

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. PRESENTATION	3
2. SCHEMA D'ARCHITECTURE	4
3. INSTALLATION NETSCALER 10.1	5
4. GENERATION DU CERTIFICAT SSL DU NETSCALER	6
5. CONFIGURATION DE LA FONCTION NETSCALER GATEWAY	13
6. CONFIGURATION DE L'AUTHENTIFICATION RADIUS POUR SMSPASSCODE	16
7. CONFIGURATION DE L'AUTHENTIFICATION RADIUS POUR SMS PASSCODE	20
8. CONFIGURATION SMSPASSECODE	24
9. ACTIVATION DE L'INTEGRATION AD AVEC SMS PASSCODE	26
10. INSTALLATION DU THEME GREEN BUBBLE SUR LE NETSCALER	30
11. INSTALLATION DU THEME GREEN BUBBLE SUR LA CITRIX WEB INTERFACE 5.4	32
12. TROUBLESHOOTING	33

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.

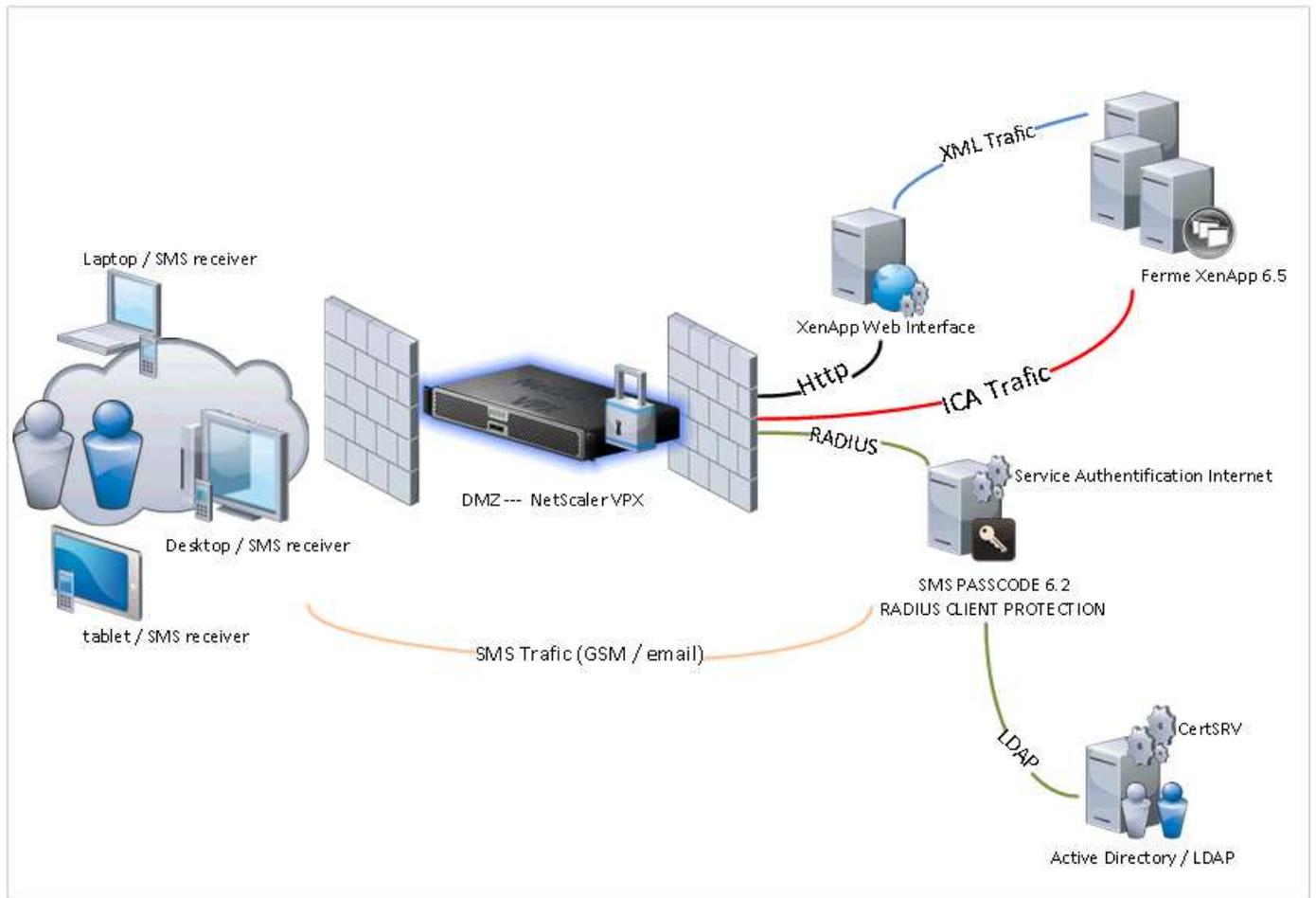
La configuration de la partie RADIUS de SMSPASSCODE.

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.

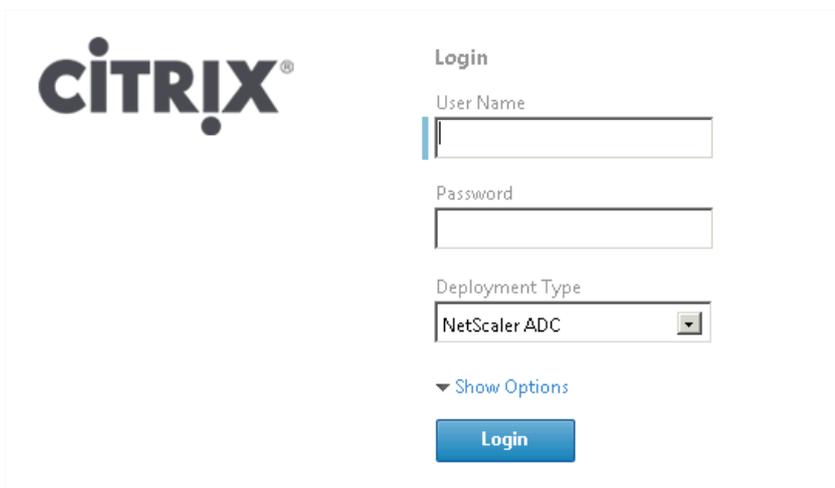
Sous Vpsphere, faire [fichier, déployer modèle OVF...](#)

(sinon <http://lmgfty.com/?q=d%C3%A9ployer+un+modele+ovf+sous+vsphere>)

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]:
```

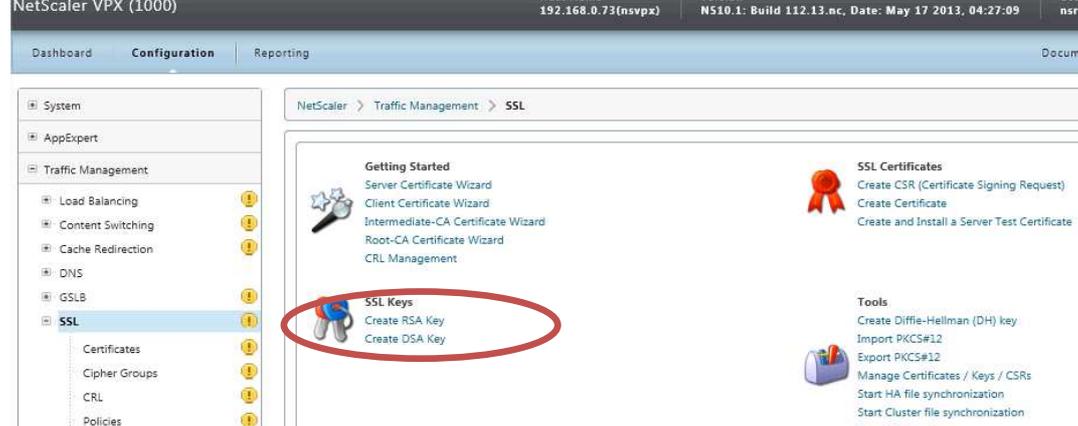
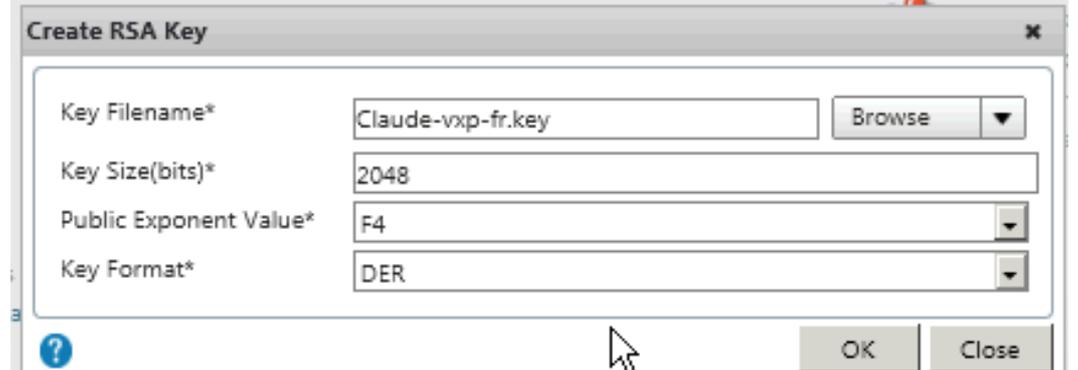
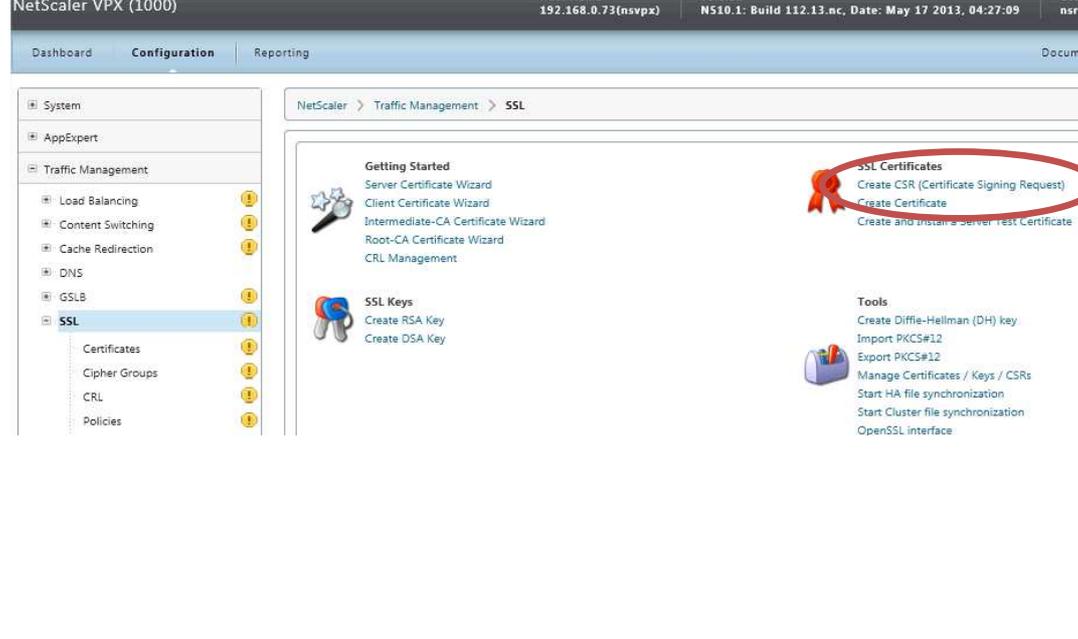
Le reste se fait à partir d'un navigateur internet.



The image shows the Citrix login interface. On the left is the Citrix logo. On the right, under the heading 'Login', there are three input fields: 'User Name', 'Password', and 'Deployment Type'. The 'Deployment Type' dropdown menu is set to 'NetScaler ADC'. Below these fields is a link that says 'Show Options' with a downward arrow. At the bottom of the form is a blue 'Login' button.

4. Génération du certificat SSL du NetScaler

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

<p>Lancer la page web de configuration du NetScaler et cliquer sur Traffic Management/SSL sur la zone de gauche.</p> <p>Cliquer sur Create RSA Key.</p>	 <p>NetScaler VPX (1000) 192.168.0.73(nsvpx) NS10.1: Build 112.13.nc, Date: May 17 2013, 04:27:09 nsro</p> <p>Dashboard Configuration Reporting</p> <p>System</p> <p>AppExpert</p> <p>Traffic Management</p> <ul style="list-style-type: none">Load BalancingContent SwitchingCache RedirectionDNSGSLBSSL<ul style="list-style-type: none">CertificatesCipher GroupsCRLPolicies <p>NetScaler > Traffic Management > SSL</p> <p>Getting Started</p> <ul style="list-style-type: none">Server Certificate WizardClient Certificate WizardIntermediate-CA Certificate WizardRoot-CA Certificate WizardCRL Management <p>SSL Keys</p> <ul style="list-style-type: none">Create RSA KeyCreate DSA Key <p>SSL Certificates</p> <ul style="list-style-type: none">Create CSR (Certificate Signing Request)Create CertificateCreate and Install a Server Test Certificate <p>Tools</p> <ul style="list-style-type: none">Create Diffie-Hellman (DH) keyImport PKCS#12Export PKCS#12Manage Certificates / Keys / CSRsStart HA file synchronizationStart Cluster file synchronizationOpenSSL interface
<p>Entrer un nom de fichier en rapport avec votre installation.</p> <p>Entrer 2048 en tant que key size et choisir le format DER.</p> <p>Cliquer sur OK.</p>	 <p>Create RSA Key</p> <p>Key Filename* Claude-vxp-fr.key Browse</p> <p>Key Size(bits)* 2048</p> <p>Public Exponent Value* F4</p> <p>Key Format* DER</p> <p>OK Close</p>
<p>Cliquer sur Create CSR.</p> <p>Entrer un nom de fichier pour la demande de certificat (nous vous suggérons une extension req).</p> <p>Puis rechercher le fichier "clé privée" que vous venez de créer.</p> <p>Choisir DER en format.</p>	 <p>NetScaler VPX (1000) 192.168.0.73(nsvpx) NS10.1: Build 112.13.nc, Date: May 17 2013, 04:27:09 nsro</p> <p>Dashboard Configuration Reporting</p> <p>System</p> <p>AppExpert</p> <p>Traffic Management</p> <ul style="list-style-type: none">Load BalancingContent SwitchingCache RedirectionDNSGSLBSSL<ul style="list-style-type: none">CertificatesCipher GroupsCRLPolicies <p>NetScaler > Traffic Management > SSL</p> <p>Getting Started</p> <ul style="list-style-type: none">Server Certificate WizardClient Certificate WizardIntermediate-CA Certificate WizardRoot-CA Certificate WizardCRL Management <p>SSL Keys</p> <ul style="list-style-type: none">Create RSA KeyCreate DSA Key <p>SSL Certificates</p> <ul style="list-style-type: none">Create CSR (Certificate Signing Request)Create CertificateCreate and Install a Server Test Certificate <p>Tools</p> <ul style="list-style-type: none">Create Diffie-Hellman (DH) keyImport PKCS#12Export PKCS#12Manage Certificates / Keys / CSRsStart HA file synchronizationStart Cluster file synchronizationOpenSSL interface

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**.

SSL KEYS 10015

Create CSR (Certificate Signing Request)

Request File Name* Browse

Key Filename* Browse

Key Format PEM DER

Distinguished Name Fields

Country* State or Province*

Organization Name* City

Email Address Organization Unit

Common Name

Attribute Fields

Challenge Password Company Name

?

OK

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

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

Key
Key

- Create Diffie-Hellman (DH) key
- Import PKCS#12
- Export PKCS#12
- Manage Certificates / Keys / CSRs**
- Start CA file synchronization
- Start Cluster file synchronization
- OpenSSL interface

Manage Certificates / Keys / CSRs

Current Directory: /nsconfig/ssl

Find Zip Back Up Create

Name	Type	Size (bytes)	Modified Date	Accessed
ns-root.key	File	493	mer., mai 29, 2013	mer., mai 29, 2013
ns-root.req	File	493	mer., mai 29, 2013	mer., mai 29, 2013
ns-root.cert	File	1 090	mer., mai 29, 2013	mer., mai 29, 2013
ns-server.key	File	493	mer., mai 29, 2013	mer., mai 29, 2013
ns-server.req	File	493	mer., mai 29, 2013	mer., mai 29, 2013
ns-root.srl	File	3	mer., mai 29, 2013	mer., mai 29, 2013
ns-server.cert	File	1 066	mer., mai 29, 2013	mer., mai 29, 2013
Claude-vxp-fr.key	File	1 191	mer., mai 29, 2013	mer., mai 29, 2013
claude-vxp-fr.req	File	928	mer., mai 29, 2013	mer., mai 29, 2013

Upload... Download... **View...** Remove

Help

Copier le contenu du fichier dans le presse-papier et fermer la fenêtre.

```
—BEGIN NEW CERTIFICATE REQUEST—
MIICHTCCAwwCAQAwQDELMAkGA1UEBhMCRIx CzA JBgNVBAgTAKZSMQwwCgYDVQQK
EwNNAWFx FjAUBgNVBAMTDWNSYXVlZS52eHAuZnlwggEIMA0GCsGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQEg3V0GixQaEKqIBrn3mTgv/sWNrdQhBVpwRpzUnQL1/JQ
pKjt5tHejyvFieg+I5oVnn0WLT02+58PCuVb+6T85tE5JAxkkjfy+GI4hXqBHHs4
wBQLQR1b5LOfYncMoUFoEF/8CAaDZol0ddWaRVawXZ6HBJV/wzqspwuHw/T23n5
M8JBjGGDs/sA8QGTPUHm6SKTOLa+4lqu6tB1VQJ/8E7s6zU9MUcmgstxC9RackGq
YqQi3uofpWnGTEvHmPeyC+dsUVWwP5llwKubCRbMvNsEurtgMVYuvRZ8I04KFKY
uk8SLZCf1YonnvB7X4flxqkvB2avY9Ypy1E7oWs9AgMBAAAGADANBgkqhkiG9w0B
AQUFAAOCAQEAVKGGQhxZ3O7Ib1nUvW6jwG4rXf3MDIqfgAlu/Y19I3nHHVsxXdfF
hJUGEWNKoVZJ3HcAKU211YaFqPRrQFdEfDrwjKcxCTB9Cdsyla00GIPD48yFMHLP
uvlJO1pN4kt8Wb4zQucfy6boRONAtyRj422o8GMciGiA03T5FQOkGfJfB0RZa4bE
Zoyzm326uwX0PZzDwXmzZYNMJEJM7efSgk06iUeGAzQXfyigiDmTgijSL0Wkkea
w4mwhKU4wJ8LNefT9Rgix8BwF8acGIBNWBjbuZSDg0d6LHhFybkindSTtHwGrtG
PRbkiKviebWbo5fJuD0SZcvwFz8XSsFiqw==
—END NEW CERTIFICATE REQUEST—
```

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/cer/tsrv>

Cliquer sur **Request a certificate.**

Services de certificats *Microsoft Active Directory* - vxpert-AD-CA

Bienvenue !

Utilisez ce site Web pour demander un certificat pour votre navigateur Web, votre programme client de messagerie ou votre programme. En utilisant un certificat, vous pouvez confirmer votre identité aux personnes avec lesquelles vous communiquez et chiffrer des messages et, selon le type de certificat que vous demandez, effectuer d'autres tâches sécurisées.

Vous pouvez également utiliser ce site Web pour télécharger un certificat d'autorité de certification, une chaîne de certification, ou vous pouvez afficher le statut d'une requête en attente.

Pour obtenir plus d'informations sur les Services de certificats Active Directory, voir [Documentation sur les Services de certificats Active Directory](#).

Sélectionnez une tâche :

- [Demander un certificat](#)
- [Afficher le statut d'une requête de certificat en attente](#)
- [Télécharger un certificat d'autorité de certification, une chaîne de certificats ou une liste de révocation des certificats](#)

<p>Choisir Advanced certificate request.</p>	<p>Services de certificats <i>Microsoft</i> Active Directory – vxpert-AD-CA</p> <hr/> <p>Demander un certificat</p> <hr/> <p>Sélectionnez le type de certificat :</p> <p>Certificat utilisateur</p> <p>Ou, soumettre un demande de certificat avancée.</p> <hr/>
<p>Choisir Submit a certificate request by using a base-64-encoded...</p>	<p>Services de certificats <i>Microsoft</i> Active Directory – vxpert-AD-CA</p> <hr/> <p>Demande de certificat avancée</p> <hr/> <p>La stratégie de l'autorité de certification détermine le type de certificats que vous pouvez demander pour :</p> <p>Créer et soumettre une demande de requête auprès de cette autorité de certification.</p> <p>Soumettez une demande de certificat en utilisant un fichier CMG ou PKCS #10 codé en base 64.</p> <p>Soumettez une demande de certificat en utilisant un fichier PKCS #7 codé en base 64.</p> <hr/>

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

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

Puis cliquer sur **Envoyer**.

Soumettre une demande de certificat ou de renouvellement

Afin de soumettre une demande enregistrée à l'autorité de certification, collez une ou une demande de renouvellement PKCS #7 générée par une source externe (tel

Demande enregistrée :

Base-64-encoded
Requête de certificat
(CMC ou
PKCS #10 ou
PKCS #7):

```
TZYM6p16LL4vTJCgvqaYwBBfZ16EY64yOIpBC1kr
J5yunsNdNJSQCQTJWCzB97jsOTOz8iJGsp4K5SY+
v6grDELVO1ut1hKyAQBaTfJK4K5uKBm1BgyGVEhM
wEinqI61oKxUJ2fND6hAQ9P8tmoK0B2kYSZDwo/E
WA==
-----END NEW CERTIFICATE REQUEST-----
```

Modèle de certificat :

Serveur Web

Attributs supplémentaires :

Attributs :

Envoyer >

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

Certificat émis

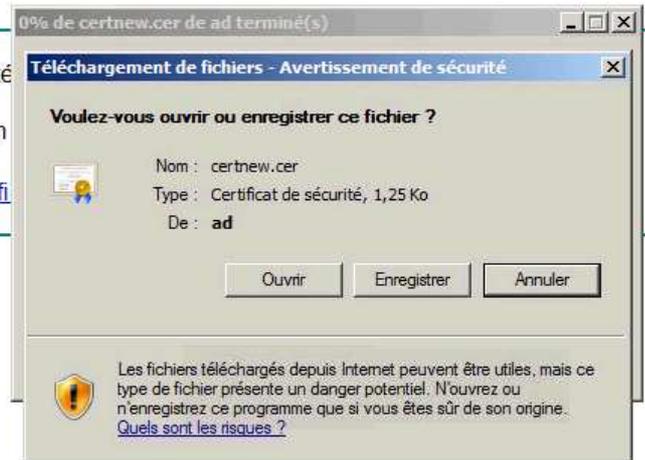
Le certificat que vous avez demandé a été

Codé DER ou Codé en



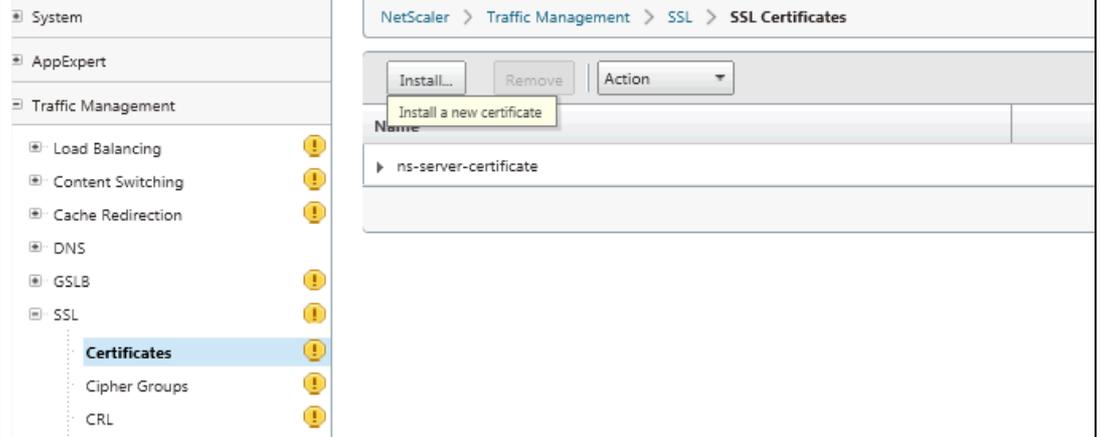
[Télécharger le certificat](#)

[Télécharger la chaîne de certifi](#)



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

Cliquer sur le bouton **Install....**

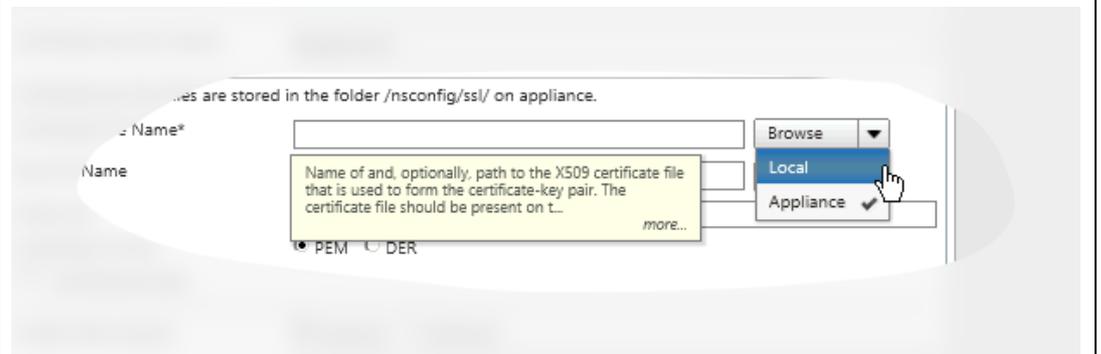
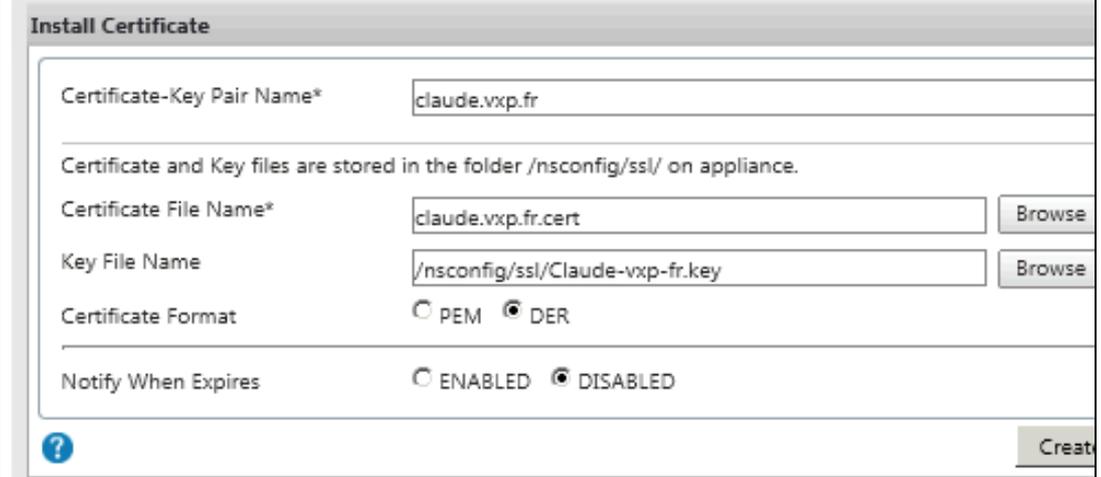


Entrer le "FQDN" dans le champ **Pair Name**.

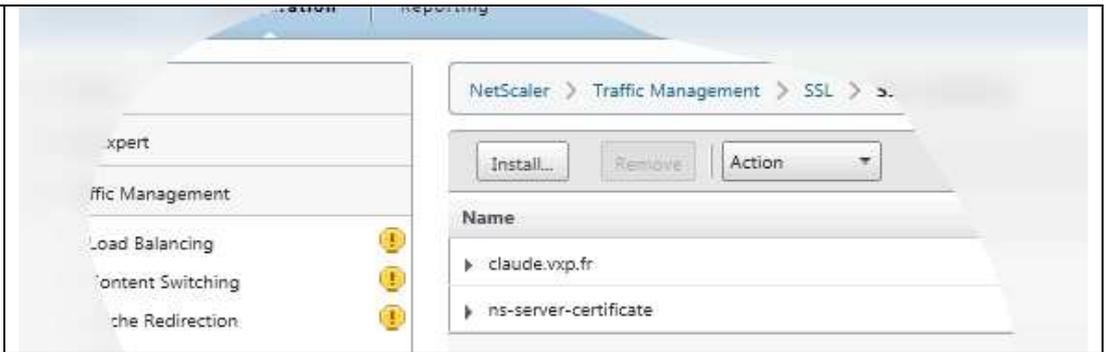
Sélectionner votre fichier cert depuis votre poste de travail (pour cela, cliquer sur Browse et choisir Local),

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**.



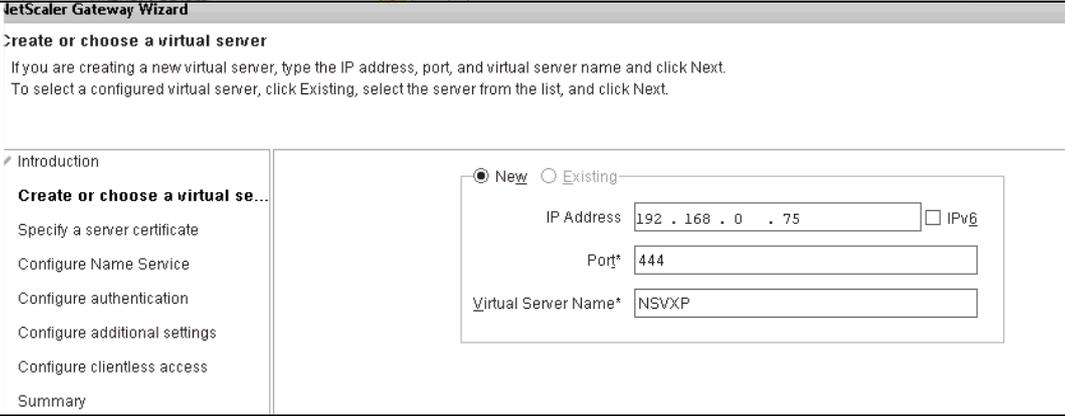
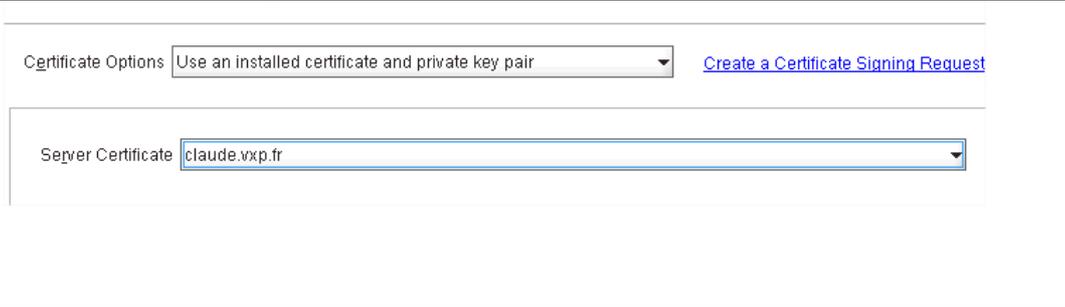
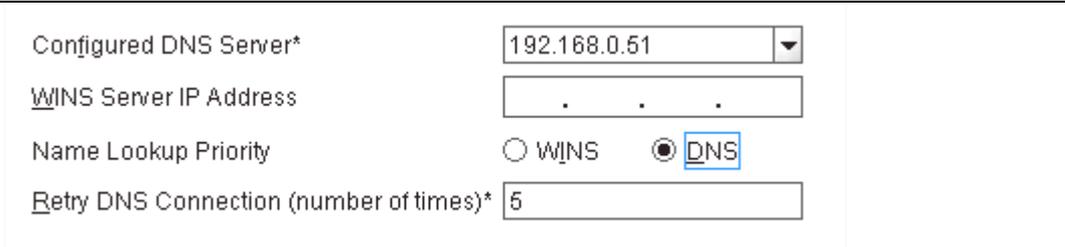
Le certificat devrait apparaître dans la liste.

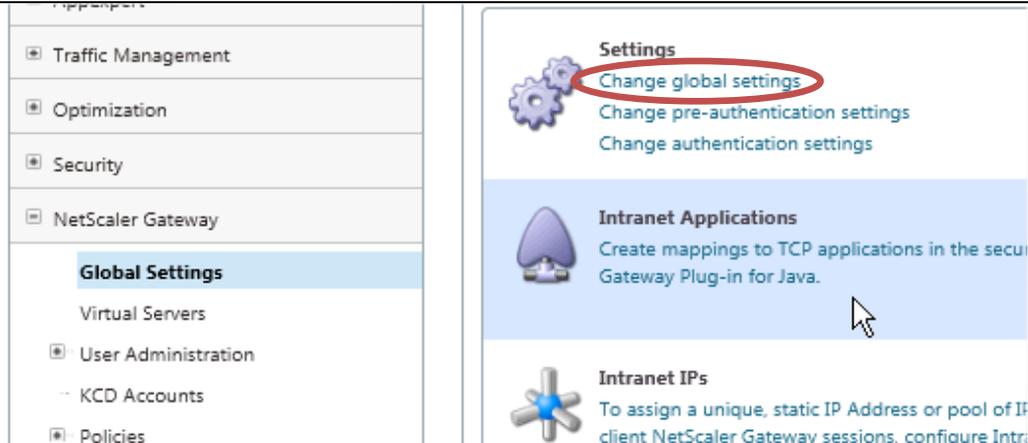


Si ce message d'erreur est obtenu, c'est qu'il n'y a pas de licence Netscape installée correctement.



5. Configuration de la fonction NetScaler Gateway

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

<p>Pour le moment, choisir LOCAL. Nous reviendrons plus tard sur la partie authentification.</p>	<p>Select an authentication type <input type="text" value="LOCAL"/></p> <p>User Name* <input type="text" value="Guest"/></p> <p>Password <input type="password" value="....."/></p>
<p>Choisir Allow.</p> <p>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.</p>	<p>Configure Authorization</p> <p><input checked="" type="radio"/> Allow <input type="radio"/> Deny</p> <p>Select authorization requirements for your users. Authorization is applied globally and can be overridden by configuring additional authorization policies. This setting can be changed in NetScaler Gateway global settings.</p> <p>Redirect Requests for Port 80 to a Secure Port</p> <p><input checked="" type="checkbox"/> Redirect to secure Web address</p> <p>Type the secure Web address <input type="text" value="https://claudio.vxp.fr"/></p> <p>Users might leave off the "s" in https:// when typing in a Web address to the NetScaler Gateway. If this occurs, you can enable the request to automatically be redirected to a secure Web address.</p>
<p>Choisir NetScaler Gateway Plug-in.</p> <p>Cliquer sur Next, Finish, et Exit.</p>	<p>Clientless Access</p> <p><input checked="" type="radio"/> NetScaler Gateway Plug-in Users are allowed to log on using the NetScaler Gateway Plug-in only.</p> <p><input type="radio"/> Use the NetScaler Gateway Plug-in and allow access scenario fallback Users log on using the NetScaler Gateway Plug-in. If users fail an endpoint analysis scan, they are permitted to log on using clientless access with limited access to network resources.</p> <p><input type="radio"/> Allow users to log on using Clientless Access only Users log on with a Web browser and are permitted limited access to network resources.</p> <p>Configure Domains for Clientless Access</p>
<p>Dans la section NetScaler Gateway, puis Global Settings, cliquer sur Change global settings.</p>	 <p>Traffic Management</p> <p>Optimization</p> <p>Security</p> <p>NetScaler Gateway</p> <p>Global Settings</p> <p>Virtual Servers</p> <p>User Administration</p> <p>KCD Accounts</p> <p>Policies</p> <p>Settings</p> <p>Change global settings</p> <p>Change pre-authentication settings</p> <p>Change authentication settings</p> <p>Intranet Applications</p> <p>Create mappings to TCP applications in the security Gateway Plug-in for Java.</p> <p>Intranet IPs</p> <p>To assign a unique, static IP Address or pool of IP client NetScaler Gateway sessions, configure Intranet</p>

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**.

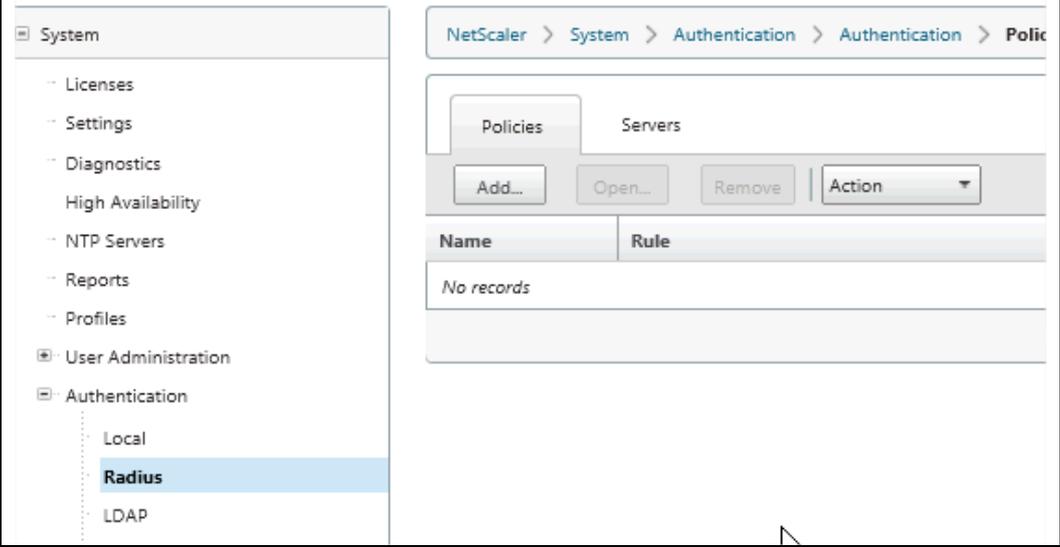
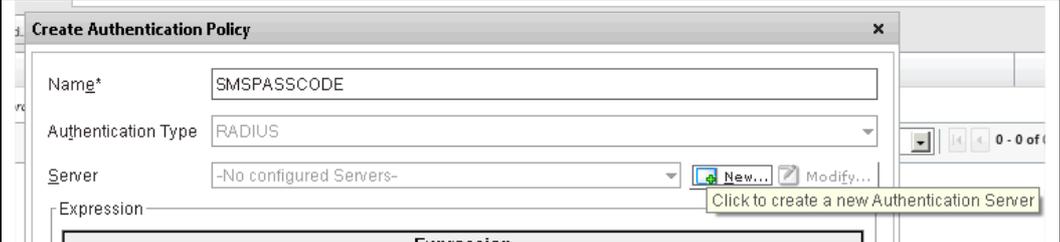
The screenshot shows the 'Global NetScaler Gateway Settings' dialog box with the 'Published Applications' tab selected. The settings are as follows:

Setting	Value
ICA Proxy*	ON
Web Interface Address	http://votre Citrix Web Interface
Web Interface Portal Mode*	NORMAL
Single Sign-on Domain	VOTRE DOMAIN
Citrix Receiver Home Page	
Account Services Address	

A yellow tooltip is visible at the bottom, stating: 'Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.' The dialog has 'OK' and 'Close' buttons at the bottom right.

6. Configuration de l'authentification RADIUS pour SMSPASSCODE

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

<p>Dans la partie System, puis Authentication, puis Radius : cliquer sur Add.</p>	
<p>Entrer un nom et cliquer sur le bouton New.</p>	

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**.

Configure Authentication Server

Name*

Authentication Type

Server

IP Address* IPv6 Port Time-out (seconds)

Details

Secret Key*

Confirm Secret Key*

Send Calling Station ID

NAS ID

Enable NAS IP address extraction

Group Vendor Identifier Group Prefix

Group Attribute Type Group Separator

IP Address Vendor Identifier IP Address Attribute Type

Password Vendor Identifier Password Attribute Type

Password Encoding Accounting

Default Authentication Group

Help

Ajouter l'expression ns_true.

Create Authentication Policy

Name*

Authentication Type

Server

Expression

Match Any Expression AND OR (+) + (-) -

Named Expressions

Preview Expression

Click to add selected Named expression

Help

Cliquer sur **Create**.

Create Authentication Policy

Name* SMSPASSCODE

Authentication Type RADIUS

Server SMSPASSCODE

Expression

ns_true

Match Any Expression Add... Modify... Remove AND OR (+) + (-) -

Named Expressions General True value Add Expression

Preview Expression ns_true

Help Create Close

Ensuite le Virtual Server NetScaler Gateway va être "lié".

Aller dans la section **NetScaler Gateway**,

puis **Virtual Servers**.

Cliquer sur la VIP Gateway puis sur **Open**.

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add... Open... Remove Action

Name	State	IP Address	Port
Claude	Up	192.168.0.104	

Show Unlicensed Features

Cliquer sur l'onglet **Authentification** et sur le bouton **Insert Policy**.

Name* Claude IP Address 192 . 168 . 0 . 104
Protocol* SSL Port* 444
 Network VServer Range 1 Max_Users 0
 SmartAccess Mode Basic Mode AppFlow Logging Down state flush Double Hop

Certificates | **Authentication** | Bookmarks | Policies | Intranet Applications | Intranet IPs | Published Applications | Advanced

User Authentication
If your NetScaler Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.
 Enable Authentication

Authentication Policies

Primary | Secondary | **Group Extraction**

Priority	Policy Name	Expression	Profile
Use "Insert Policy" to get started.			

Details
No item selected.

Insert Policy Unbind Policy Regenerate Priorities

Sélectionner la policy **SMSPASSCODE** précédemment créée, puis cliquer sur **OK**.

Authentication Policies

Primary | Secondary | **Group Extraction**

Priority	Policy Name	Expression	Profile
100	SMSPASSCODE	ns_true	SMSPASSCODE

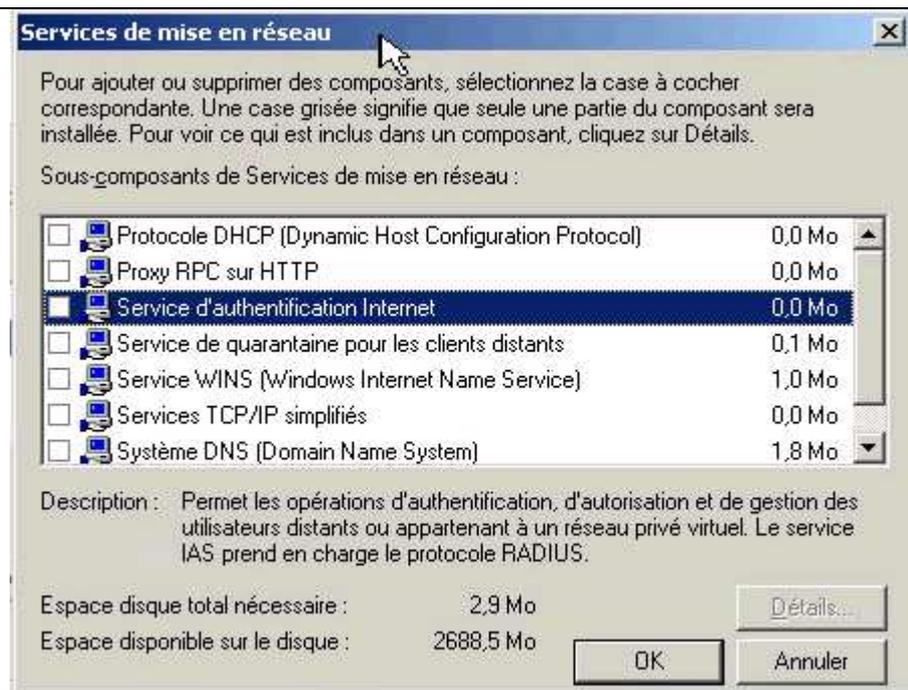
Details : SMSPASSCODE
Type: RADIUS Request Profile: SMSPASSCODE Rule: ns_true

7. Configuration de l'authentification RADIUS pour SMS PASSCODE

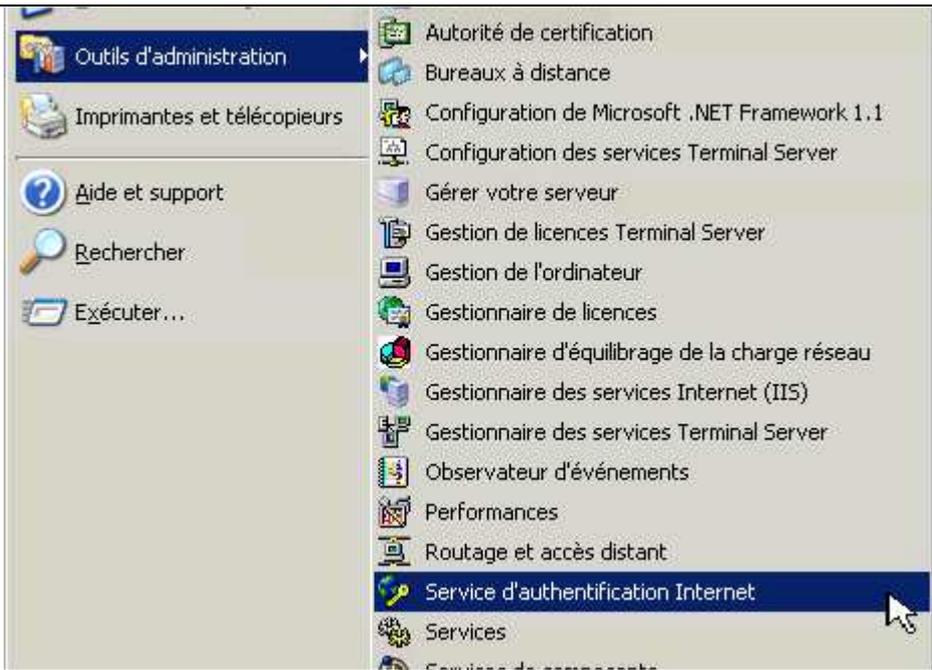
Pour faire fonctionner l'authentification SMS PASSCODE avec NetScaler, il est nécessaire d'installer le composant "Service d'authentification Internet". Ce service peut être installé sur le serveur ou est installé SMSPASSCODE.

Sur un Windows 2003 :

Ajouter le composant "Service d'authentification Internet".



Lancer ensuite la console d'administration : **Service d'authentification Internet**

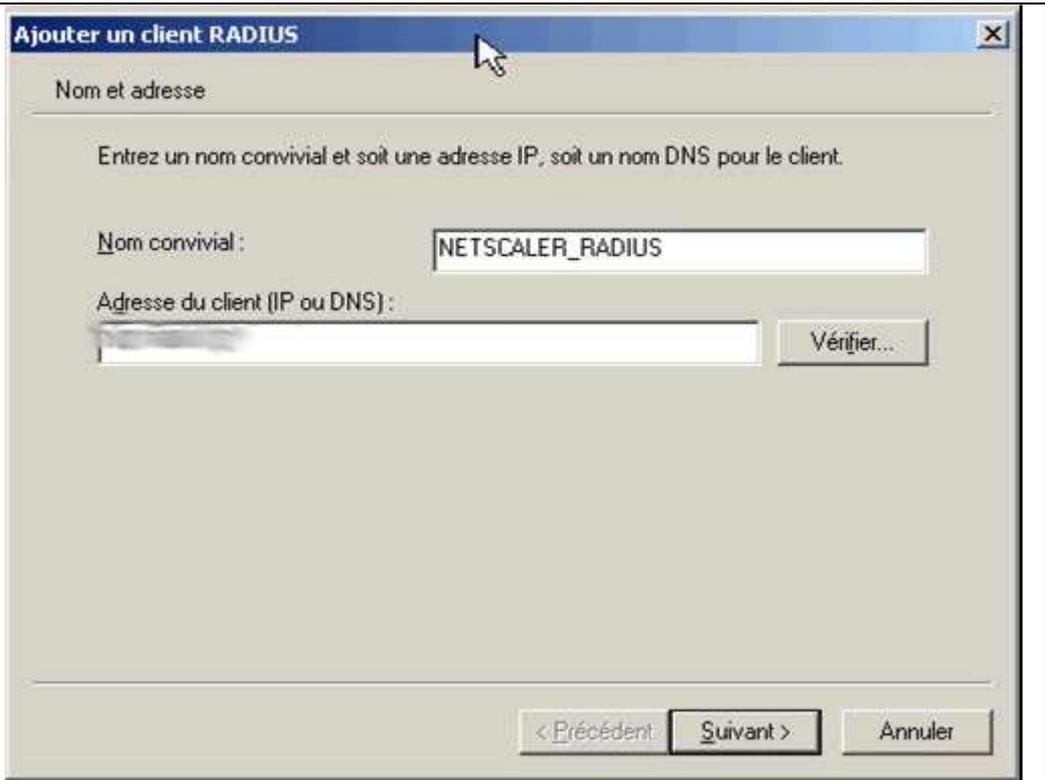


Dans la zone Client RADIUS, cliquer sur **Ajouter un client RADIUS.**



Ajouter les informations IP de l'Appliance NetScaler Gateway.

Ne pas mettre la VIP Gateway.



Ajouter un client RADIUS

Nom et adresse

Entrez un nom convivial et soit une adresse IP, soit un nom DNS pour le client.

Nom convivial : NETSCALER_RADIUS

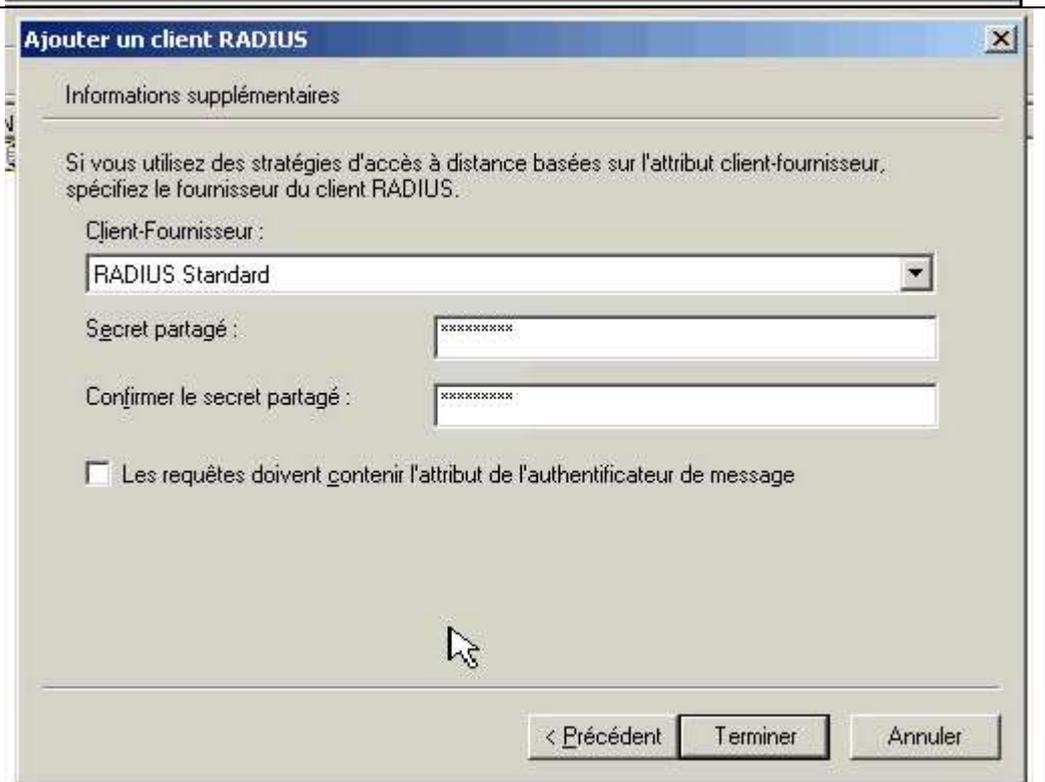
Adresse du client (IP ou DNS) :

Véifier...

< Précédent Suivant > Annuler

Entrer les informations suivantes :

RADIUS standard
et choisir un mot de passe.



Ajouter un client RADIUS

Informations supplémentaires

Si vous utilisez des stratégies d'accès à distance basées sur l'attribut client-fournisseur, spécifiez le fournisseur du client RADIUS.

Client-Fournisseur : RADIUS Standard

Secret partagé :

Confirmer le secret partagé :

Les requêtes doivent contenir l'attribut de l'authentificateur de message

< Précédent Terminer Annuler



8. Configuration SMSPASSECODE

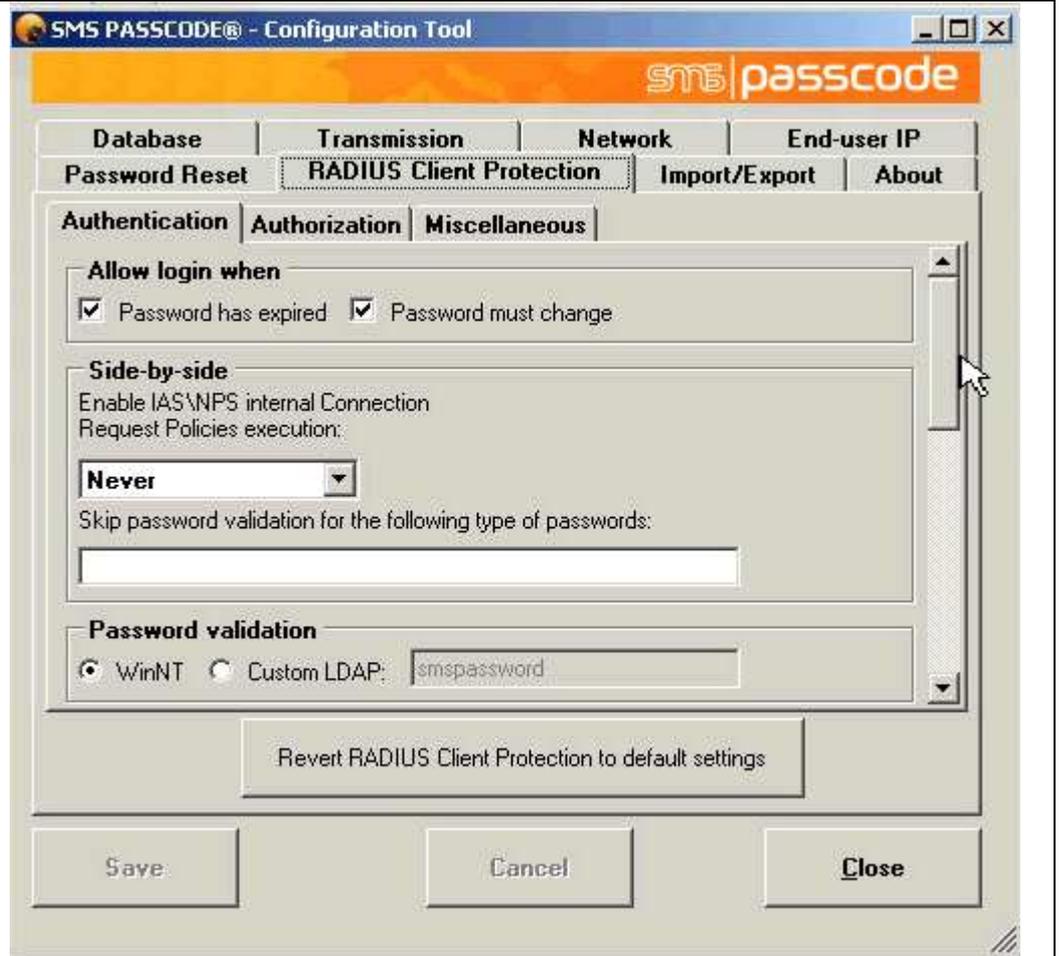
Lancer le setup de SMS PASSCODE sur le serveur SMS PASSCODE.



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

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

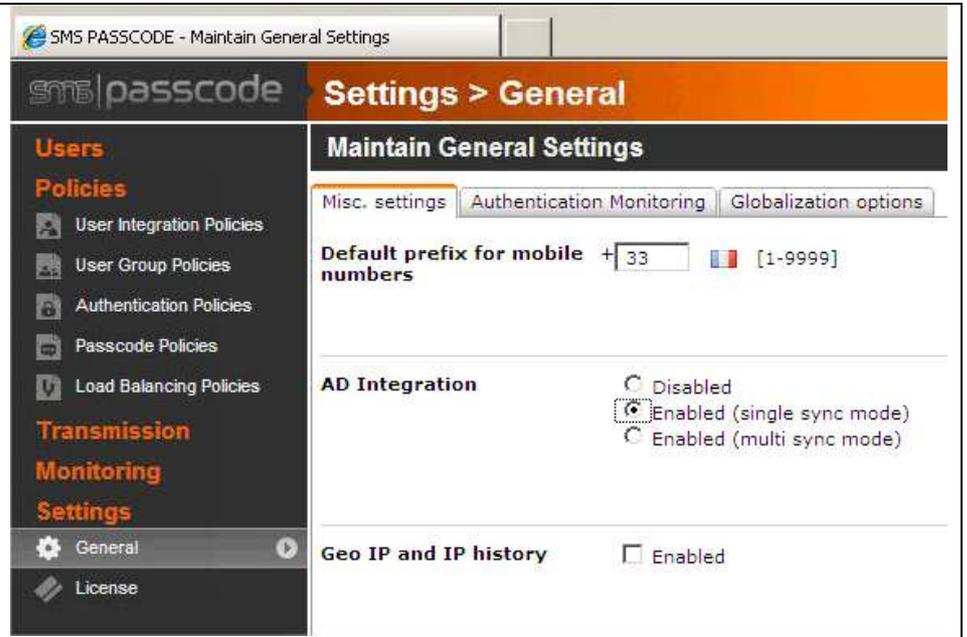
Cliquez sur SAVE si besoin.



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.

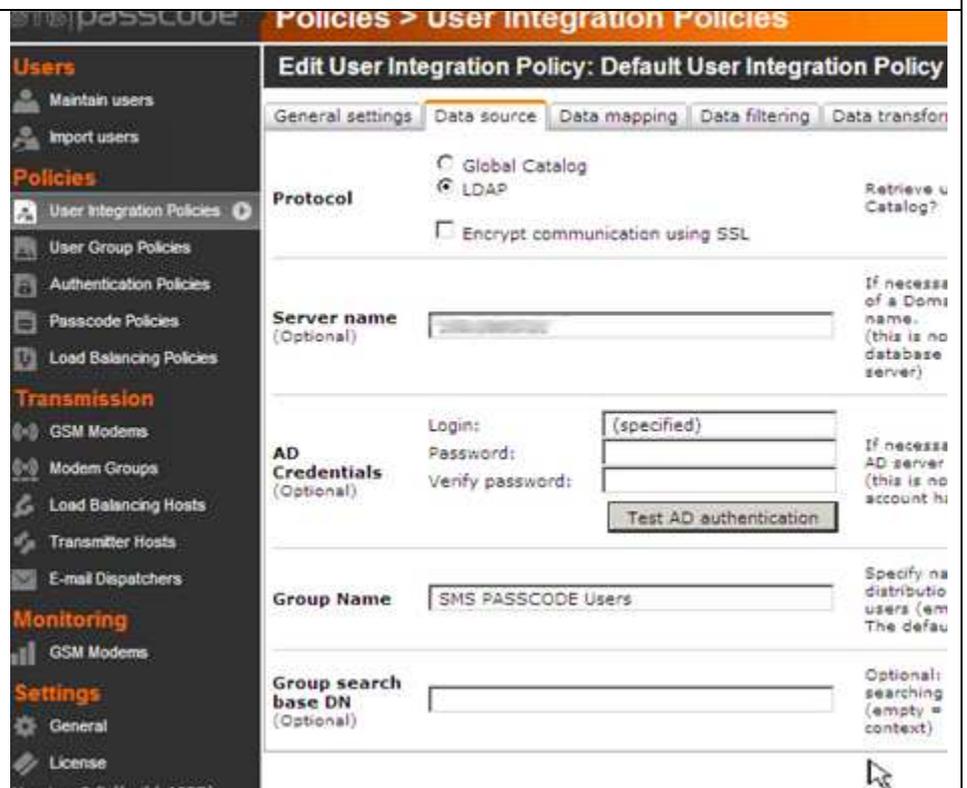
Dans la zone **Settings > General**
Cocher la case **Enabled** dans la zone **AD intégration**.



The screenshot shows the 'SMS PASSCODE - Maintain General Settings' page. The left sidebar contains navigation options: Users, Policies (User Integration Policies, User Group Policies, Authentication Policies, Passcode Policies, Load Balancing Policies), Transmission, Monitoring, Settings (General, License), and License. The main content area is titled 'Settings > General' and 'Maintain General Settings'. It includes tabs for 'Misc. settings', 'Authentication Monitoring', and 'Globalization options'. The 'Default prefix for mobile numbers' is set to '+33 [1-9999]'. The 'AD Integration' section has three radio buttons: 'Disabled', 'Enabled (single sync mode)' (which is selected), and 'Enabled (multi sync mode)'. The 'Geo IP and IP history' section has an 'Enabled' checkbox.

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.



The screenshot shows the 'SMS PASSCODE - Policies > User Integration Policies' page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Edit User Integration Policy: Default User Integration Policy'. It includes tabs for 'General settings', 'Data source', 'Data mapping', 'Data filtering', and 'Data transform'. The 'Data source' tab is active. The 'Protocol' section has two radio buttons: 'Global Catalog' and 'LDAP' (which is selected). There is a checkbox for 'Encrypt communication using SSL'. The 'Server name' field is optional. The 'AD Credentials' section has fields for 'Login', 'Password', and 'Verify password', with a 'Test AD authentication' button. The 'Group Name' field is set to 'SMS PASSCODE Users'. The 'Group search base DN' field is optional.

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.

Propriétés de : SMS PassCode Users

Général Membres Membre de Géré par

SMS PassCode Users

Nom de groupe (antérieur à Windows 2000) : SMS PassCode Users

Description :

Adresse de messagerie :

Étendue du groupe

Domaine local

Globale

Universelle

Type de groupe

Sécurité

Distribution

Remarques :

OK Annuler Appliquer

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 où les SMS sont inutilisables (PB de réseaux GSM...).

Propriétés de : François GAGNÉ.

Environnement Sessions Contrôle à distance

Profil des services Bureau à distance Bureau virtuel personnel COM+

Général Adresse Compte Profil Téléphones Organisation Membre de Appel entrant

François GAGNÉ.

Prénom : François Initiales : GAGNÉ

Nom :

Nom complet : François GAGNÉ.

Description :

Bureau :

Numéro de téléphone : Autre...

Adresse de messagerie : fgagne@vxpert.fr

Page Web : Autre...

OK Annuler Appliquer Aide

Vérifier les champs Tél. mobile.

Propriétés de : François GAGNÉ. ?

Profil des services Bureau à distance | Bureau virtuel personnel | COM+

Environnement | Sessions | Contrôle à distance

Général | Adresse | Compte | Profil | **Téléphones** | Organisation | Membre de | Appel entrant

Numéros de téléphone

Domicile : Autres...

Radiomessagerie : Autres...

Tél. mobile : Autres...

Télécopie : Autres...

Téléphone IP : Autres...

Et vérifier l'appartenance de l'utilisateur au groupe SMS PassCode Users.

Propriétés de : François GAGNÉ. ?

Environnement | Sessions | Contrôle à distance

Profil des services Bureau à distance | Bureau virtuel personnel | COM+

Général | Adresse | Compte | Profil | Téléphones | Organisation | Membre de | Appel entrant

Membre de :

Nom	Dossier Services de domaine Active Directory
SMS PassCode Users	
Utilisateurs du domaine	

Ajouter... Supprimer

Groupe principal : Utilisateurs du domaine

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

Users

- Maintain users
- Import users

Policies

- User Integration Policies
- User Group Policies
- Authentication Policies
- Passcode Policies
- Load Balancing Policies

Transmission

- GSM Modems

Maintain users

AD Integration

Last refresh attempt **Successful**

Last successful refresh

- Time: 03/06/2013 18:06:10
- Duration: 0,1s
- Server: [redacted]
- Users found: 1

Add new user... **4 licenses remaining**

Select columns Set filter

Display Name	Login (SAM)	Login (UPN)	Mobile number	Locked Out	
François GAGNÉ.	[redacted]	[redacted]	+336761 [redacted]	No	Test... Edit...

Voici le résultat lors du login sur le NetScaler.

Citrix Receiver

Ouvrez une session pour continuer.

Nom d'utilisateur :

Mot de passe:

Puis la demande du Passcode.

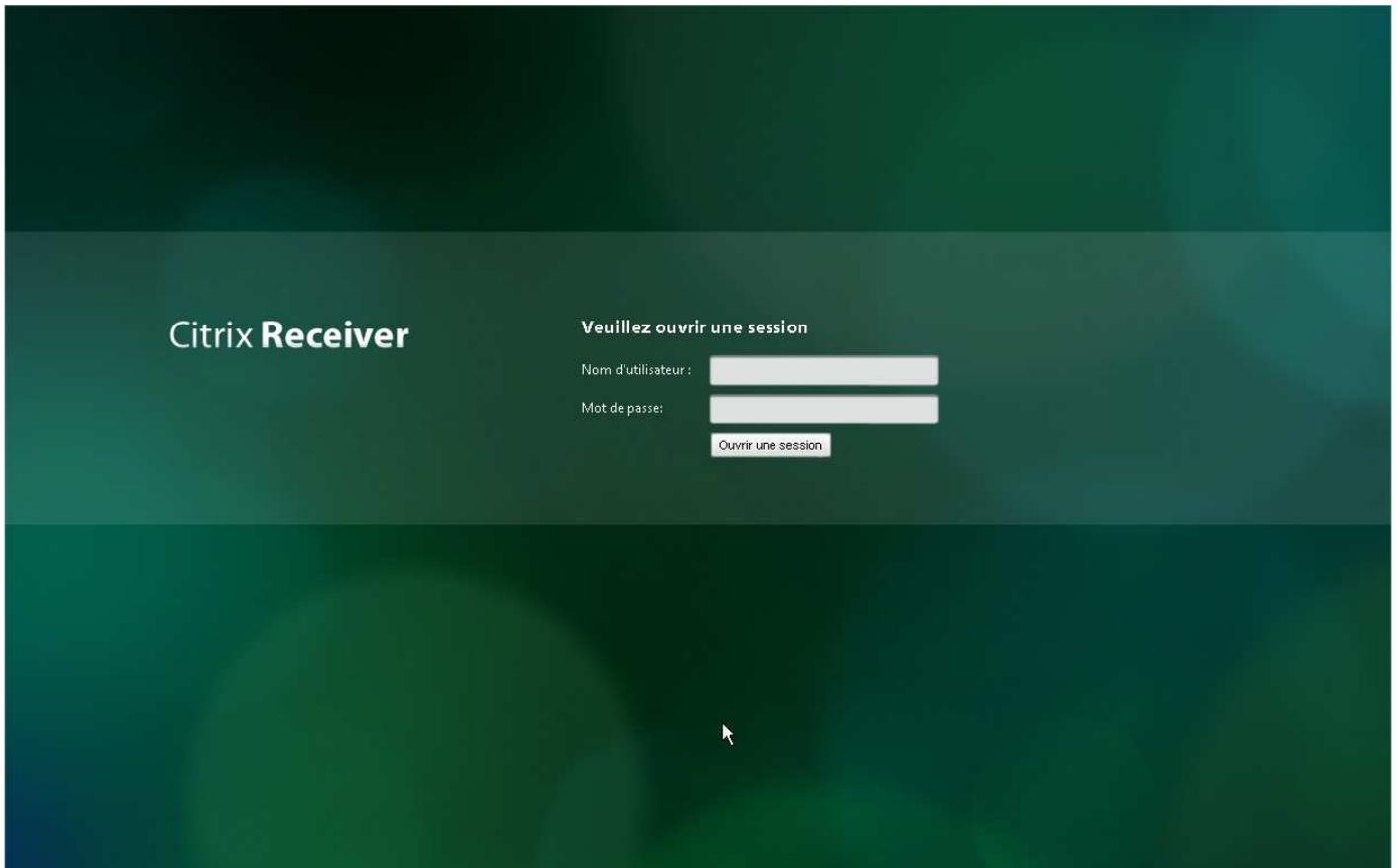
Citrix Receiver

Informations supplémentaires requises

Entrez votre réponse ci-dessous.

Enter 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
```

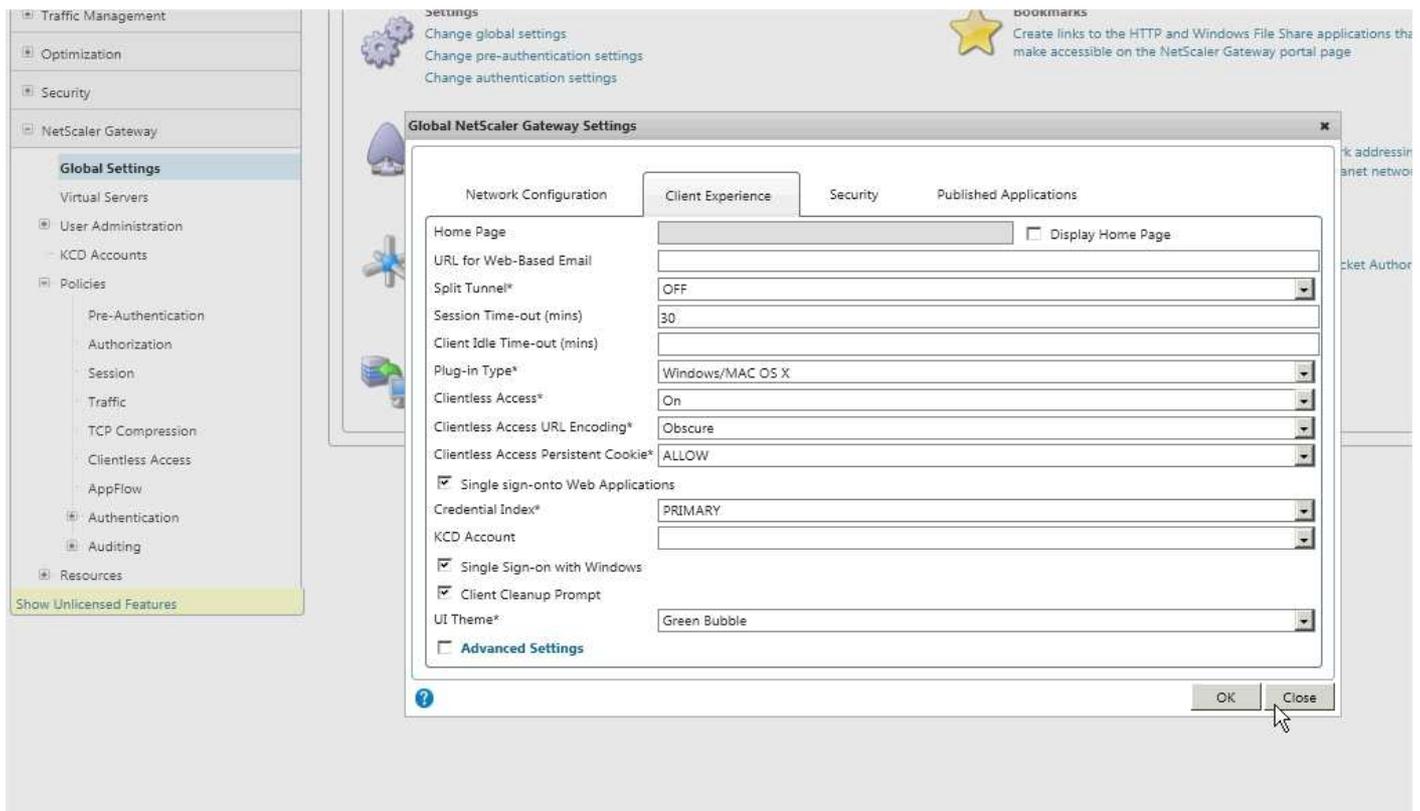
```

+ 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 /

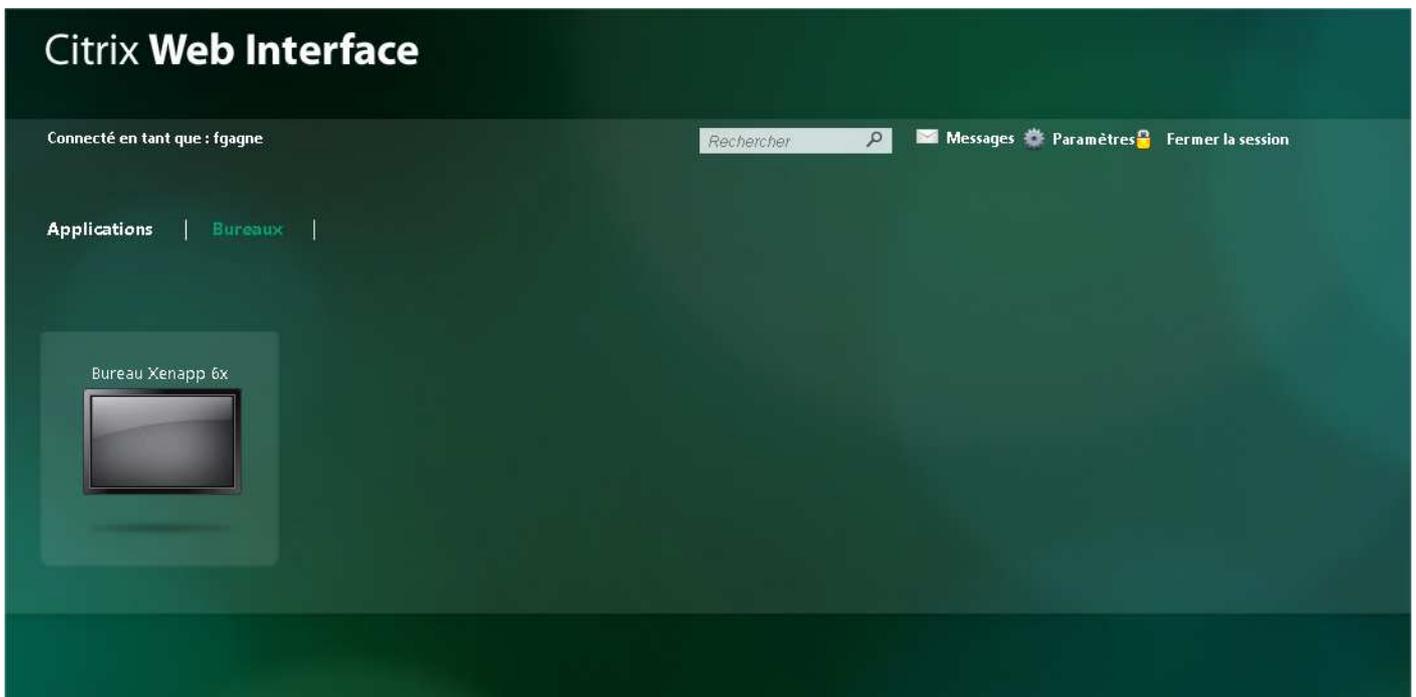


11. Installation du thème GREEN BUBBLE sur la Citrix Web Interface 5.4

<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