

Support de l'authentification forte

[FCS 3.1.8]

Sage - 10 rue Fructidor - 75 834 Paris Cedex 17 - France



SOMMAIRE

1	Principes de fonctionnement / Pré-requis	3
2	Paramétrage de l'authentification forte	3
2.1	Paramétrage de l'utilisateur	3
2.2	Paramètres de sécurité des certificats	4
2.2.1	Contrôle de la liste de révocation	5
2.2.2	Check certificate signature.....	5
2.2.3	Check certificate expiration date.....	5
2.2.4	Check certificate chain	5
2.2.5	Delete dead sessions every	6
2.3	Généralités	7
2.3.1	Certificats X509.....	7
2.3.2	Durée de validité d'une session ouverte en authentification forte.....	7
2.3.3	FAQ sur l'Active Directory	7

1 Principes de fonctionnement / Pré-requis

L'authentification forte est un système d'authentification en deux phases :

- Vérification du certificat sur l'Active Directory de l'entreprise
- Challenge/Response entre le client et le composant d'authentification permettant de vérifier que l'identité revendiquée par le client est bien la sienne.

Il est donc indispensable qu'un annuaire Active Directory, incluant pour chaque utilisateur un certificat valide, soit en place pour autoriser l'authentification forte des utilisateurs.

L'authentification forte ne concerne pour l'instant que les accès Web de SAGE Business Exchange.

Le fonctionnement de l'authentification forte est le suivant :

- L'utilisateur sélectionne son certificat dans la liste des certificats disponibles.
- Les informations sont envoyées à un composant d'authentification qui va vérifier auprès de l'Active Directory que le certificat existe, est valide, etc.
- Dans le cas où la vérification du certificat est faite, le composant d'authentification renvoie un challenge au client.
- Le client à l'aide de sa clef privée scelle le challenge et le renvoie au composant d'authentification.
- Le composant d'authentification vérifie le sceau du client et accepte la connexion, s'il parvient à décrypter le challenge du client.

A partir du moment où un certificat est vérifié sur l'Active Directory, la seconde étape (challenge/Response) doit s'effectuer dans un délai maximum d'une minute.

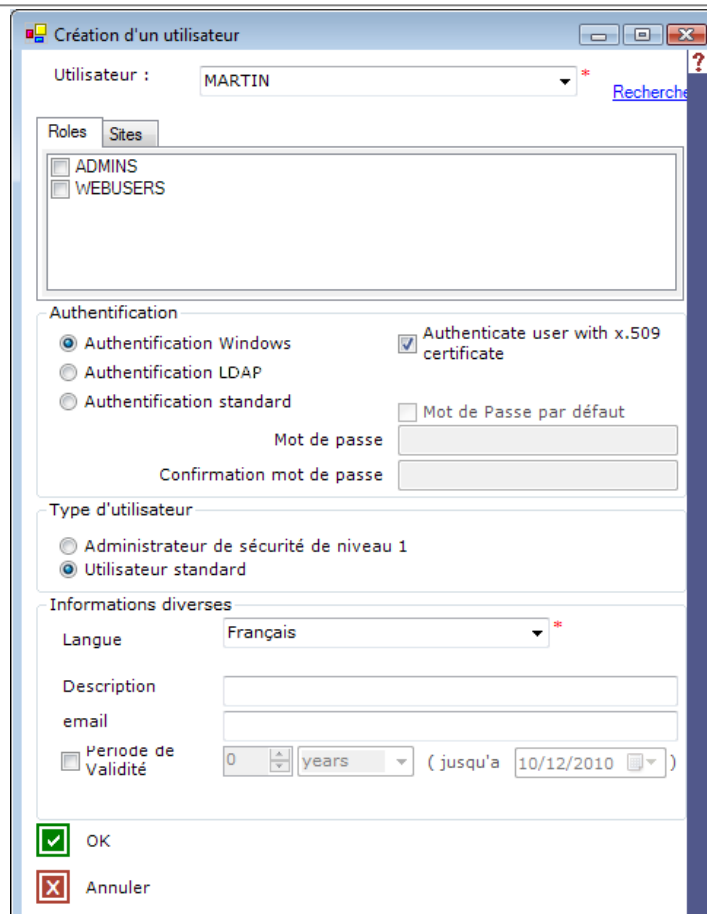
2 Paramétrage de l'authentification forte

2.1 Paramétrage de l'utilisateur

Pour paramétrer un utilisateur qui devra se connecter en authentification forte, celui-ci doit être déclaré en utilisateur Windows ou annuaire LDAP.

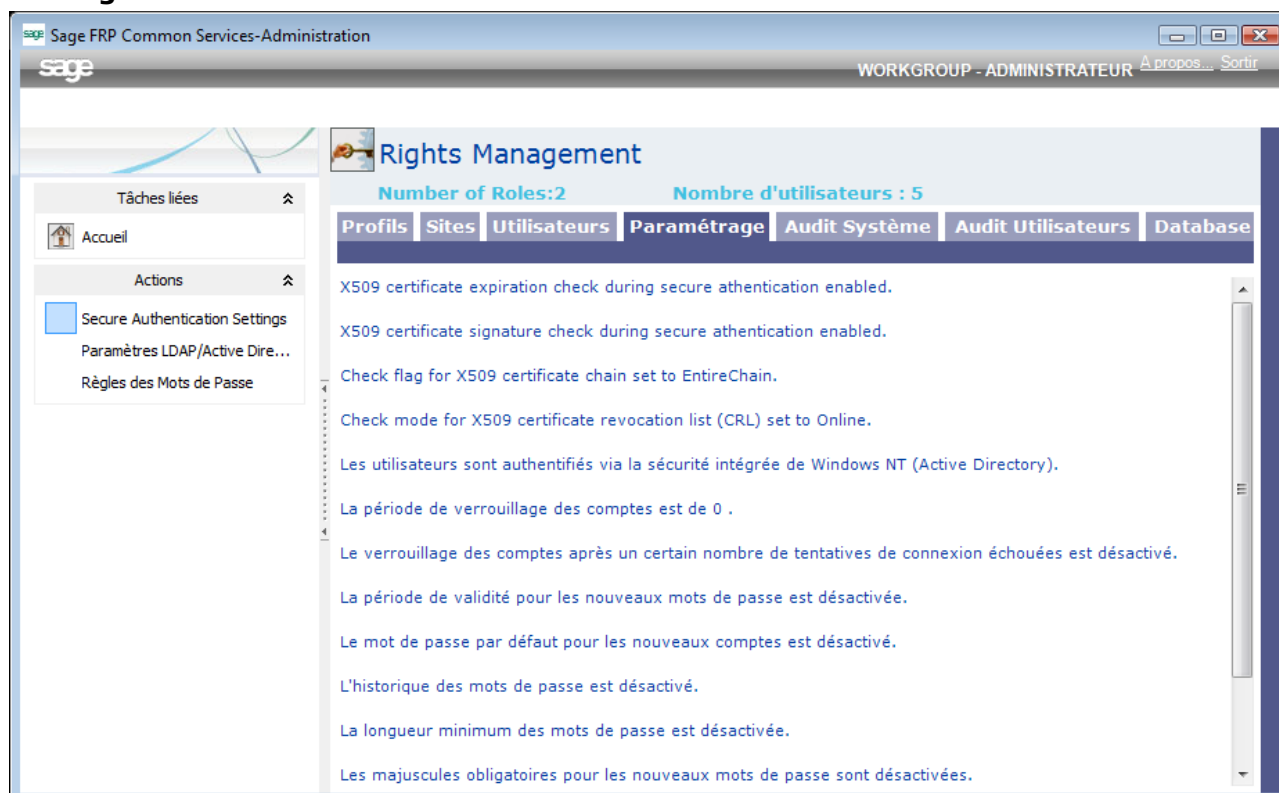
On a alors accès à l'option : « **Authenticate user with x.509 certificate** ».

C'est en cochant celle-ci que l'on indique que l'utilisateur doit se connecter via un certificat X509 et donc en authentification forte.



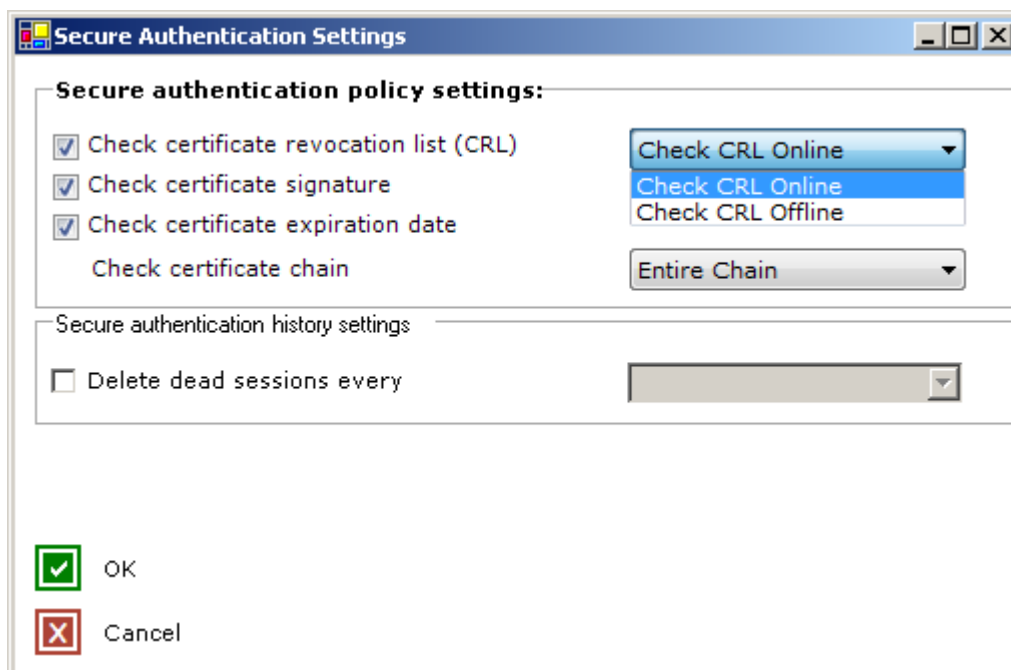
2.2 Paramètres de sécurité des certificats

En allant dans l'onglet **Paramétrage** de la gestion des droits, il est possible d'accéder à la gestion de la sécurisation des certificats en cliquant sur « **Secure Authentication Settings** » :



2.2.1 Contrôle de la liste de révocation

La première option est appelée « **Check certificate revocation list (CRL)** ».



Activée par défaut. Tant qu'elle est activée cette option déclenche la vérification de la présence d'un certificat que l'on tente d'utiliser dans une liste de révocation (CRL). Si c'est le cas, la tentative est alors rejetée, le certificat étant révoqué.

Peut fonctionner en mode Online ou Offline :

- **Online** : Valeur par défaut. La CRL sera recherchée sur le(s) point(s) de distribution indiqué(s) dans le certificat.
- **Offline** : La CRL sera recherchée sur un fichier contenu dans un des magasins locaux. La mise à jour de cette CRL est gérée par l'administrateur de sécurité du système d'information.

2.2.2 Check certificate signature

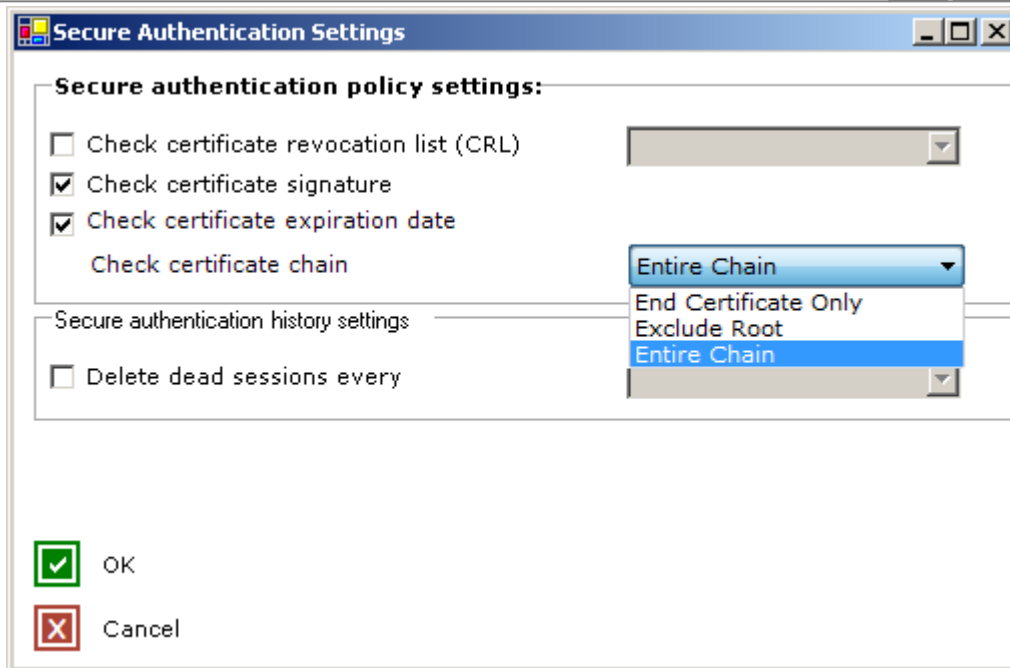
Activée par défaut. Assure la vérification de la signature du certificat à travers un processus CryptoAPI de Microsoft.

2.2.3 Check certificate expiration date

Activée par défaut. Assure le contrôle de l'atteinte de la date de fin de validité du certificat à travers la CryptoAPI de Microsoft.

2.2.4 Check certificate chain

Activée par défaut. Permet d'indiquer à quel niveau on contrôle la chaîne de certification.



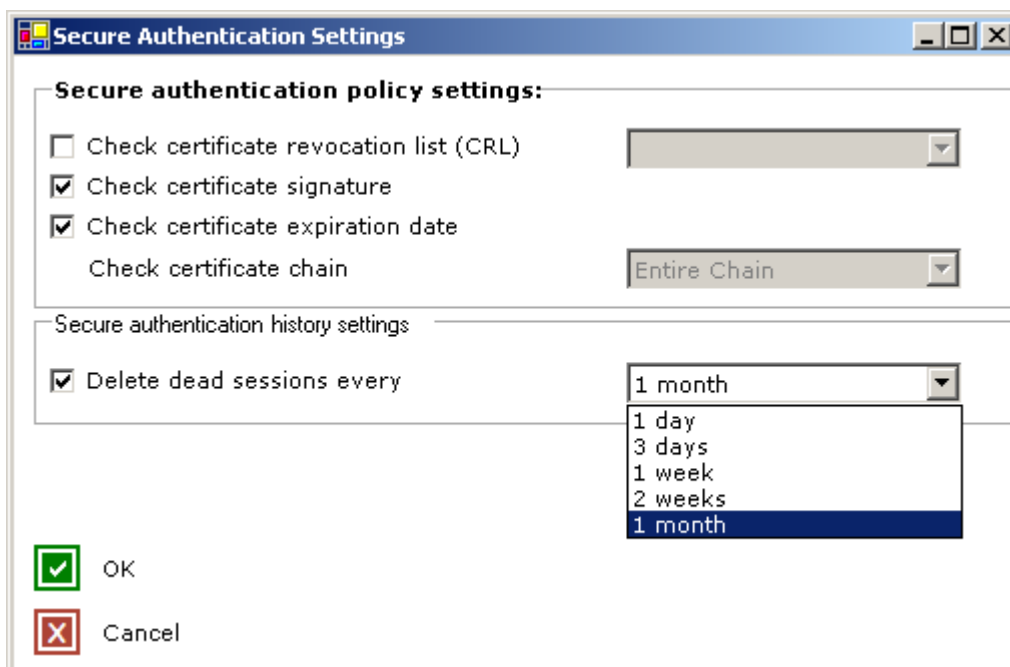
Entire Chain : Activée par défaut. Contrôle s'effectue sur l'intégralité de la chaîne de certification.

Exclude Root : Contrôle s'effectue sur l'intégralité de la chaîne de certification, à l'exclusion du certificat de l'Autorité de Certification (AC).

End Certificate Only : Contrôle effectué uniquement sur le certificat de l'utilisateur.

2.2.5 Delete dead sessions every

Désactivée par défaut. Permet d'indiquer combien de jour on souhaite conserver l'historique des sessions ouvertes au niveau de FCS.



Le fonctionnement, si l'option est activée, est le suivant : A chaque nouvelle ouverture d'une entrée dans la base de données des sessions (en effectuant une tentative de connexion par exemple), les données au-delà de la période choisie (1 jour, 3 jours, 1 semaine, 2 semaines ou 1 mois) sont purgées de la base de données.

2.3 Généralités

2.3.1 Certificats X509

Pour plus de renseignements sur les certificats X509, consulter les [RFC 2459](#) (section 4) et/ou la [RFC 5280](#).

2.3.2 Durée de validité d'une session ouverte en authentification forte

Une session utilisateur ouverte au niveau d'On Line Banking de SBE, en authentification forte, reste active tant qu'il n'y a pas de déconnexion de l'utilisateur.

Il n'y a pas de demande d'authentification supplémentaire en fonction d'un évènement ou d'une durée de connexion (par exemple, toutes les 10 minutes).

La durée d'une session Web reste liée à la période de timeout définie dans l'Administration Système de SBE (Service de Transaction – Dispositif protocole – On Line Banking – Timeout du cache de login), valeur par défaut = 600s.

2.3.3 FAQ sur l'Active Directory

- Peut-il y avoir plusieurs certificats définis pour un user ?
 - ⇒ Techniquement oui, rien ne s'y oppose.
- Peut-on forcer l'utilisation de tel ou tel certificats ?
 - ⇒ Au niveau du paramétrage FCS, non. Par contre l'utilisateur doit choisir avec quel certificat il se connecte à l'application lors de sa connexion.