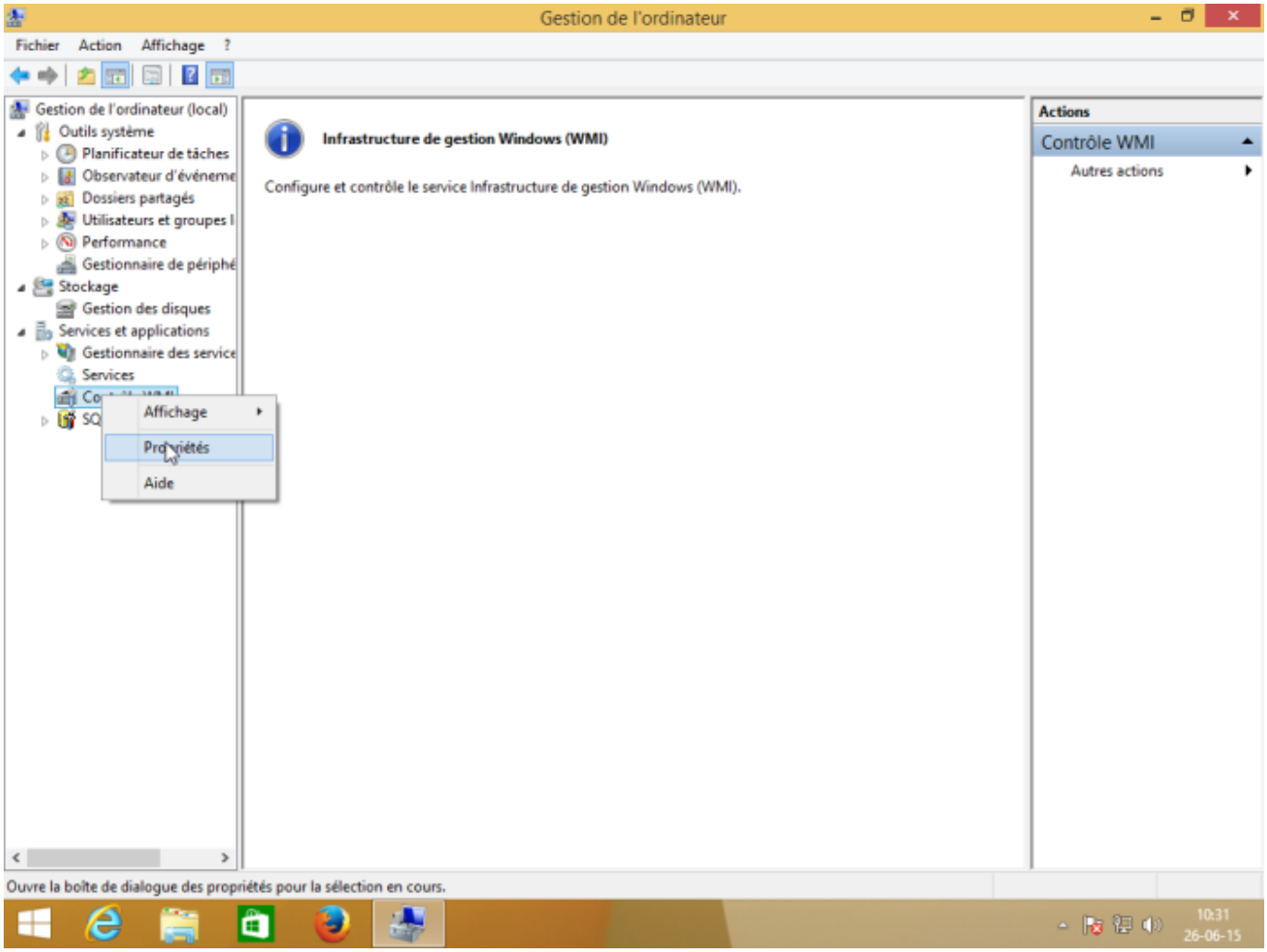
Enable WMI on Windows 7, 8 & 10

Enable remote access to WMI (always necessary)

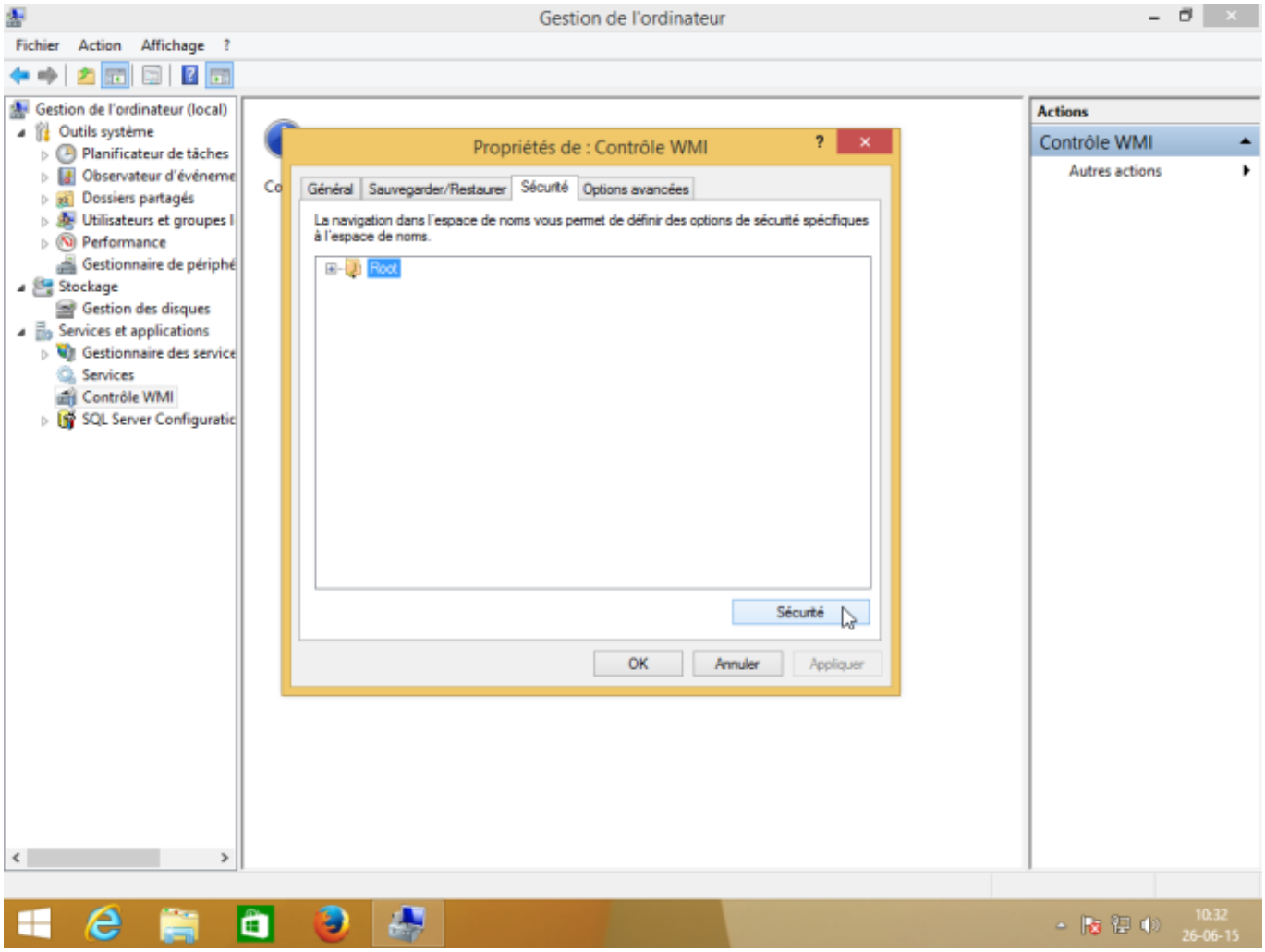
This involves giving remote access rights to the user account that will be used by ESIA to access WMI data. To do this :

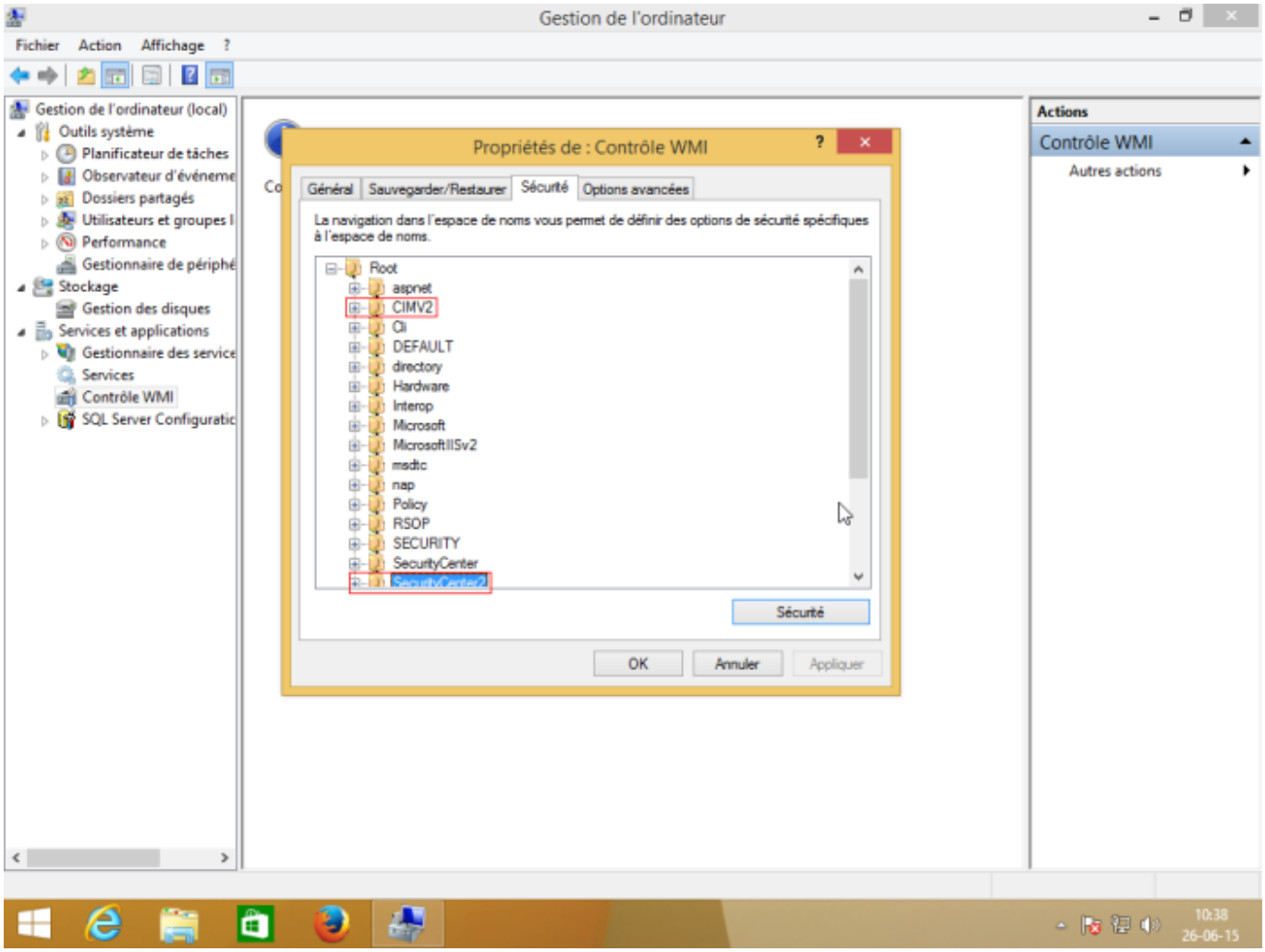
Go to “Computer Management” (or enter the command “wmimgmt.msc”). Then, scroll down to “Services and Applications” so that you can right-click on “WMI Control” and click on “Properties”.



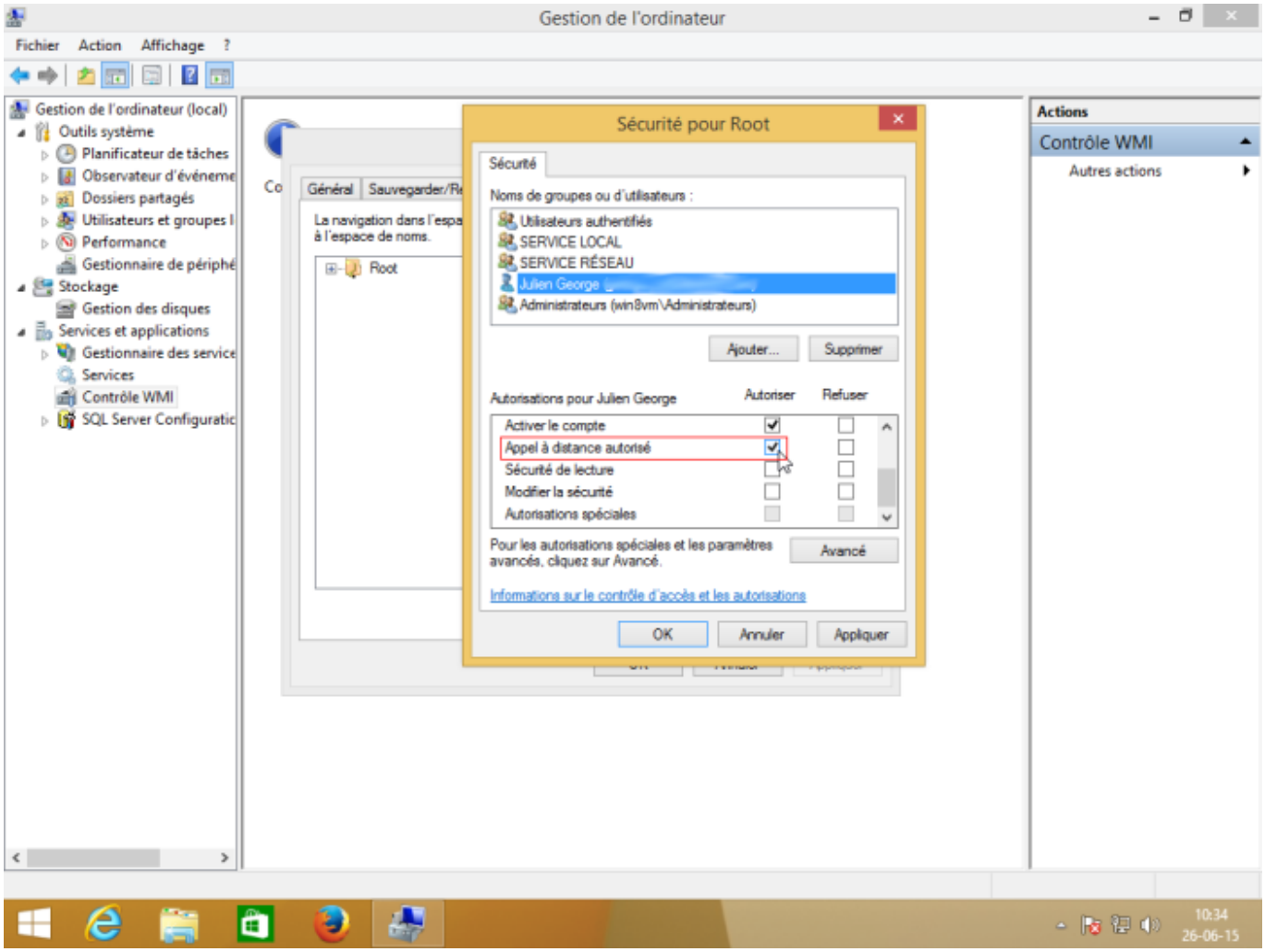
In the “Security” tab of “WMI Control Properties”, select the “Root” namespace and then click on “Security”.

If you want to fine-tune security, the namespaces 'Root→CIMV2' and 'Root→SecurityCenter2' are those used by ESIA.

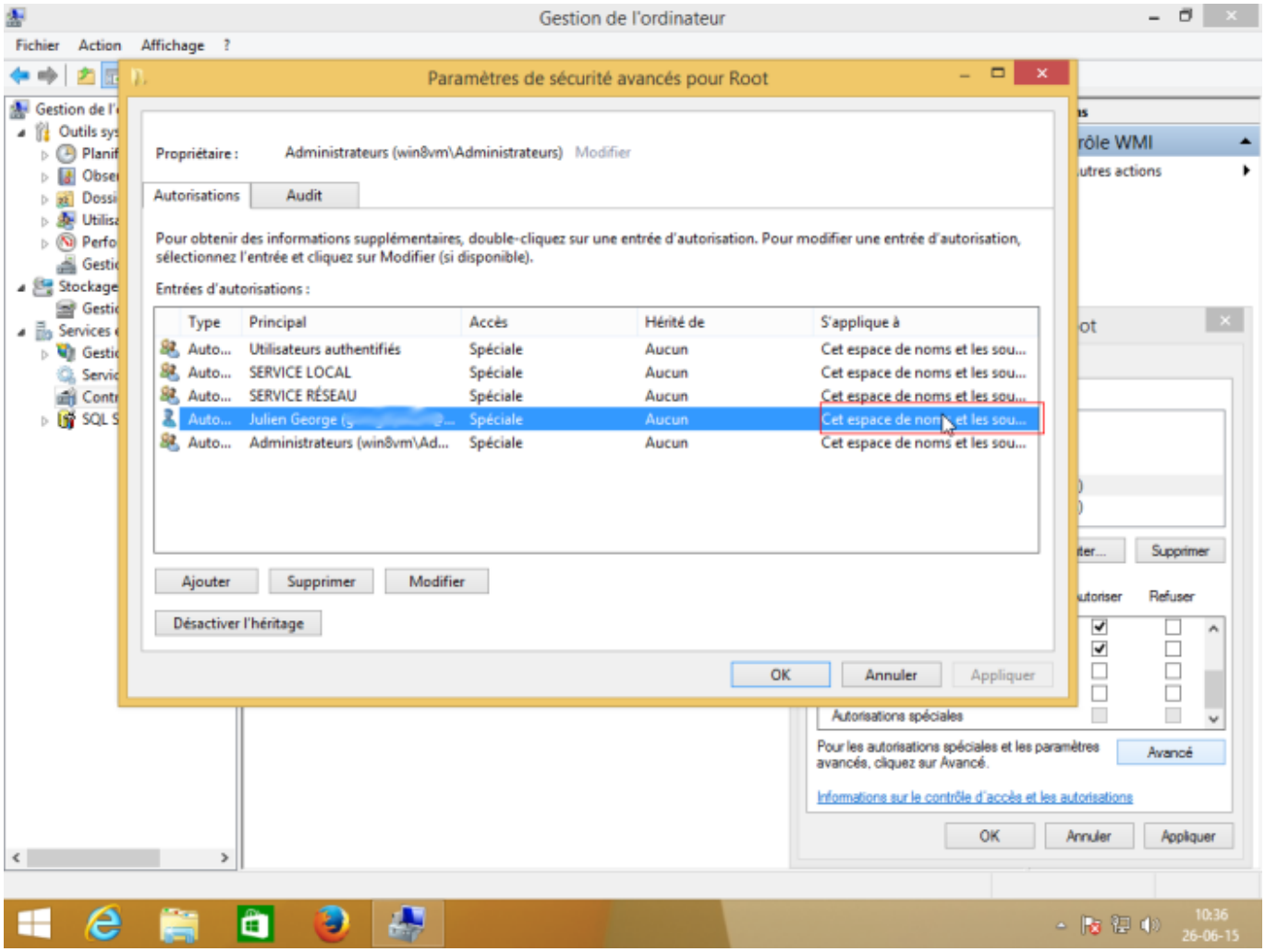

Gestion de l'ordinateur
Fichier Action Affichage ?
Gestion de l'ordinateur (local)
Outils système
Planificateur de tâches
Observateur d'événeme
Dossiers partagés
Utilisateurs et groupes l
Performance
Gestionnaire de périphé
Stockage
Gestion des disques
Services et applications
Gestionnaire des service
Services
Contrôle WMI
SQL Server Configuratic
Propriétés de : Contrôle WMI
Général
Sauvegarder/Restaurer
Sécurité
Options avancées
La navigation dans l'espace de noms vous permet de définir des options de sécurité spécifiques à l'espace de noms.
Root
Sécurité
OK
Annuler
Appliquer
Actions
Contrôle WMI
Autres actions
10:32
26-06-15



Select the user account that will be used for remote access and tick the “Authorise” boxes for “Enable account” and “Remote call authorised”, which are the 2 authorisations required.

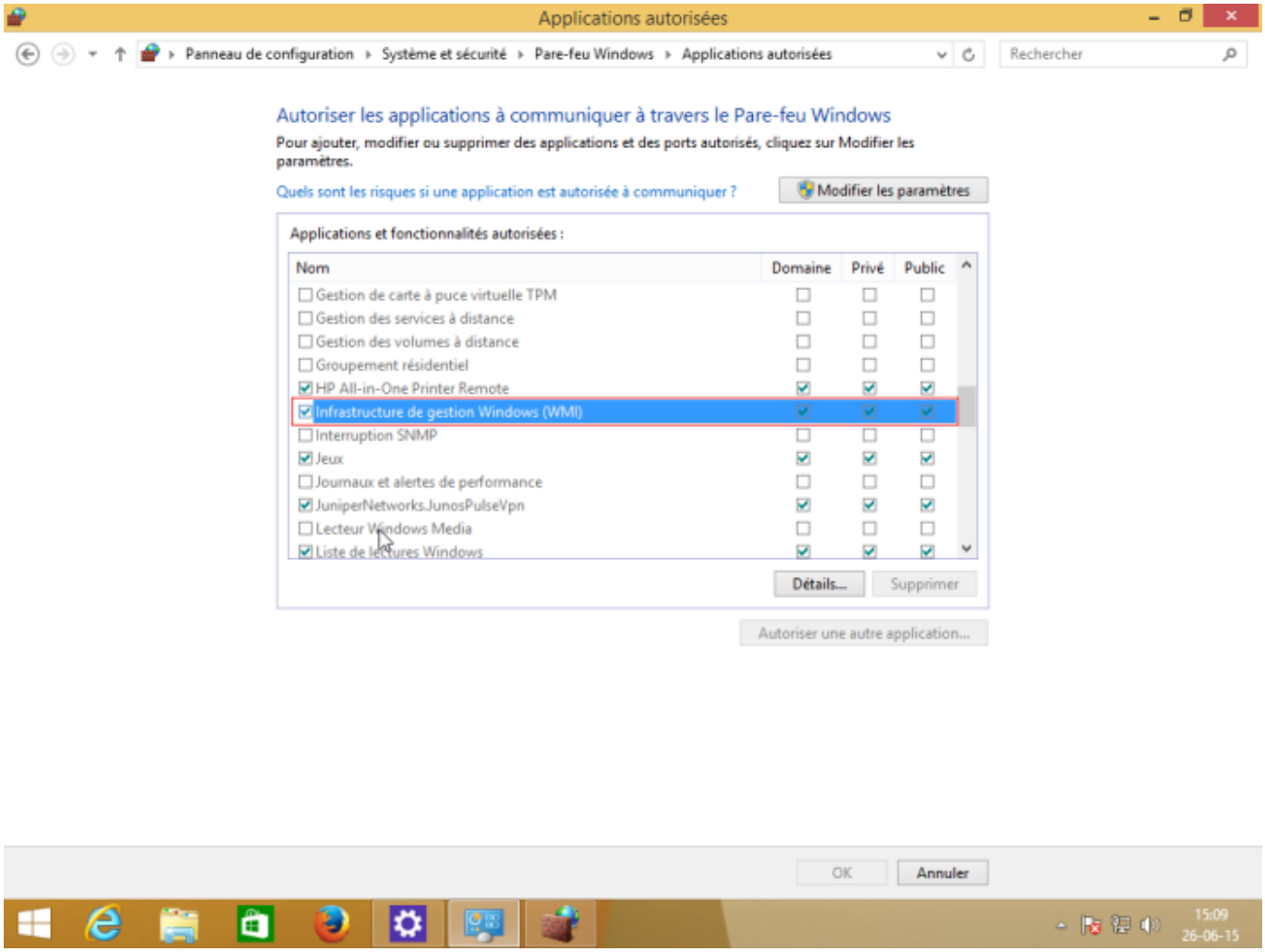


Make sure that the permissions have been applied to the selected namespace and its sub-namespaces by clicking on “Advanced” to check the “Applies to” column.



Allow access through the firewall (If you are using a firewall)

To prevent the firewall from blocking WMI requests, the easiest way is to run the following command line as Administrator: “netsh firewall set service RemoteAdmin enable” You can also do this via the Windows firewall configuration page:

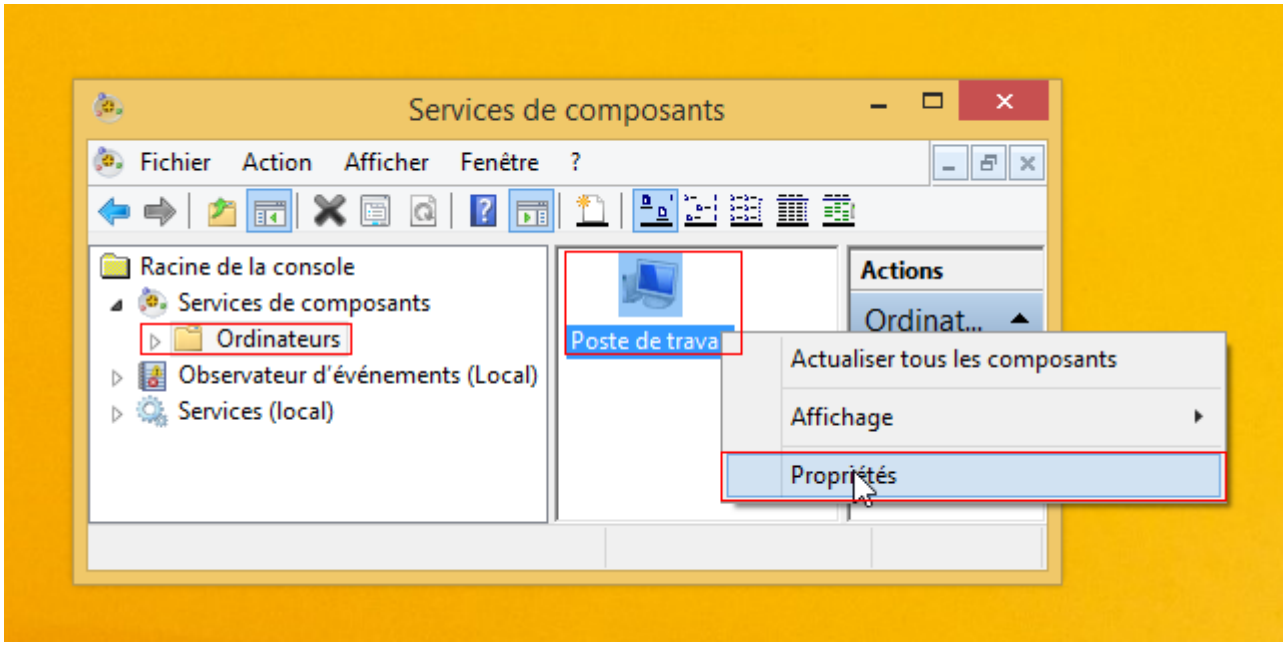


Add the user to a group with remote access permissions

To be able to access WMI remotely, WMI must be part of the “Administrator” group.

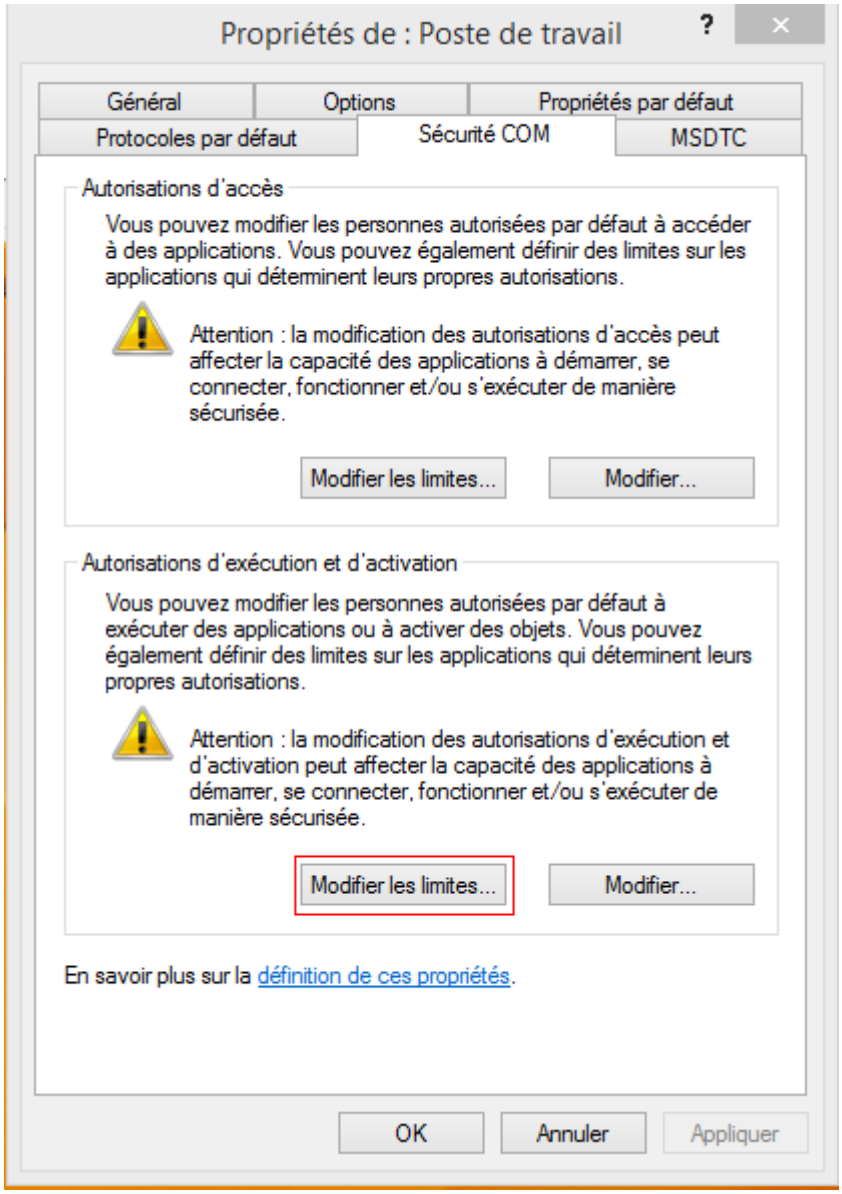
Enable DCOM access (if necessary)

Run the “dcomcnfg” application

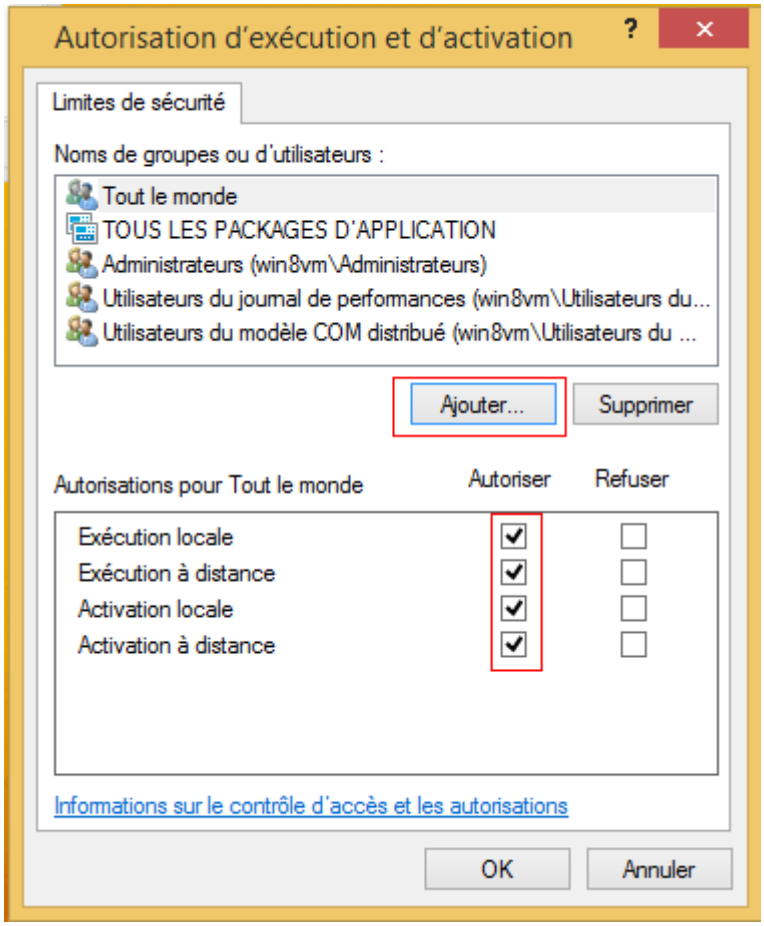


In the " **Console Root → Component Service → Computers** "right-click on "My Computer" and then click on "Properties".

Go to the "DCOM Security" tab and, in "Execution and Activation Permissions", click on the "Modify Limits" button.



Add the user for WMI to the list and activate the remote authorisations:



Note: If this doesn't work, always try the other “Modify limits” button and the other 2 buttons (“Modify”).

Performance group

If you get an unknown output of the type with a message containing “2 WMI samples%”. You need to add the user to the local “Performance Log” group if he/she is not the machine administrator.

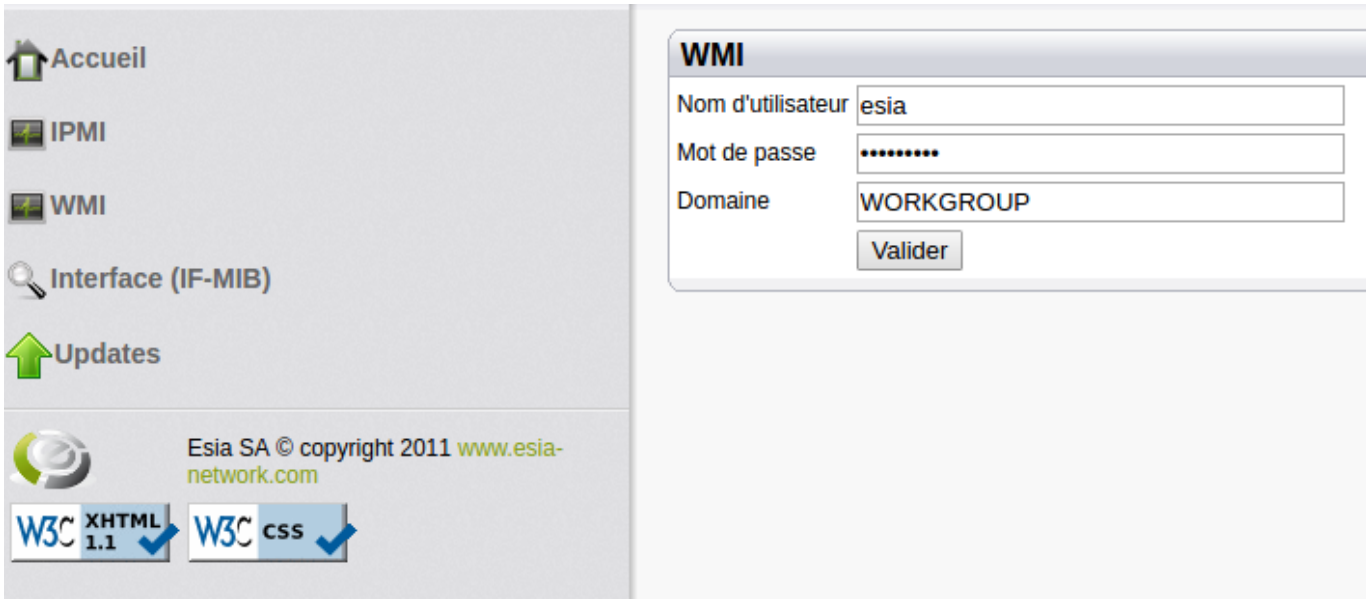
Fill in the WMI credentials on the ESIA Unity box.

Once all the above steps have been completed, all that remains is to enter the WMI credentials on the Unity box.

To do this, go to the web interface of the Unity box via its IP address and enter the credentials. (How to configure the IP of a Unity?).

- The default user name is : **esia**
- Password is : **gesa**

Next, go to the WMI tab. Here you can enter the user, password and domain to be used for WMI queries:



From:
https://wiki.esia-sa.com/ - **Esia Wiki**

Permanent link:
https://wiki.esia-sa.com/en/advanced/wmi_win_7_8

Last update: **2023/11/09 18:06**