

Installing Rmail Outlook-AddIn in Terminal Server Environment

Introduction

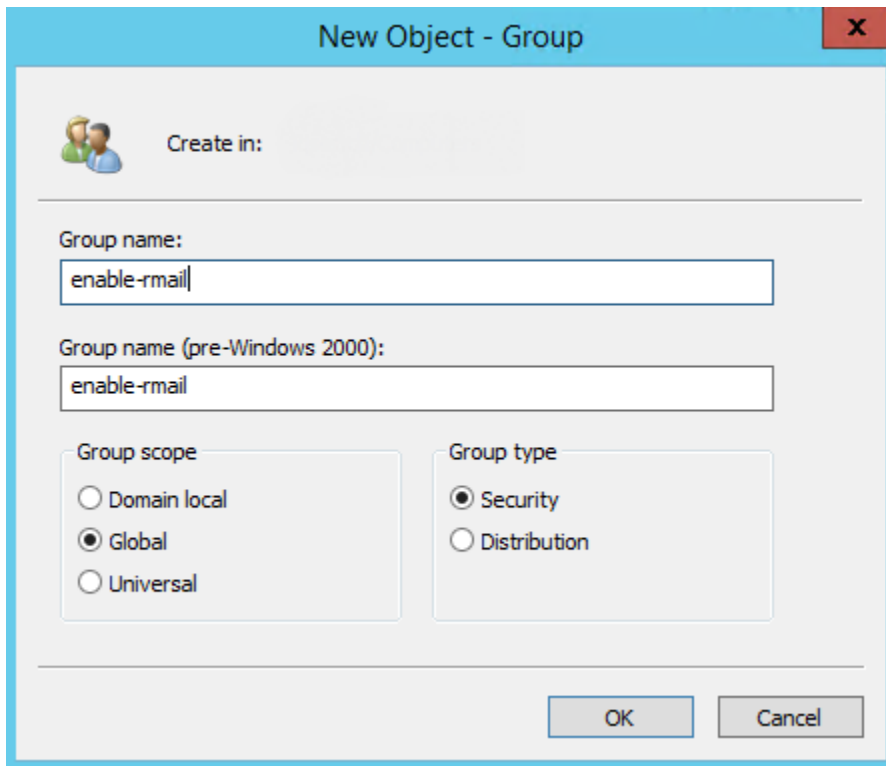
RMail is providing an Outlook-AddIn to be used with its services. In a Terminal Server Environment, the AddIn will eventually be installed on a server where both kind of users are login in, users needing the AddIn and users which should not be bothered by the AddIn.

The AddIn does not support this scenario itself, but by utilizing the Active Directory and Group Policy Objects this can be implemented easily.

Preparation

Active Directory Security Group

Create an Active Directory Security Group for users that should be able to use the AddIn. In our Example the Security Group is called "enable-rmail".

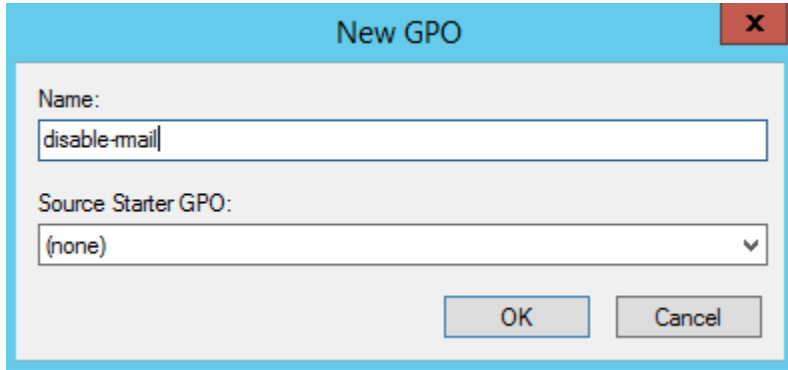


The screenshot shows a Windows dialog box titled "New Object - Group". It has a light blue header bar with a red "X" button in the top right corner. Below the header, there is a "Create in:" label with a group icon. The main area contains two text input fields: "Group name:" and "Group name (pre-Windows 2000):", both containing the text "enable-rmail". Below these fields are two sections: "Group scope" and "Group type". In the "Group scope" section, three radio buttons are present: "Domain local", "Global" (which is selected), and "Universal". In the "Group type" section, two radio buttons are present: "Security" (which is selected) and "Distribution". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Add corresponding user objects or other security groups as members.

Group Policy Object “disable-rmail”

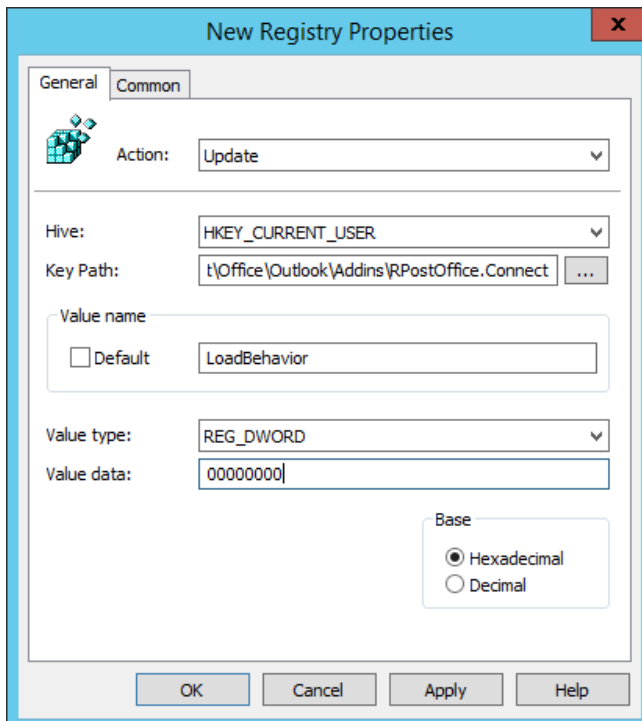
Launch the Group Policy Editor and create a new Group Policy Object. We will call the policy “disable-rmail” in our example.



Edit the group policy, navigate to “User Configuration \ Preferences \ Windows Settings \ Registry”. Add a new Registry Item with following properties:

General

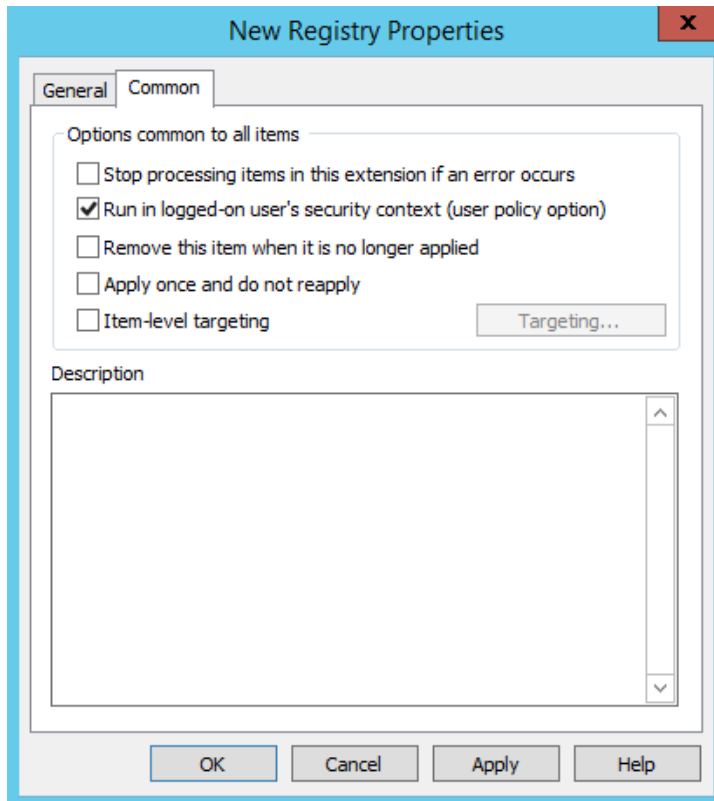
Action: Update
 Hive: HKEY_CURRENT_USER
 Key Path: SOFTWARE\Microsoft\Office\Outlook\Addins\RPostOffice.Connect
 Value name: LoadBehavior
 Value type: REG_DWORD
 Value data: 00000000
 Basis: Hexadecimal



Common

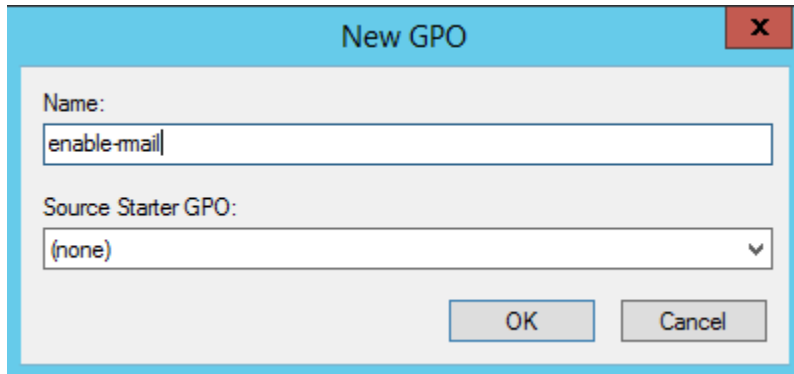
Options common to all items:

[x] Run in logged-on user's security context (user policy option)



Group Policy Object “enable-rmail”

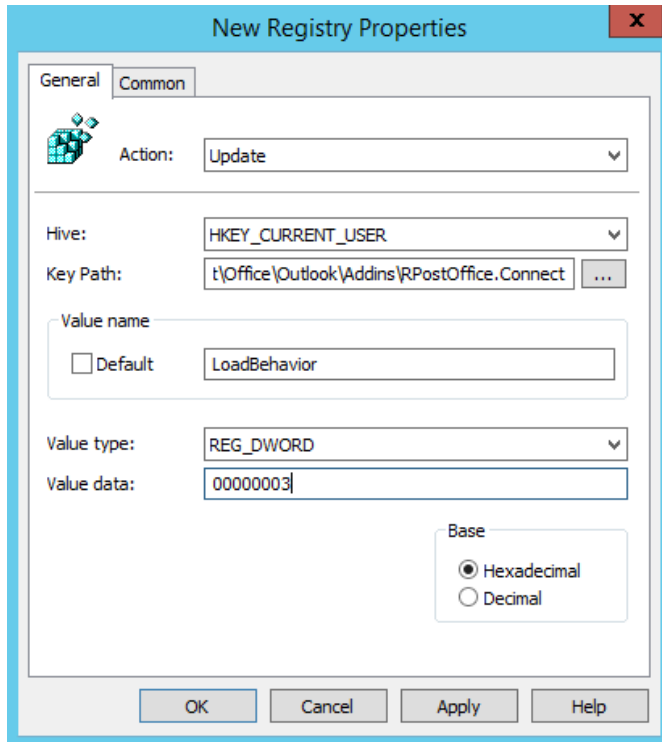
Launch the Group Policy Editor and create a new Group Policy Object. We will call the policy “enable-rmail” in our example.



Edit the group policy, navigate to “User Configuration \ Preferences \ Windows Settings \ Registry”. Add a new Registry Item with following properties:

General

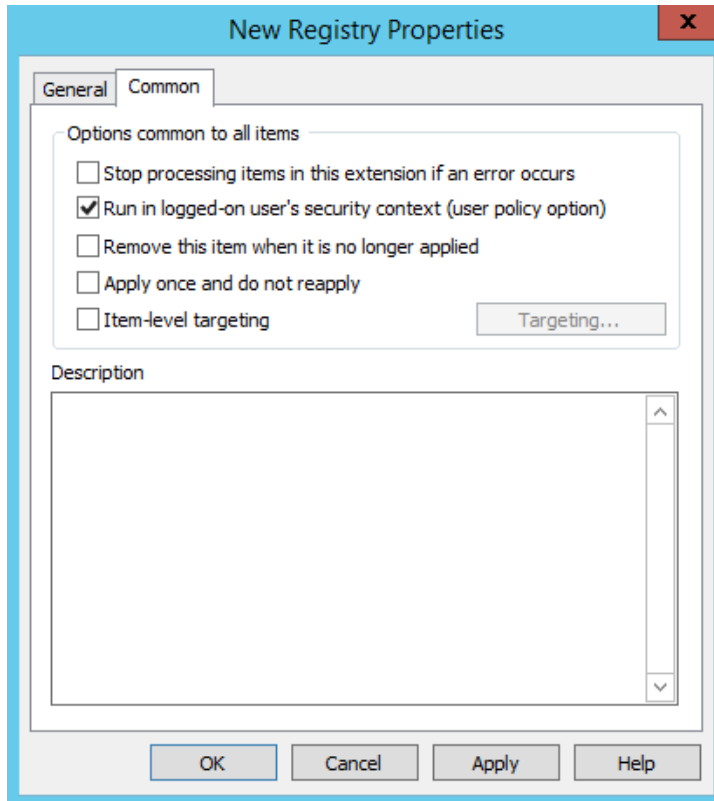
Action: Update
 Hive: HKEY_CURRENT_USER
 Key Path: SOFTWARE\Microsoft\Office\Outlook\Addins\RPostOffice.Connect
 Value name: LoadBehavior
 Value type: REG_DWORD
 Value data: 00000003
 Basis: Hexadecimal



Common

Options common to all items:

[x] Run in logged-on user's security context (user policy option)



Security Filtering / Delegation

You have now two Group Policy objects, “disable-rmail” and “enable-rmail”.

For the Group Policy “disable-rmail” leave the Security Filtering to defaults. It should look similar to this:

disable-rmail

Scope Details Settings Delegation Status

Links


Display links in this location:

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
< III >			

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name	
 Authenticated Users	▲

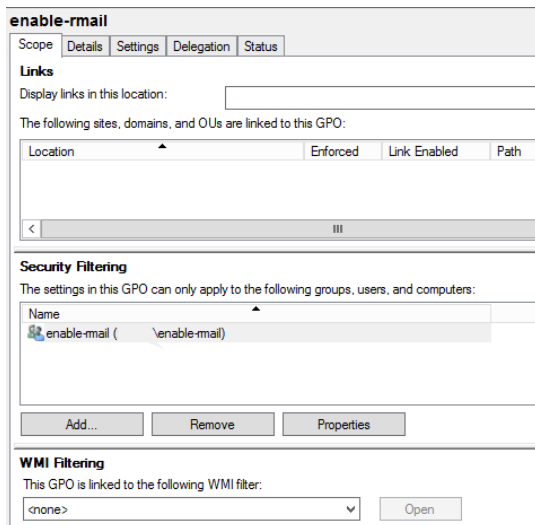
WMI Filtering

This GPO is linked to the following WMI filter:

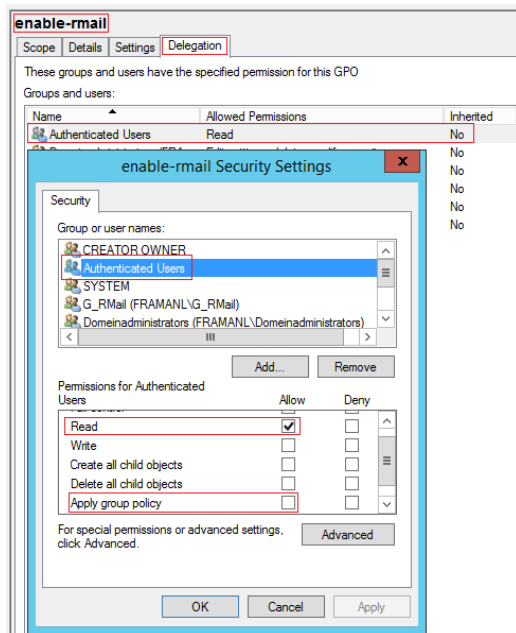
<none>

This way, the “disable-rmail” Policy will be applied to all Authenticated Users.

Now we need to adjust the Group Policy “enable-rmail”. We will limit the Security Filtering of this Policy to the Security Group “enable-rmail”. It should look similar to this:



Attention: Since Security Update MS16-072 (released June 2016) the Security Group “Authenticated Users” have to be manually assigned “Read” Privileges under Delegation if the Security Filtering was changed. Otherwise, the GPO will fail to apply.

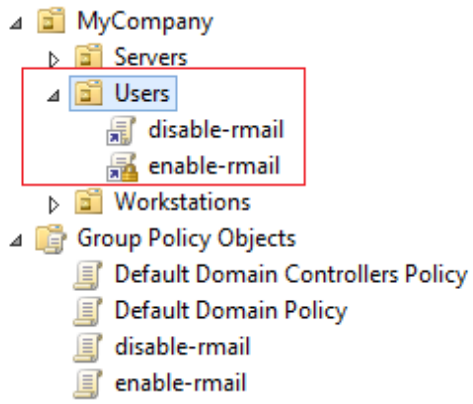


<https://support.microsoft.com/en-us/help/3163622/ms16-072-security-update-for-group-policy-june-14,-2016>

If this is done, for Users in the Security Group “enable-rmail”, both Policies will be applied. To ensure Rmail-Users are getting the correct policy applied, the GPO “enable-rmail” has to be enforced. If two policies contain the same settings, the enforced one will have precedence.

Linking GPOs

The last step is to link the newly created Group Policy Objects to the Organizational Unit(s), where the users reside:



Installing Rmail AddIn

If you have prepared the Active Directory Security Groups and the Group Policy Objects, you can proceed with installing the AddIn.

Before you start with the Installation make sure all Users are logged off.

During the Installation, make sure you select "Everyone" when asked for whom the AddIn should be installed:

