

KB - Granting folder permissions to IIS application pools

Whenever a new application pool is created, IIS creates a security identifier (SID) that represents the name of the application pool itself. For example, if you create an application pool with the name "Smartcrypt," a security identifier with the name "Smartcrypt" is created in Windows. Resources can be secured by using this identity. However, the identity is not a real user account and will not show up as a user in the Windows User Management Console.

This can be configured by selecting a folder in Windows Explorer and adding the "Smartcrypt" identity to the folder's Access Control List (ACL).

1. Open Windows Explorer
2. Select the directory the Smartcrypt Manager is installed under (eg: c:\web\mds)
3. Right click the directory and select **Properties**
4. Select the **Security** tab
5. Click the **Edit** button and then **Add** button
6. Click the **Locations** button and make sure that you select your computer.
7. Enter **IIS AppPool\<myappoolname>** (eg: IIS AppPool\smartcrypt) in the **Enter the object names to select:** text box.
8. Click the **Check Names** button and click **OK**.
9. Check **Modify** under the **Allow** column, and click **OK**, and **OK**.

By doing this, the file or directory you selected will now also allow the **Smartcrypt** identity access.

You can do this via the command-line by using the ICACLS tool. The following example gives modify access to the **Smartcrypt** identity to the folder C:\web\mds and all contents.

```
ICACLS "C:\web\mds" /grant "IIS AppPool\Smartcrypt":M /t
```