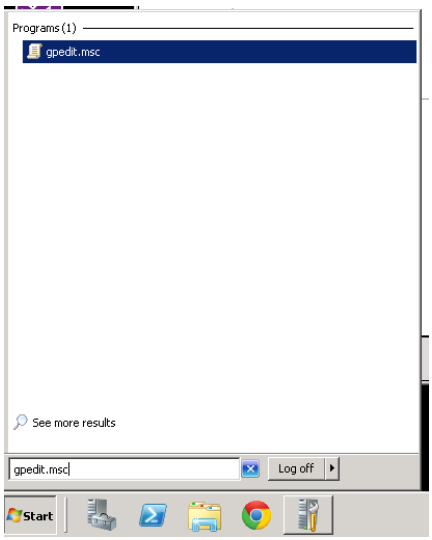
RDP-Guard

Needed Settings for WIN Server 2008 R2 /WIN7/8

Define the security level for RDP - Connections:

First of all, we need to define the security level of the rdp protocol. This setting has the effect, that NOT TS/SSL – protocol will be used. If you use the TS/SSL, actually the IP-addresses of the clients don't will be submitted in the windows logs.

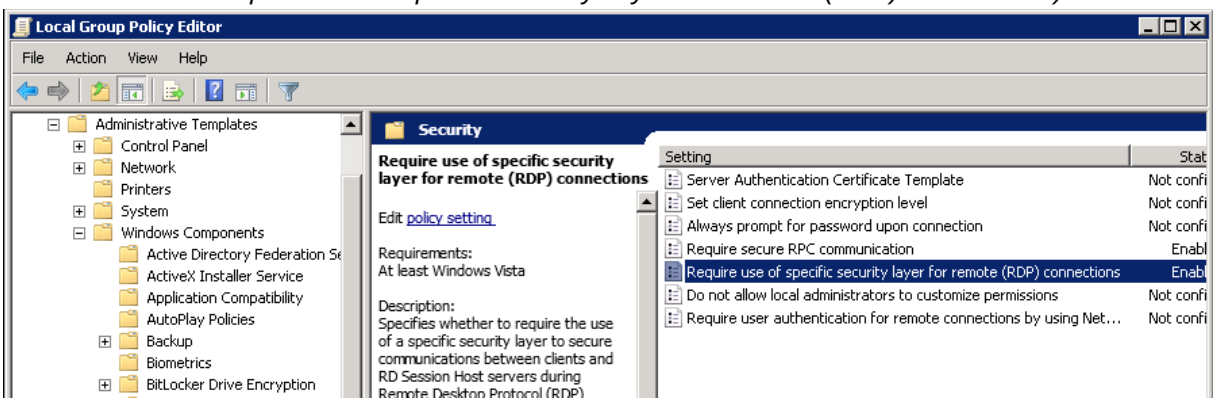
1. Open the local group policy editor by entering *gpedit.msc* in the search box:



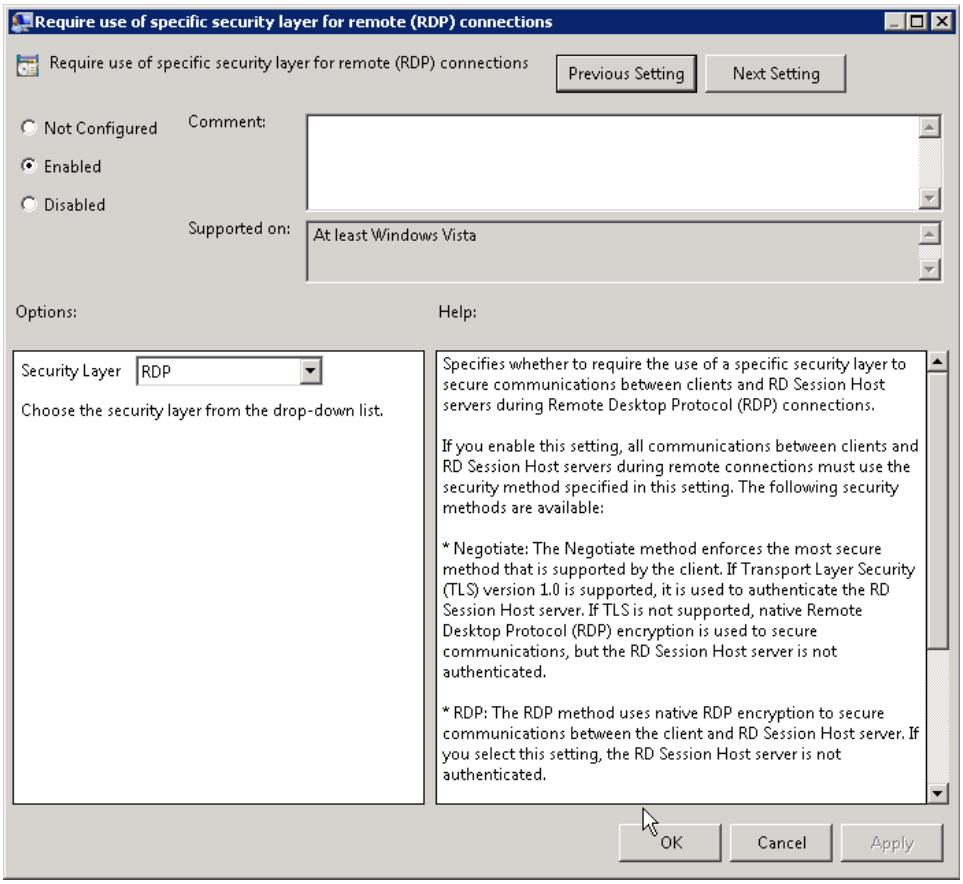
2. Please navigate in the TreeView on the left side to:

   Computer Configuration -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security

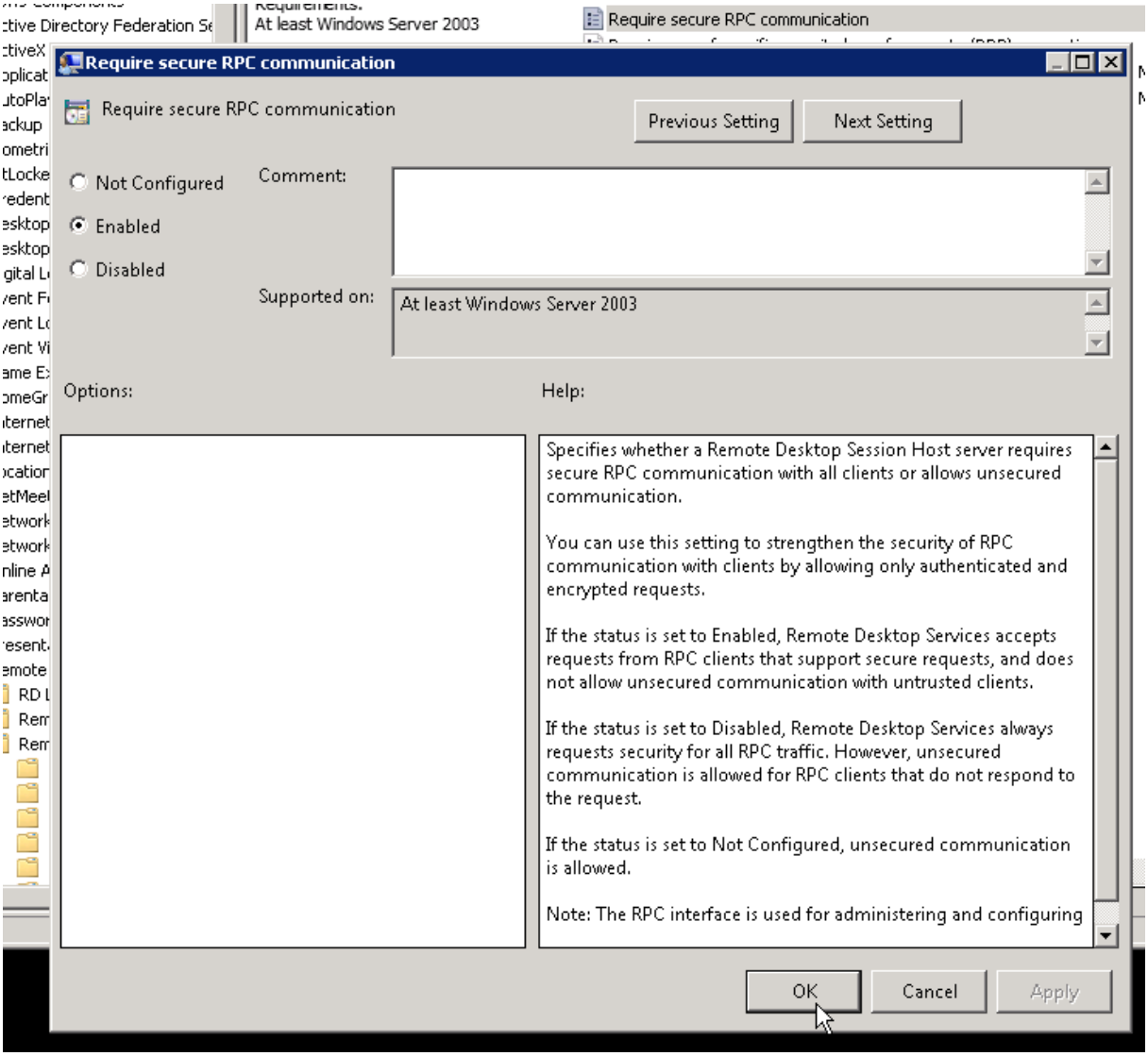
3. Double click on "*Require Use Of Specific Security Layer For Remote (RDP) Connections)*"



4. Enable this policy and press “OK”:



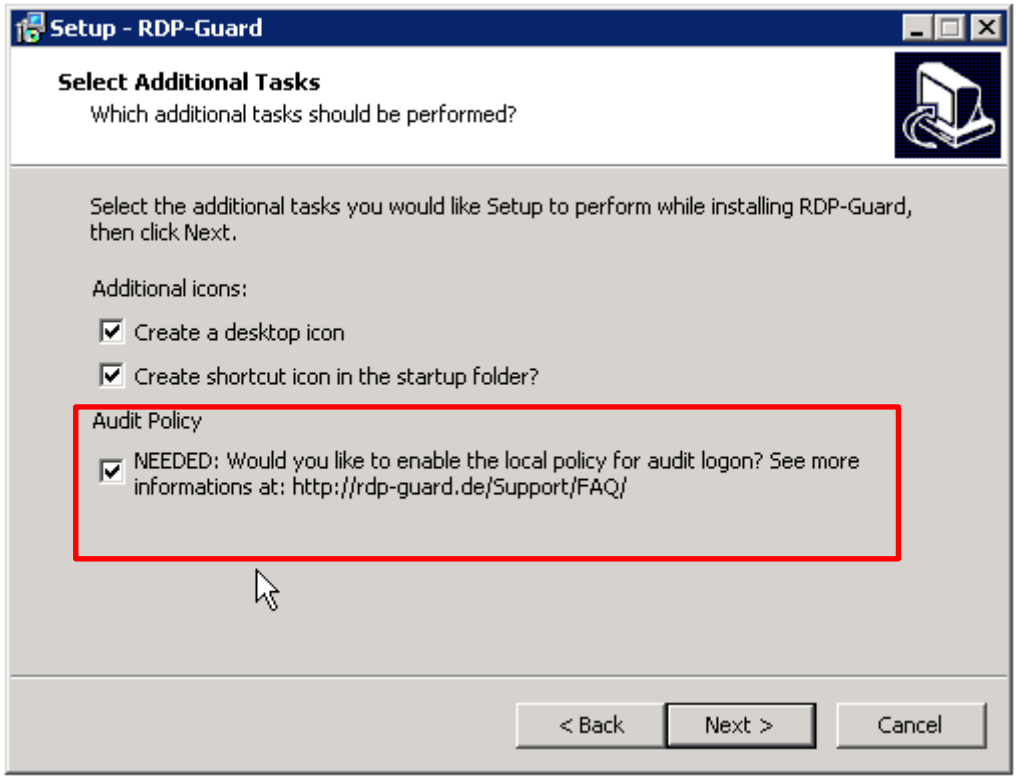
5. Double click on “*Require secure RPC communication*” to allow only secure connections (which makes your server more safe) and enable this policy:



Setup Audit Logon Policy

To detect attacks, it is necessary, that Windows logs all failed logon attempts in the windows event log. If you have already setup your server (or you defined it in the domain policies, etc) to log all failed login attempts, this step is not needed.

In the process of installation you will find this mask:

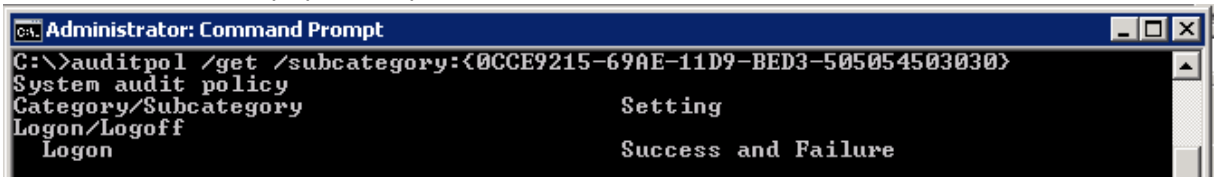


If you have enabled this option, the RDP-Guard is going to setup your system automatically.

You can check if the local audit logon policy is enabled, if you type in

auditpol /get /subcategory:{0CCE9215-69AE-11D9-BED3-505054503030}

in the Command Prompt (cmd.exe):



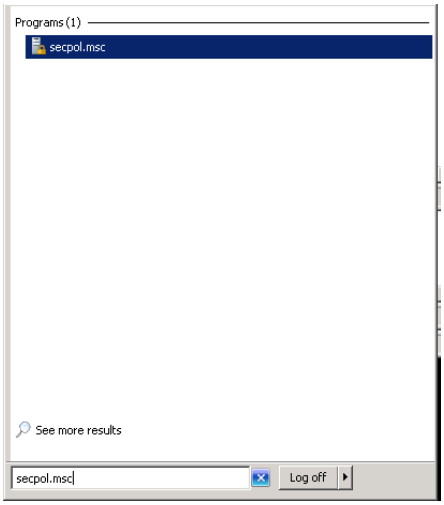
Setup the local audit logon policy manually:

If you want to enable the audit logon policy manually, type in the Command Prompt this command, please:

auditpol /set /subcategory:{0CCE9215-69AE-11D9-BED3-505054503030} /success:enable /failure:enable

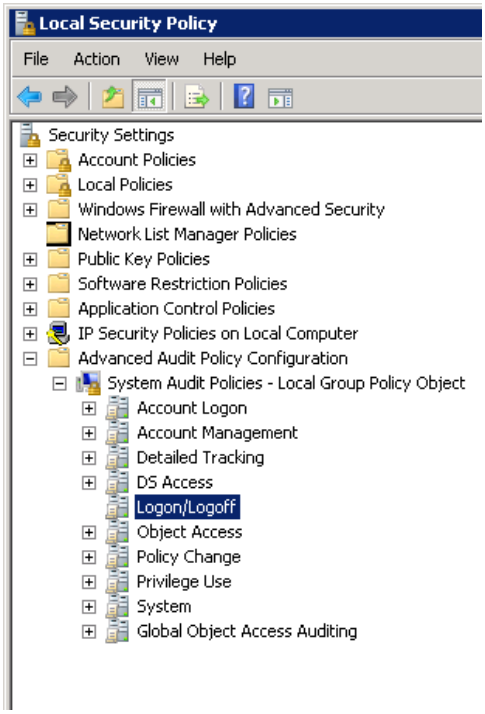
If no event logs generated by failed login attempts do the following steps:

1. Type in “*secpol.msc*” in the search box:

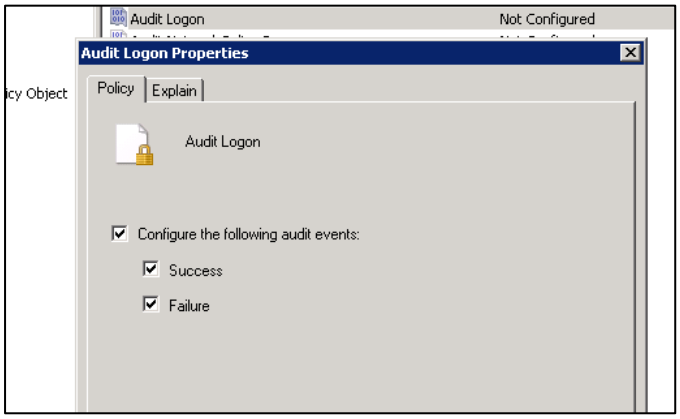


2. Please navigate in the TreeView on the left side to:

   Security Settings -> Advanced Audit Policies – Local Group Policy Object -> Logon / Logoff:



3. Double click “*Audit Logon*” on the right side and enable the checkboxes
   a. “Configure the following audit events”
   b. “Success”
   c. “Failure”



4. You have the option, if you use, the default policy settings or the advanced policy settings. You can use the default policy settings (Security Settings -> Local Policies -> Audit Policy) if your operating system, doesn't support the Advanced Audit Policies. But if the advanced policies are supported, we need to define, that only the advanced policies are relevant.

   Go to: Security Settings –> Local Policies -> Security Options

   Open the policy:

   Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings

   …and enable it: