

How to Configure Windows Event Forwarding (WEF)

Task. Configure WEF.

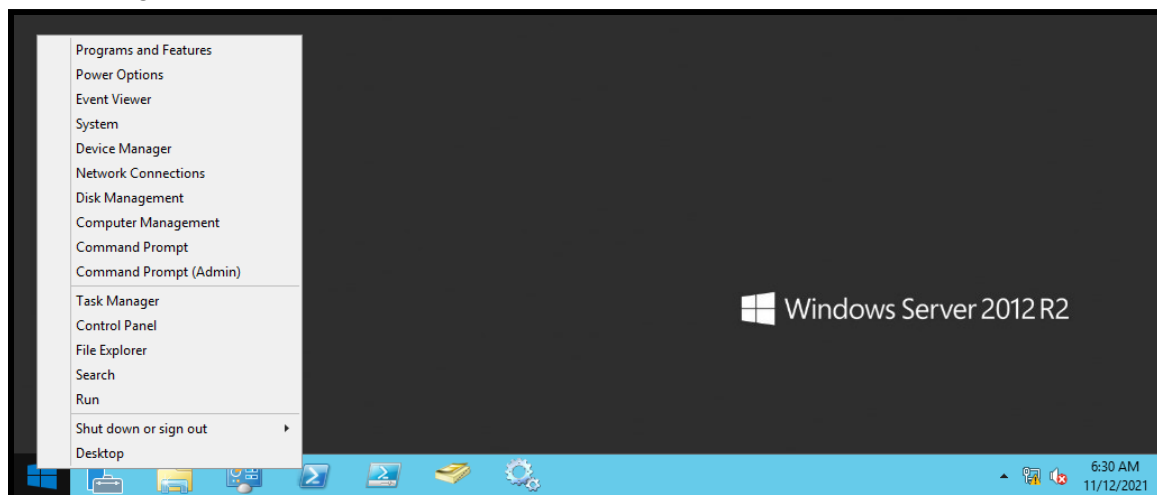
Purpose. WEF allows for Windows events (a.k.a “logs”) to be pushed/pulled to one or more Windows Event Collector (WEC) servers.

Conditions. You have domain administrator privileges and access to either a domain controller or a workstation with Remote Server Administration Tools (RSAT) installed.

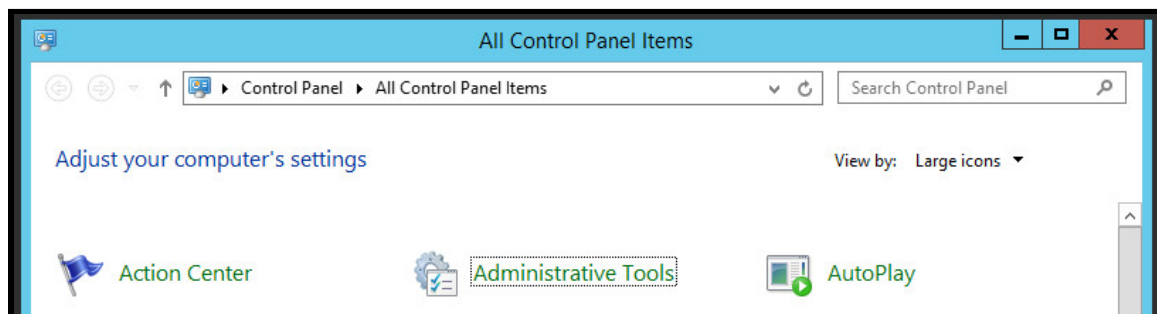
Standard. You were able to create a Group Policy Object (GPO) for WEF.

Step 1. Login to your domain administrator account on either a domain controller or a workstation with RSAT installed.

Step 2. Right-click on the Windows icon in the bottom-left corner and select “Control Panel.”

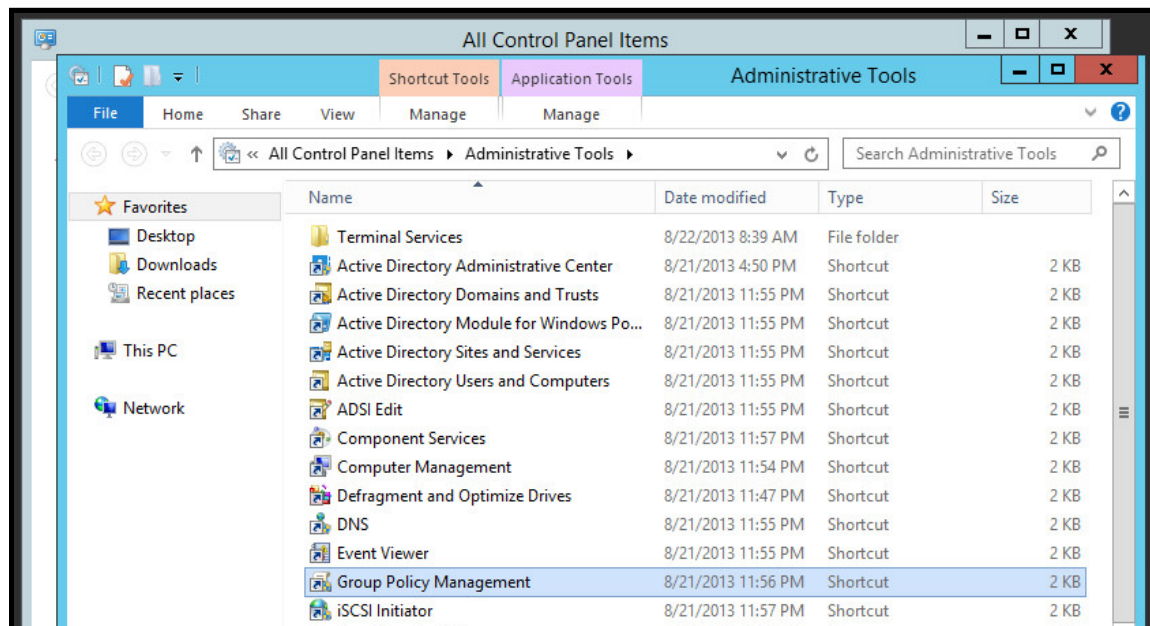


Step 3. Click-on “Administrative Tools.”

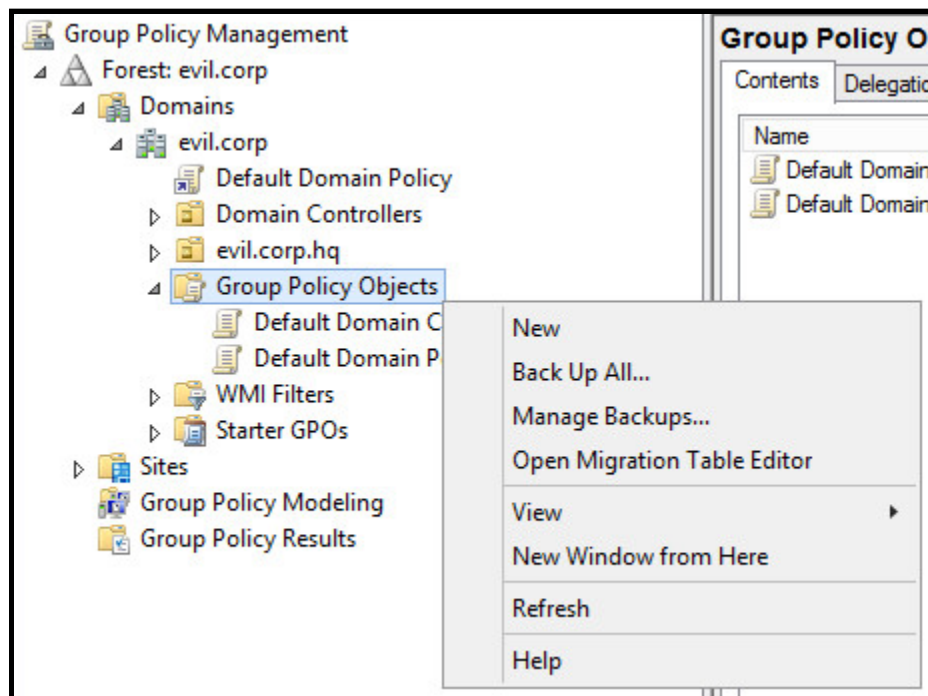


How to Configure Windows Event Forwarding (WEF)

Step 4. Double-click “Group Policy Management.”

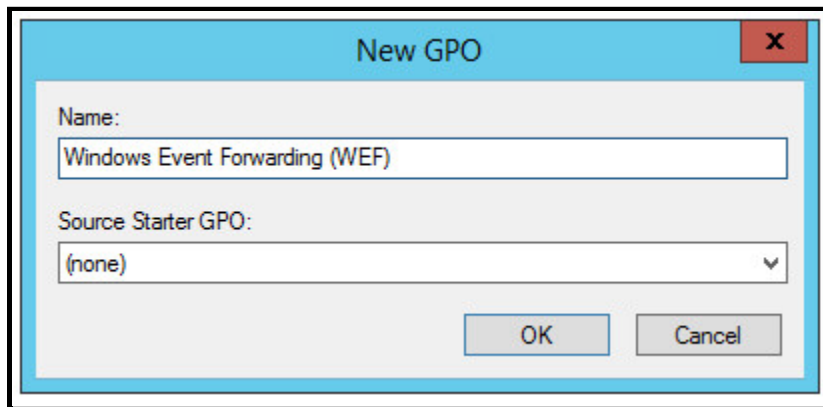


Step 5. Right-click the “Group Policy Objects” container and select “New.”

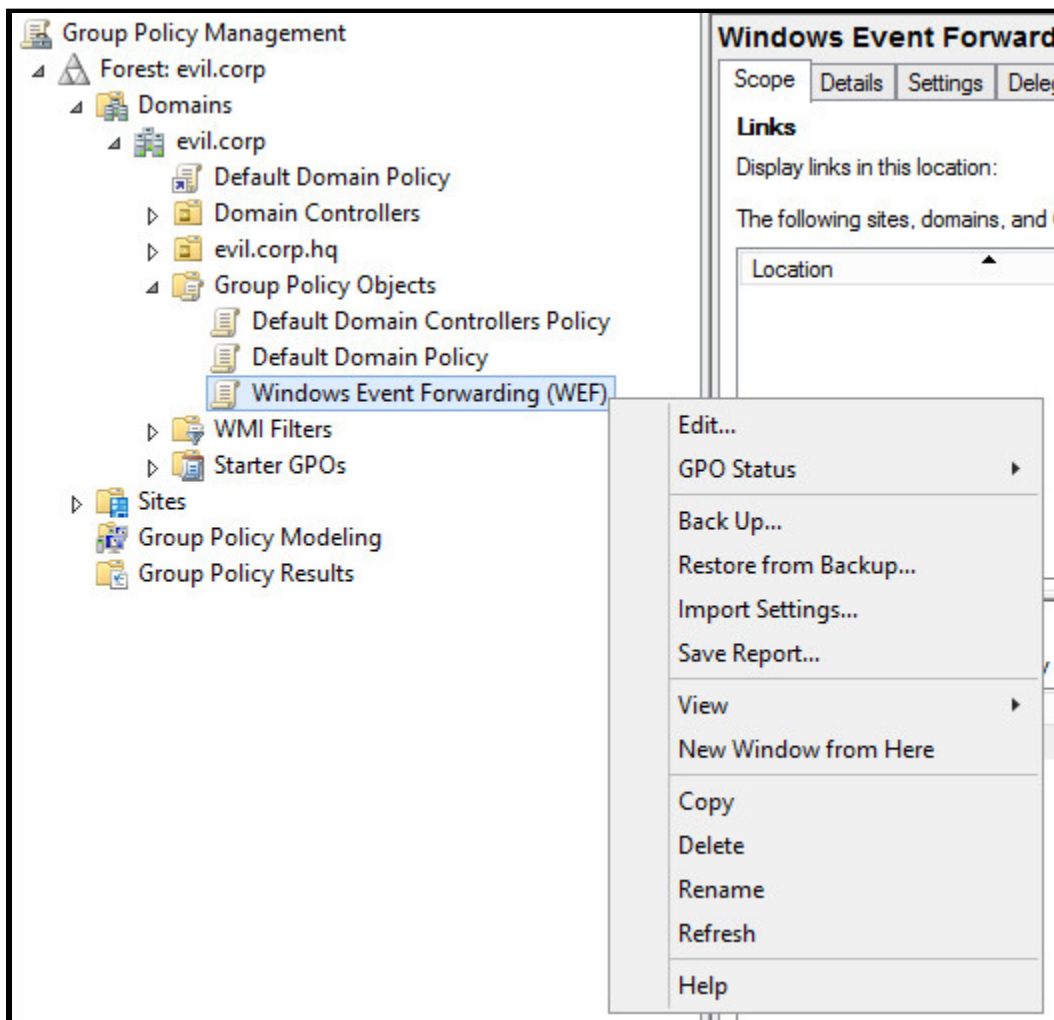


How to Configure Windows Event Forwarding (WEF)

Step 6. Type “Windows Event Forwarding (WEF)” in the “Name” field.

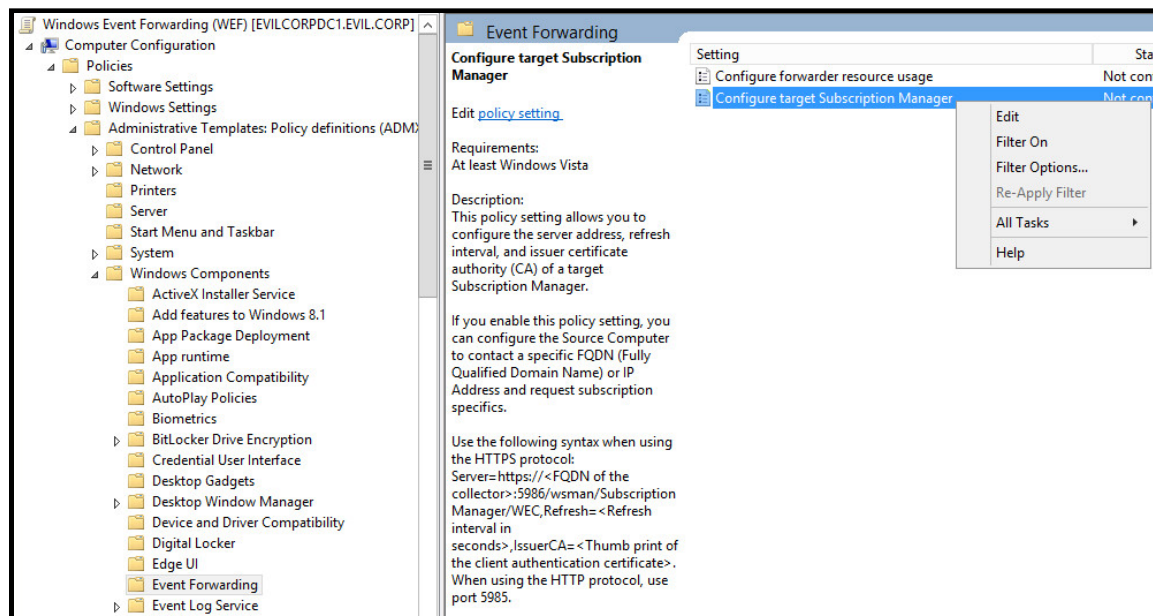


Step 7. Right-click the GPO you created and select “Edit.”

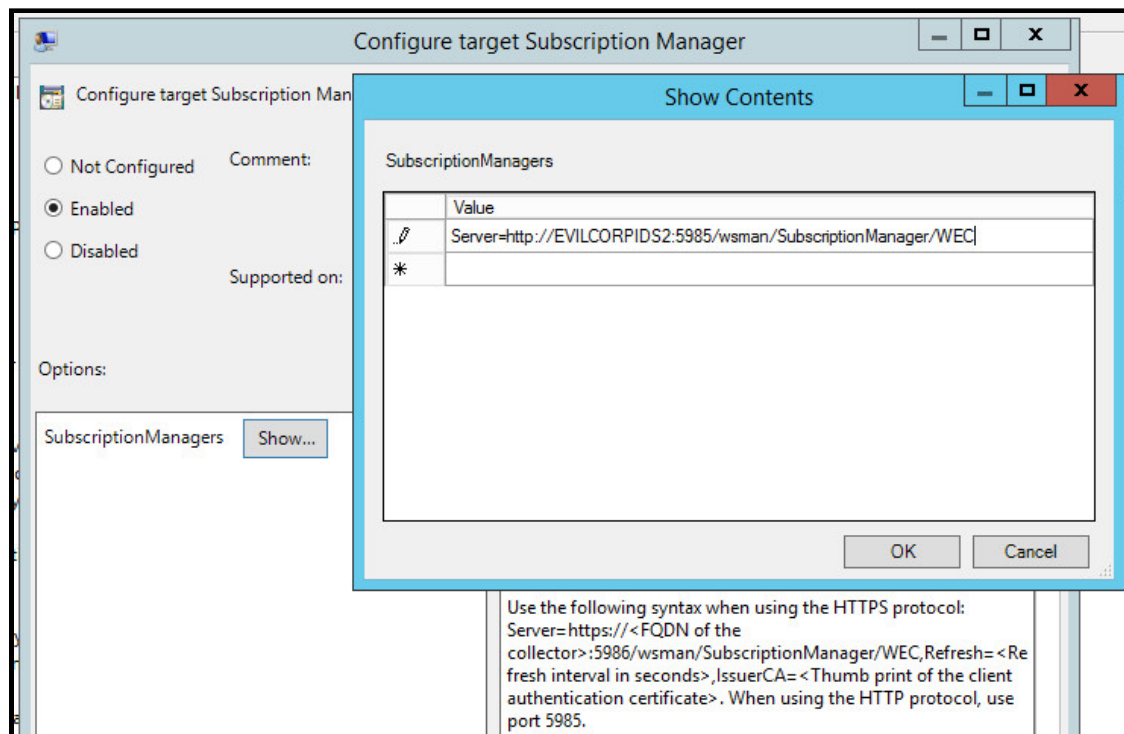


How to Configure Windows Event Forwarding (WEF)

Step 8. With the GPO open, navigate to the following path: “Computer Configuration” > “Policies” > “Administrative Templates” > “Windows Components” > “Event Forwarding.” Right-click “Configure target Subscription Manager” and select “Edit.”

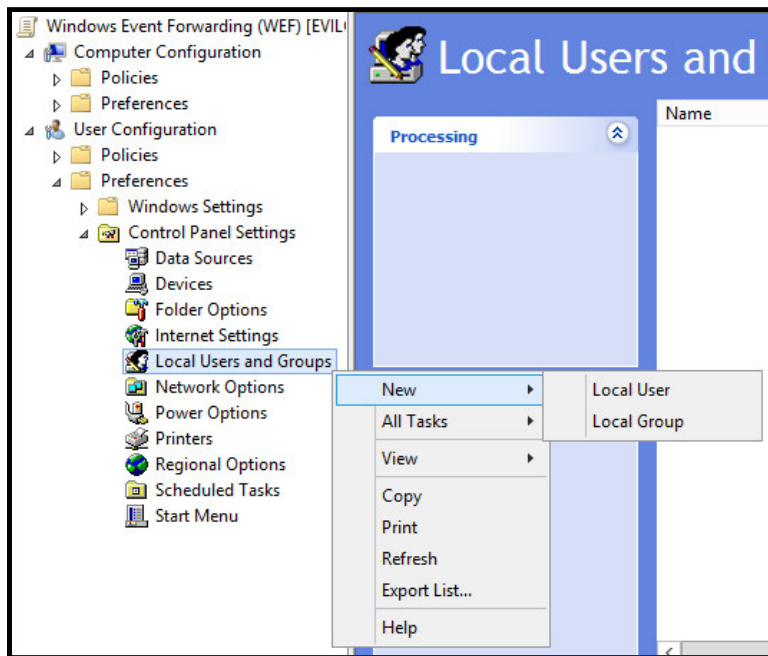


Step 9. Select “Enabled.” Click “Show...” and fill-in the SubscriptionManagers Value field using the correct syntax. For example, if the hostname of your WEC server is “EVILCORPIDS2,” you would type “http://EVILCORPIDS2:5985/wsman/SubscriptionManager/WEC.” Once complete, click “OK” to close the “Show Contents” window. Click “Apply” and “OK” to close the “Configure target Subscription Manager” window.

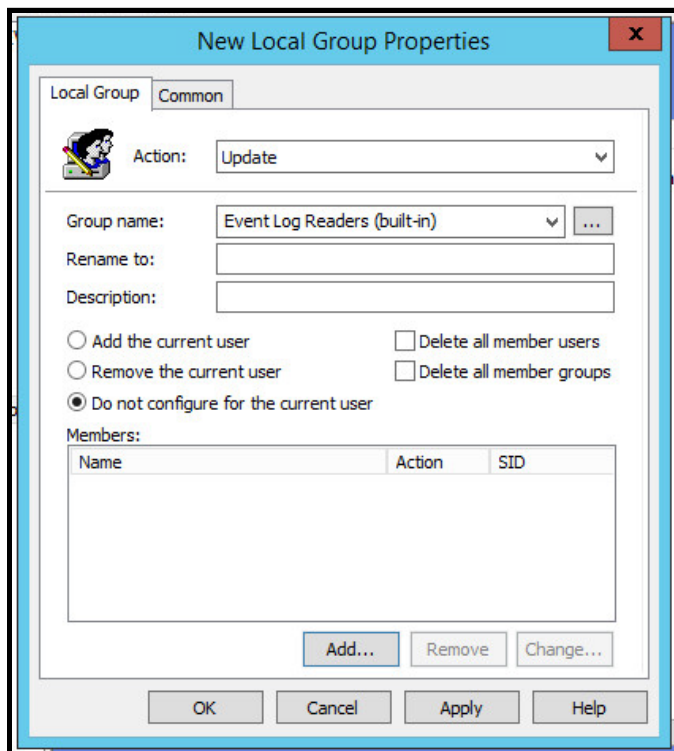


How to Configure Windows Event Forwarding (WEF)

Step 10. With the GPO still open, navigate to the following path: “User Configuration” > “Preferences” > “Control Panel Settings.” Right-click “Local Users and Groups.” Click “New” and select “Local Group.”

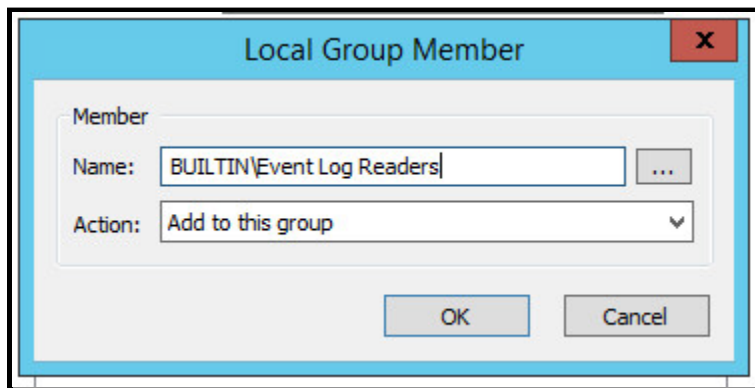


Step 11. Using the “Action” drop-down menu, select “Update.” Using the “Group name” drop-down menu, select “Event Log Readers (built-in).” In the “Members” section, click “Add.”

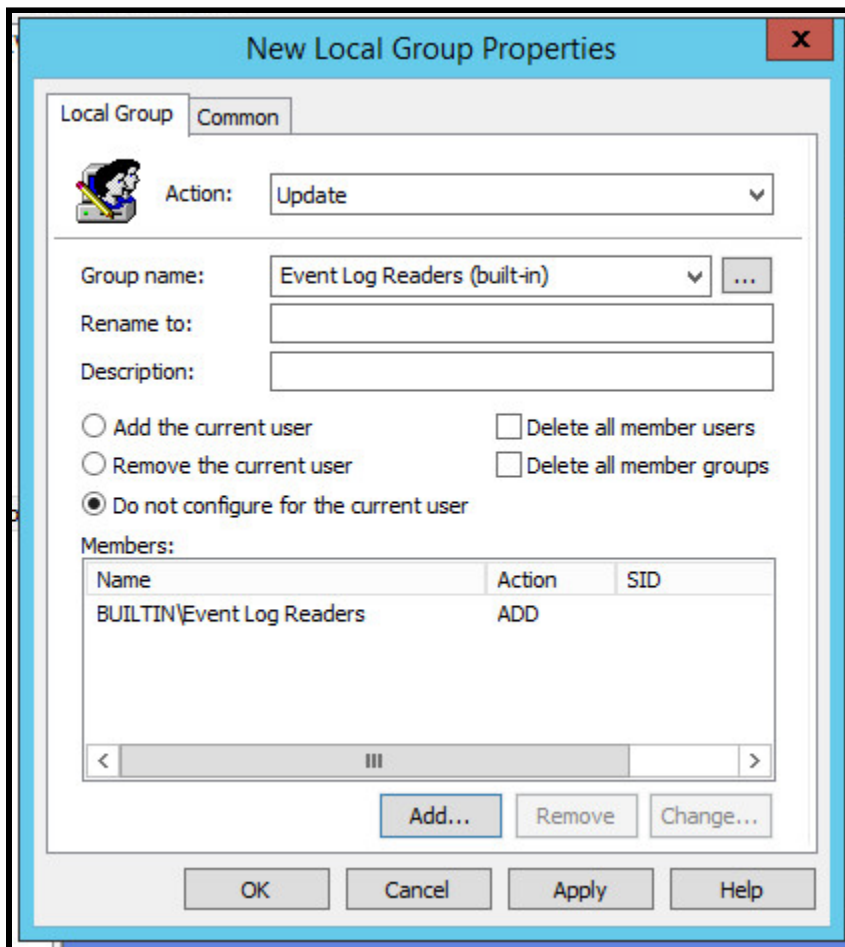


How to Configure Windows Event Forwarding (WEF)

Step 12. Type “BUILTIN\Event Log Readers” in the “Name” field and click “OK” to close the “Local Group Member” window.

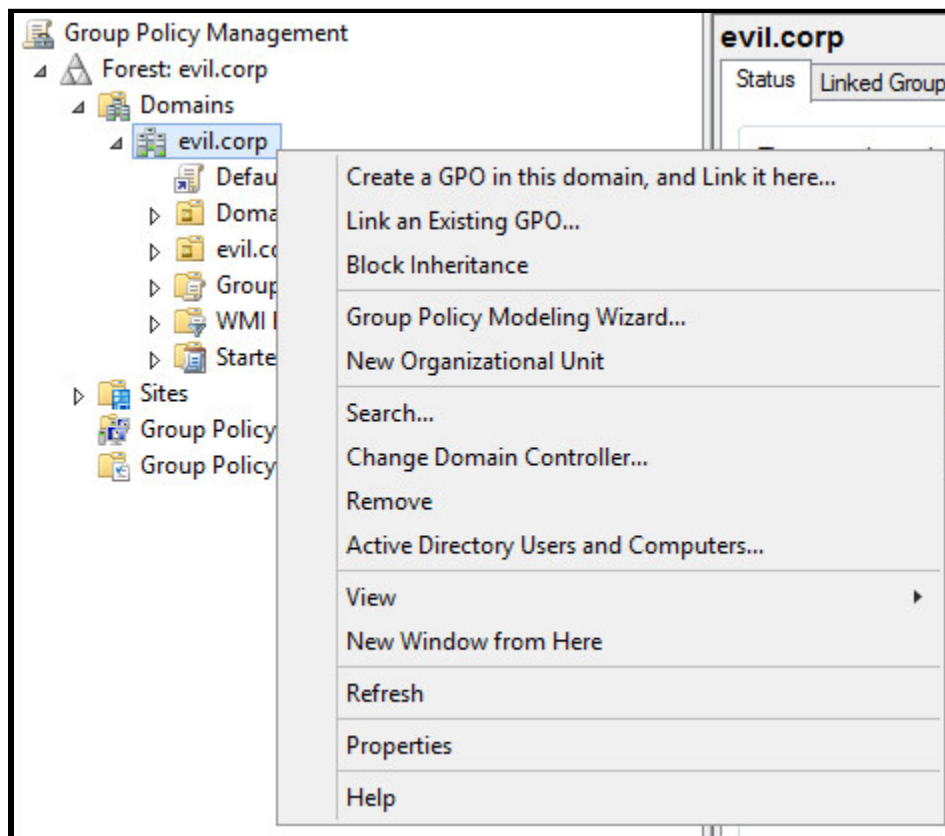


Step 13. Click “Apply” and click “OK.” Close the GPO.



How to Configure Windows Event Forwarding (WEF)

Step 12. Right-click on your domain and select “Link an Existing GPO...”



Step 13. Select the GPO you created and click-on “OK.”

