



Purpose

This article will describe the necessary additional steps to follow to enable WMI support between the eControl host server and Windows 2008 servers hosting user home folders. WMI support is a mandatory requirement for creating user accounts with home folders in Active Directory using eControl create profiles.

Requirements for eControl Host Server

For eControl installed on a Windows 2008 server, ensure the following additional requirements are met:

- Windows Management Service is installed and started.
- The following **Web Server (IIS)** roles are installed:
 - Web Server > Security > Basic Authentication
 - Web Server > Security > Windows Authentication
 - Management Tools > IIS 6 Management Compatibility
- Windows Firewall is enabled for WMI (Windows Management Instrumentation).

Requirements for Home Folder Server

For Windows 2008 server that hosts user home folders (where eControl will create new AD user account home folders), ensure the following additional requirements are met:

- Windows Management Service is installed and started.
- Windows Firewall is enabled for WMI.
- Enable DCOM permissions for remote WMI requests for the local administrators group.
- Enable namespace and subnamespace privileges for the local administrators group.
- Disable remote User Account Control (UAC).

Steps to Enable WMI in Windows Firewall

You must allow WMI traffic through the firewall of the eControl host server and the home folder host server(s). The following procedure walks you through allowing WMI through the Windows Firewall.

To allow WMI traffic through the Windows Firewall:

1. Ensure that you are logged into the local server as an administrator account.
2. Navigate to **Start > Control Panel > Windows Firewall**.
3. Click **Allow a program through Windows Firewall**.



4. In the “Windows Firewall Settings” window, under the “Exceptions” tab, ensure that **Windows Management Instrumentation (WMI)** is checked, and click **OK** and close the “Windows Firewall” window.

Steps to Enable DCOM Permissions

You must enable DCOM permissions on the home folder host server(s):

1. Log on to the home folder host server with an administrator account.
2. Click **Start**, click **Run**, type **DCOMCNFG**, and then click **OK**.
3. Expand **Component Services**, expand **Computers**, and right-click **My Computer** and click **Properties**.
4. Select the **COM Security** tab. Under **Access Permissions** click **Edit Limits**.
5. Ensure the local ANONYMOUS LOGON account has `Local Access` and `Remote Access`, and then click **OK**.
6. Click **Edit Default**, and then ensure the local eControl service account user (or the Administrators group) has `Local Access` and `Remote Access`, and then click **OK**.
7. Under **Launch and Activation Permission**, click **Edit Limits**.
8. Ensure the local eControl service account user (or the Administrators group) has `Local Launch`, `Remote Launch`, `Local Activation`, and `Remote Activation`, and then click **OK**.
9. Click **Edit Default**, and then ensure the local eControl service account user (or the Administrators group) has `Local Launch`, `Remote Launch`, `Local Activation`, and `Remote Activation`.
10. Click **OK**.

Steps to Enable Account Privileges in WMI

The local eControl service account user on the Home Folder host server must possess security access to the namespace and subnamespaces of the monitored target computer. To enable these privileges, complete the following procedure.

To enable namespace and subnamespaces privileges:

1. Log on to the home folder host server with an administrator account.
2. Navigate to **Start > Administrative Tools > Computer Management**. Expand **Services and Applications**, right-click **WMI Control**, and select **Properties**.
3. Under the Security tab expand the **Root** folder and select the **CIMV2** folder.
4. Click **Security** and add the local eControl service account user account and the local Administrator’s group and ensure you grant the following permissions:
`Enable Account`
`Remote Enable`
5. Click **Advanced**, and then select the user account used to access this computer.

6. Click **Edit**, select `This namespace` and `subnamespaces` in the **Apply to** field, and then click **OK**.
7. Click **OK** on the Advanced Security Settings for CIMV2 window.
8. Click **OK** on the Security for Root\CIMV2 window.
9. Click **OK** on the WMI Control Properties window.
10. Click **Services** in the left navigation pane of Computer Management and restart the **Windows Management Instrumentation** Service.

Steps to Allow WMI through the Windows Firewall

You must allow WMI traffic through the firewall of the eControl Host Server and the Home Folder Host Server. The following procedure walks you through allowing WMI through the Windows Firewall.

To allow WMI traffic through the Windows Firewall:

1. Log on to the computer you want to monitor with an administrator account.
2. Navigate to **Start > Control Panel > Security Center**. You need to switch to the Classic View of the Control Panel to use this navigation path.
3. Click **Windows Firewall** in the left navigation pane.
4. Click **Allow a program through Windows Firewall** in the left navigation pane.
5. Check **Windows Management Instrumentation (WMI)**, and then click **OK**.

Steps to Disable Remote User Account Control (UAC)

Because WMI uses the local eControl service user account, you need to disable remote User Account Control (UAC).

Warning: The following procedure requires the modification or creation of a registry key. Changing the registry can have adverse effects on your computer and may result in an unbootable system. Consider backing up your registry before making these changes.

To disable remote UAC for a workgroup computer:

1. Log on to the computer you want to monitor with an administrator account.
2. Click **Start > Accessories > Command Prompt**.
3. Enter `regedit`.
4. Expand
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.
5. Locate or create a DWORD entry named `LocalAccountTokenFilterPolicy` and provide a DWORD value of 1.

Note: To re-enable remote UAC, change this value to 0.