

Numéro d'article: 329290 - Dernière mise à jour: lundi 29 octobre 2007 - Version: 8.4

Comment faire pour utiliser l'utilitaire ASP.NET pour chiffrer des chaînes d'identification et de connexion pour l'état de la session

Important Cet article contient des informations sur la modification du Registre. Avant de modifier le Registre, pensez à le sauvegarder et assurez-vous que vous savez le restaurer en cas de problème. Pour plus d'informations sur la sauvegarde, la restauration et la modification du Registre, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft.

[256986](http://support.microsoft.com/kb/256986/) (<http://support.microsoft.com/kb/256986/>) Description du Registre de Microsoft Windows

Résumé

Cet article explique étape par étape l'utilisation de l'utilitaire Aspnet_setreg.exe pour chiffrer des chaînes d'identification et de connexion pour l'état de la session. La version 1.0 de Microsoft ASP.NET requiert que vous stockiez les informations d'identification en texte brut dans les fichiers de configuration si vous souhaitez effectuer l'une des opérations suivantes :

- Modifier l'identité du processus de travail ASP.NET.
- Spécifier une identité d'emprunt.
- Spécifier une chaîne de connexion pour l'état de la session.

Lorsque vous appliquez le correctif logiciel décrit dans l'article 329250 de la Base de connaissances Microsoft (voir la section « Références »), vous pouvez utiliser des données chiffrées stockées dans le Registre au lieu de texte brut dans les sections de configuration suivantes :

- `<identity userName= password= />`
- `<processModel userName= password= />`
- `<sessionState stateConnectionString= sqlConnectionString= />`

Introduction

Recourez à l'utilitaire Aspnet_setreg.exe pour chiffrer et stocker ces valeurs d'attributs dans le Registre sous une clé sécurisée. Utilisez la fonction **CryptProtectData** avec l'indicateur CRYPTPROTECT_LOCAL_MACHINE pour chiffrer les informations d'identification. Étant donné que toute personne ayant accès à l'ordinateur peut appeler **CryptUnprotectData**, les données chiffrées sont stockées sous une clé de Registre sécurisée avec une liste de contrôle d'accès discrétionnaire forte (DACL). Lorsque ASP.NET analyse le fichier de configuration, il lit la clé de Registre sécurisée puis utilise **CryptUnprotectData** pour déchiffrer les données.

Inetinfo.exe qui s'exécute sous l'identité Système lit la section `< processModel />`. Pour lire les clés de Registre qui stockent le nom d'utilisateur et le mot de passe d'un processus de travail ASP.NET, le compte système doit avoir l'autorisation de lecture de ces clés.

Le processus de travail ASP.NET (Aspnet_wp.exe) lit les sections `< identity />` et `< sessionState />`. Pour lire ces clés de Registre, le compte du processus de travail doit avoir l'autorisation de lecture de ces clés. Si le contenu est hébergé sur un partage de noms UNC (Universal Naming Convention), le compte utilisé pour accéder au partage UNC doit avoir l'autorisation de lecture de ces clés.

Par défaut, les clés de Registre créées par Aspnet_setreg.exe accordent le contrôle total aux comptes Système, Administrateur et Créateur Propriétaire. Vous pouvez utiliser Regedt32.exe pour modifier la DACL sur la clé de Registre. Assurez-vous que les utilisateurs arbitraires ne peuvent pas lire les clés de Registre.

Redémarrage des services Internet (IIS)

Pour que les modifications prennent effet, vous devez redémarrer Microsoft Internet Information Services (IIS). En redémarrant les services Internet (IIS), vous démarrez un nouveau processus de travail ASP.NET. Pour cela, cliquez sur **Démarrer**, sur **Exécuter**, tapez **iisreset** dans la zone **Ouvrir**, puis cliquez sur **OK**.

Remarque Si le serveur que vous avez configuré est un contrôleur de domaine, vous devrez peut-être redémarrer le serveur.

Plus d'informations

Téléchargement et exécution d'Aspnet_setreg.exe

Vous pouvez télécharger le fichier suivant à partir du Centre de téléchargement Microsoft :



[Télécharger le package Aspnet_setreg.exe maintenant.](http://download.microsoft.com/download/2/9/8/29829651-e0f0-412e-92d0-e79da46fd7a5/aspnet_setreg.exe) (http://download.microsoft.com/download/2/9/8/29829651-e0f0-412e-92d0-e79da46fd7a5/aspnet_setreg.exe)

Date de publication : 11 avril 2003

Pour plus d'informations sur la façon de télécharger des fichiers des services de support technique Microsoft, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft.

[119591](http://support.microsoft.com/kb/119591/) (<http://support.microsoft.com/kb/119591/>) Comment faire pour obtenir des fichiers de support technique Microsoft auprès des services en ligne

Microsoft a analysé ce fichier en vue de détecter la présence de virus. Microsoft a utilisé les logiciels de détection de virus les plus récents disponibles à la date de publication de ce fichier. Le fichier est conservé sur des serveurs sécurisés, empêchant toute modification non autorisée du fichier.

Pour afficher tous les commutateurs de ligne de commande disponibles et leur utilisation, exécutez cet outil à partir de l'invite de commandes sans commutateur de ligne de commande. Si vous avez enregistré cet outil sur C:\Tools\, exécutez la commande suivante à partir de l'invite de commandes pour afficher tous ses commutateurs disponibles et les fichiers d'aide associés :

C:\Tools>aspnet_setreg.exe

Utilisation d'attributs chiffrés dans le fichier de configuration

Avertissement Toute modification incorrecte du Registre à l'aide de l'Éditeur du Registre ou d'une autre méthode peut entraîner des problèmes sérieux. Ces problèmes peuvent vous obliger à réinstaller votre système d'exploitation. Microsoft ne peut pas garantir que ces problèmes puissent être résolus. Vous assumez l'ensemble des risques liés à la modification du Registre.

Remarque Cet outil crée les clés de Registre sous la sous-arborescence **HKEY_LOCAL_MACHINE**. Par défaut, seuls les administrateurs peuvent créer des clés sous cette sous-arborescence. Assurez-vous que vous avez ouvert une session en tant qu'administrateur pour pouvoir créer ces clés de Registre.

1. Chiffrez les attributs **userName** et **password** qui seront utilisés dans la section **<identity>**. (Vous pouvez également procéder de cette façon pour les autres sections mentionnées dans cet article.) Pour cela, tapez la commande suivante sur la ligne de commande :

**C:\Tools>aspnet_setreg.exe -k:SOFTWARE\MY_SECURE_APP\identity -
u:"yourdomainname\username" -p:"password"**

Cette commande chiffre les attributs **userName** et **password**, crée des clés de Registre à l'emplacement que vous spécifiez, puis stocke les attributs dans ces clés de Registre. Cette commande génère également une sortie spécifiant comment modifier votre fichier Web.config ou Machine.config afin qu'ASP.NET utilise ces clés pour lire ces informations dans le Registre.

Une fois cette commande exécutée, vous recevez une sortie en ces termes :

Please edit your configuration to contain the following:

```
userName="registry:HKLM\SOFTWARE\MY_SECURE_APP\identity\ASPNET_SETREG,userName"
password="registry:HKLM\SOFTWARE\MY_SECURE_APP\identity\ASPNET_SETREG,password"
```

The DACL on the registry key grants Full Control to System, Administrators, and Creator Owner.

If you have encrypted credentials for the <identity/> configuration section, or a connection string for the <sessionState/> configuration section, ensure that the process identity has Read access to the registry key. Furthermore, if you have configured IIS to access content on a UNC share, the account used to access the share will need Read access to the registry key. Regedt32.exe may be used to view/modify registry key permissions.

You may rename the registry subkey and registry value in order to prevent discovery.

2. Modifiez le fichier de configuration correspondant pour pointer sur ces clés de Registre. Si ces valeurs doivent être utilisées dans la section **<identity>**, la section **<identity>** résultante se présente de la manière suivante.

```
<identity impersonate="true"
userName="registry:HKLM\SOFTWARE\MY_SECURE_APP\identity\ASPNET_SETREG,userName"
password="registry:HKLM\SOFTWARE\MY_SECURE_APP\identity\ASPNET_SETREG,password" />
```

3. Accordez des autorisations de lecture au compte de processus Aspnet_wp.exe. Pour plus d'informations sur la modification des autorisations d'accès aux clés de Registre, consultez la section « Utilisation de Regedt32.exe pour accorder au compte ASP.NET des autorisations d'accès à ces clés de Registre » dans cet article.

Utilisation de Regedt32.exe pour accorder au compte ASP.NET des autorisations d'accès à ces clés de Registre

Avertissement Toute modification incorrecte du Registre à l'aide de l'Éditeur du Registre ou d'une autre méthode peut entraîner des problèmes sérieux. Ces problèmes peuvent vous obliger à réinstaller votre système d'exploitation. Microsoft ne peut pas garantir que ces problèmes puissent être résolus. Vous assumez l'ensemble des risques liés à la modification du Registre.

1. Cliquez sur **Démarrer**, sur **Exécuter**, tapez **regedt32** dans la zone **Ouvrir**, puis cliquez sur **OK**.
2. Cliquez sur la sous-clé HKEY_LOCAL_MACHINE\SOFTWARE\MY_SECURE_APP\.
3. Dans le menu **Sécurité**, cliquez sur **Autorisations** pour ouvrir la boîte de dialogue **Autorisations**.

Sur un ordinateur Microsoft Windows XP ou Windows Server 2003, cliquez avec le bouton droit sur la clé de

Registre, puis cliquez sur **Autorisations**.

4. Cliquez sur **Ajouter**. Dans la boîte de dialogue qui s'ouvre, tapez **nom_serveur\ASPNET**(ou **nom_serveur\NetWork Service** si vous utilisez Windows Server 2003 (IIS 6.0)), et cliquez sur **OK**.
5. Assurez-vous que le compte que vous venez d'ajouter possède des autorisations de lecteur, puis cliquez sur **OK**.
6. Fermez l'Éditeur du Registre.

Références

Pour plus d'informations sur le correctif vous permettant d'utiliser les fonctionnalités décrites dans cet article, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft.
[329250](http://support.microsoft.com/kb/329250/) (<http://support.microsoft.com/kb/329250/>) CORRECTIF : Informations d'identification renforcées pour processModel, identité et sessionState

Pour plus d'informations sur le Registre de Microsoft Windows, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft.

[256986](http://support.microsoft.com/kb/256986/) (<http://support.microsoft.com/kb/256986/>) Description du Registre de Microsoft Windows

Pour plus d'informations sur ASP.NET, cliquez sur les numéros ci-dessous pour afficher les articles correspondants dans la Base de connaissances Microsoft.

[315158](http://support.microsoft.com/kb/315158/) (<http://support.microsoft.com/kb/315158/>) CORRECTIF : ASP.NET ne fonctionne pas avec le compte ASPNET par défaut sur un contrôleur de domaine

[317012](http://support.microsoft.com/kb/317012/) (<http://support.microsoft.com/kb/317012/>) Identité du processus et de la demande dans ASP.NET

Les informations contenues dans cet article s'appliquent au(x) produit(s) suivant(s):

- Microsoft ASP.NET 1.1
- Microsoft ASP.NET 1.0

Mots-clés : kbproductlink kbdownload kbconfig kbfix kbhowtomaster kbsecurity kbstate KB329290

L'INFORMATION CONTENUE DANS CE DOCUMENT EST FOURNIE PAR MICROSOFT SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE. L'UTILISATEUR ASSUME LE RISQUE DE L'UTILISATION DU CONTENU DE CE DOCUMENT. CE DOCUMENT NE PEUT ETRE REVENDU OU CEDE EN ECHANGE D'UN QUELCONQUE PROFIT.



Vous avez besoin d'une aide supplémentaire ?

Contactez le support technique par email, en ligne ou par téléphone