**Solution for Outlook security patches through GPO**

The security updates for Outlook released on September 12, 2017 are affecting the contentACCESS email archive. The users are no longer able to open the original archived messages from shortcuts, only the shortcut itself. This is caused by the Microsoft’s decision to disable Outlook form scripting by default.

After installing the security updates for Outlook, emails that were archived by third-party application are showing an unwanted behavior. All programs and applications using custom Outlook forms are affected.

More information: <http://tech-arrow.com/documentation/contentaccess-documentation-version-3-3/?section=solution-for-outlook-security-patches-v-3-3>

The Outlook form scripting is disabled by default but it can be enabled using registry keys as described in the section mentioned above. This document describes the solution for the Outlook security patches through GPO.

The solution consist of three steps:

1. Prepare the Distribution point
2. Create the group policy object and assign it to the affected machines
3. Check the changes
4. **Prepare the Distribution point**

To use the GPO for the solution, a distribution point has to be created on the publishing server:

* Log on to the server computer (Domain controller) as an administrator.
* Create a shared network folder which will contain the **CustomFormFix** folder that you want to distribute. Extract the CustomFormFix.zip to this folder.
* Set permissions on the shared folder to allow access to the distribution point (everyone should have at least read access).
* In this demo case the distribution group path is \\SharedFolder.

***Note:*** Do not use special characters in setup names or be careful of long UNC paths.

1. **Create the group policy object and assign it to the affected machines**

To apply the solution, a new group policy object should be created and the CustomFormsFix.ps1 PowerShell script should be set in the GPO.

* On the domain controller start the group policy management.
* In your domain create a new group policy object.
* Link the newly created GPO object to your domain.

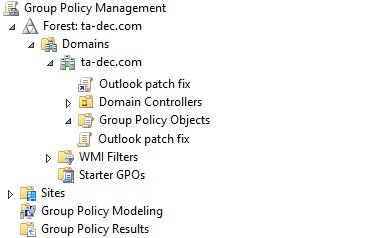


Figure 1 The created GPO object "Outlook patch fix" is linked to the ta-dec.com domain

* Set the Security filtering for the required computers (in our case we chose the Domain computers group).
* Right click and choose Edit on the new GPO.
* Choose the Compute configuration -> Windows Settings -> Scripts -> Startup option.
* In the Startup properties windows choose the PowerShell Scripts tab.

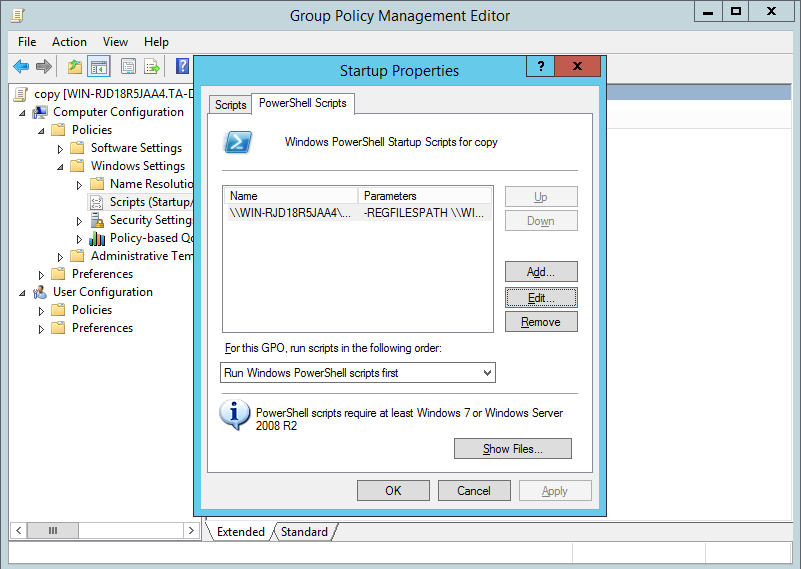


Figure 1 The GPO for Computer Startup configuration window

* Click on the Add button and create a new configuration.   
  The script name in our case is: **\\ShareFolder\CustomFormFix\CustomFormFix.ps1** (the shared path of the extracted PowerShell script) and the Script Parameters is **-REGFILESPATH \\ShareFolder\CustomFormFix** (the –REGFILESPATH parameter plus the shared path of the earlier created CustomFormFix folder)

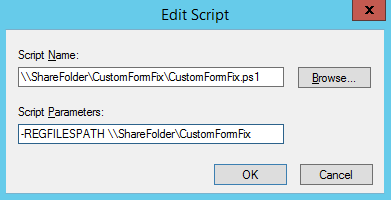


Figure 2 The configuration for the GPO

1. **Check the changes**

To check if our configuration and GPO deployment was successful, it’s necessary to restart a client machine, which was set in the **Security filtering**.

* + Open the Registry Editor (regedit.exe)
  + Find the path  
    HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\ or the path HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\  
    and open the Outlook KEY, which is created by your office version, for example:  
    HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Office\15.0\Outlook
  + There should be two new keys in this folder: Forms and Security

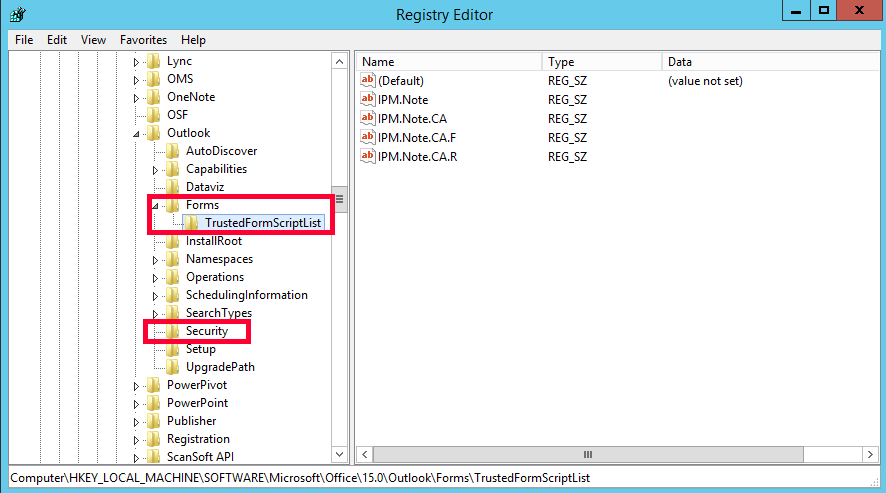


Figure 3 The deployed registry changes