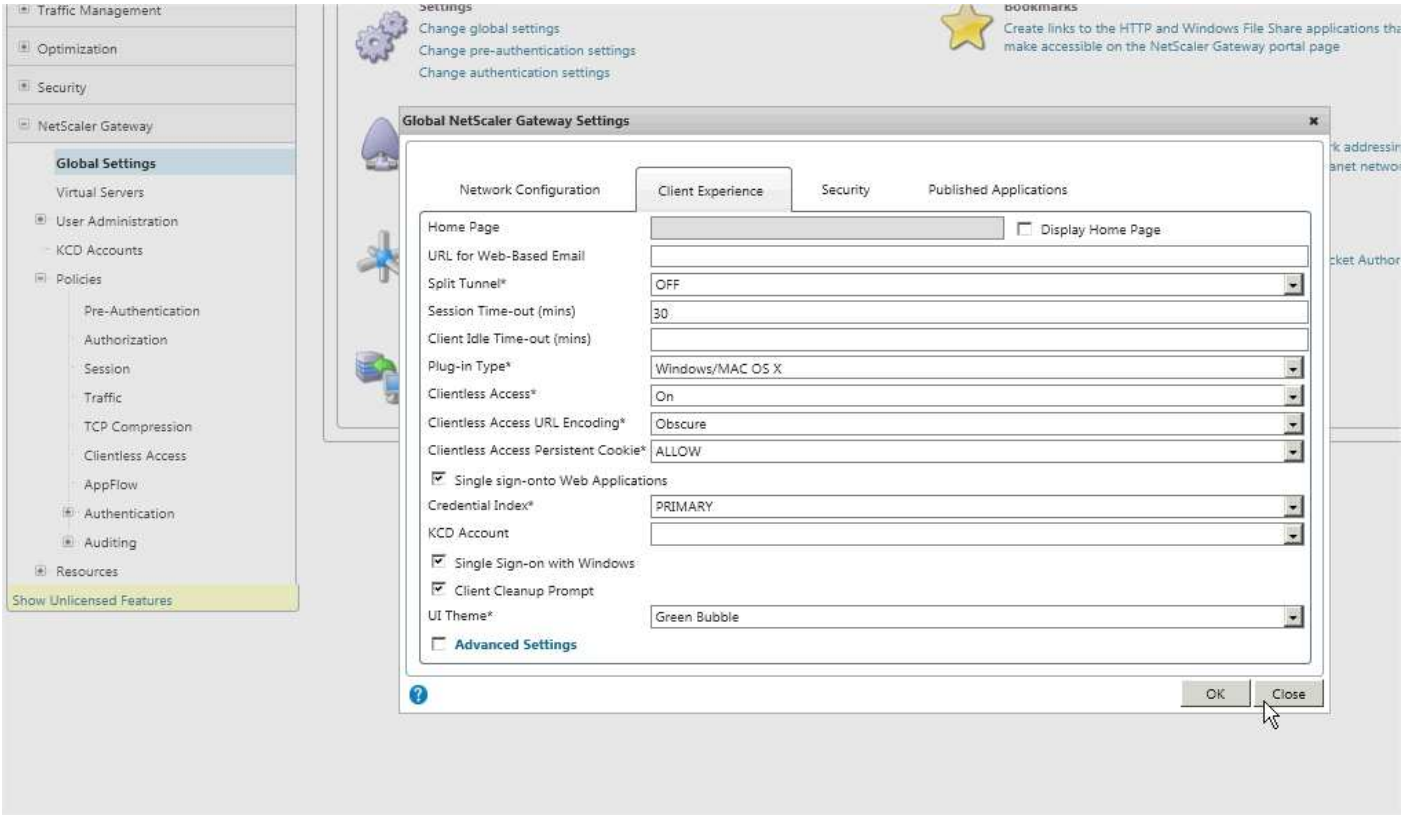
chmod +x GreenBubble1.sh
./GreenBubble1.sh

Il devrait y avoir un retour de ce type :
+ basename ./GreenBubble1.sh .sh
+ SKINNAME=GreenBubble1
+ SKINARC=GreenBubble1.gz
+ SKINDIR=/var/vpn/customizations
+ DL=/tmp
+ EPA=ns_gui/epa/epa.html
+ SKINURL=http://citrixdownloads.techstur.com/GreenBubble1.gz
+ [-d /var/vpn/customizations/GreenBubble1]
+ fgrep var nsversion= /var/vpn/customizations/GreenBubble1/ns_gui/epa/epa.html

+ cut -d" -f2
+ OLDCOMMAVER=10.0.54.7
+ echo 10.0.54.7
+ tr , .
+ OLDDOTVER=10.0.54.7
+ nsapimgr -d hwinfo
+ grep Version:
+ sed -e s/Version: NetScaler NS// -e s/: Build /\./ -e s/, Date.//*
+ cut -d. -f1,2,3,4
+ DOTVER=10.0.54.7
+ echo 10.0.54.7
+ tr . ,
+ COMMAVER=10,0,54,7
+ [10.0.54.7 != 10.0.54.7]
+ cp -rf /var/vpn/customizations/GreenBubble1/ /netscaler/
+ cp ./GreenBubble1.sh /var/vpn/customizations
+ chmod 755 /var/vpn/customizations/GreenBubble1.sh
+ touch /nsconfig/nsafter.sh
+ chmod 755 /nsconfig/nsafter.sh
+ fgrep -q /var/vpn/customizations/GreenBubble1.sh /nsconfig/nsafter.sh

Rebooter le NetScaler et vérifier l'installation.

Si ce n'est pas le cas, vérifier les propriétés du NetScaler Gateway/ Global Setting/ onglet Client Experience / UI Theme /

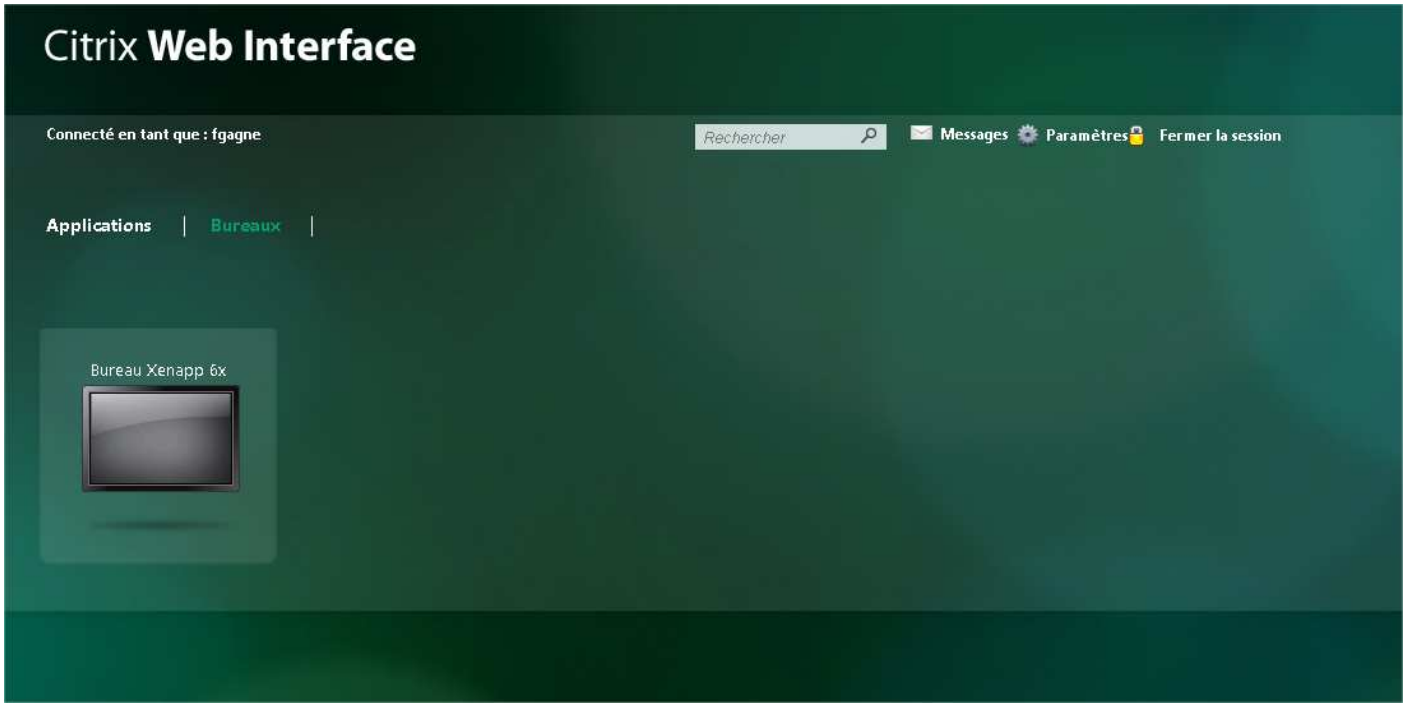


11. Installation du thème GREEN BUBBLE sur la Citrix Web Interface 5.4

http://www.techstur.com/getdownloads/2012/06/green-bubble-theme-for-web-interface-5-4/

Copier le contenu du zip dans le répertoire C:\inetpub\wwwroot.

Vider le cache du browser avant de tester.



12. Troubleshooting

Le SSO ne fonctionne pas entre le NetScaler et la Web Interface.

Symptôme :
Les utilisateurs s'authentifient une fois sur le NetScaler et sont obligés par l'interface Web de s'authentifier à nouveau.

Résolution :
Pour résoudre ce problème, suivre la technote CTX106202: **http://support.citrix.com/article/CTX106202**

Télécharger le fichier **AGWISSO.zip** depuis le lien. Extraire et copier le contenu du Zip dans le répertoire correspondant à votre version de Web Interface (voir le readme du zip).

Version des produits :

PRODUIT	Version
NETSCALER	10.1
Windows Server	2003
XenApp	6.5
Citrix Web Interface	5.4
SMS PASSCODE	6.2

Historique des versions du document

Version	Changement	Auteur	Date
DRAFT	Initial document	François GAGNÉ	Juin 2013
1	Distribution	François GAGNÉ	Octobre 2013

Vxpert SYSTEMES, entreprise indépendante spécialisée dans l'intégration de solutions de virtualisation de serveurs, d'applications, de stockage et de postes de travail. Forte de dix ans d'expérience dans l'intégration de service sur les produits Citrix, Vmware et Microsoft, Vxpert SYSTEMES propose une offre complète de solutions et de services pour vous garantir la réalisation de tous vos projets de virtualisation.

fgagne@vxpert.fr