MonitorPack solutions

TECK SYSTEM SOFT

Prerequisites for MonitorPack

Introduction

This document is an installation guide "step by step" to the attention of IT managers and administrators.
The support team development & TECK SYSTEM SOFT provide all materials needed for installation & monitoring MonitorPack Solutions.

MonitorPack Solution

No agent to deploy, which saves transition cost and bring you the expected IT efficiency.
To complete the configuration, a Windows process takes about five minutes is necessary to ensure security.

This procedure is to allow a single time from a single machine the MonitorPack applications and only from this machine for all Windows domain to monitor and inventory, this guarantees the security of the entire Active Directory forest. If you install plural MontorPack Guard licenses for example in each AD site you will have to allow all IPs

1 - Create Windows service account for MonitorPack

Why

As Microsoft regular security process, MonitorPack Windows's service named "MonitorPack Engine" needs to use a Windows account which has proper access rights on each remote servers and workstations you are going to monitor.

What

We recommend to create a service account named "svc_monitorpack" in your Active Directory Forest and embed it in Forest Active Directory Built-in group "administrators". This account will be available directly on all machines in the forest as the built-in group is by default local administrator on all servers and workstations in the AD forest.

Where

In the Active Directory Users and Computers MMC (dsa.msc)

When

Only once if you are in an Active Directory forest.

How

In Active Directory, create a dedicated service account for monitoring and inventorying your infrastructure as "svc_monitorpack".

Embed svc_monitorpack account in the built-in group "administrators" in your Active Directory forest.

2 - Link service account to MonitorPack Windows service

Why

MonitorPack Engine Windows's service is used by the MonitorPack Guard application to execute measures requests to local or remote computers.

Where

On MonitorPack workstation or server where MonitorPack Guard is installed (will not impact anything in Active Directory as the solution is agentless).

How

1. On MonitorPack workstation or server, run services.msc
2. In the right tab double click on "MonitorPack Engine" Service
3. Select Log On tab.
4. Click on Browse button and select "svc_monitorpack" account that has administrator's rights on all servers and workstations you are going to monitor.
5. Start Windows services for MonitorPack "MonitorPack Engine" and "MonitorPack Control". When you install MonitorPack Guard the windows service "MonitorPack Engine" is not running by default.

3 - Data Execution Prevention

What

Since Windows server 2003 SP1, Data Execution Prevention (DEP) is a security feature that helps prevent damage from viruses and other security threats by monitoring your programs to make sure they use system memory safely. It also blocks any non-Microsoft product to run by default on your servers.

Why

To allow MonitorPack executables to run locally.

When

When you install a new MonitorPack Guard or MonitorPack Asset on a server or Workstation.

Where

On server or workstation where MonitorPack Guard or MonitorPack Asset is going to be installed.

How

1. Go to Start > Control Panel.
2. Click System Security.
3. Click Advanced System Settings. The System Properties dialog box appears.
4. Click the “Advanced tab”.
5. Click the Settings button. The Performance Options dialog box appears.
6. Click the Data Execution Prevention tab.

   Add this executables to the exception list:

   MonitorPack Guard
   - MonitorPackGuard.exe
   - MonitorPackEngine.exe
   - MonitorPackControl.exe

   MonitorPack Asset
   - MonitorPackAsset.exe

Note: If you hardware does not Support DEP you may not have this tab on the Performance Options dialog box. You can cancel out of the procedure now and proceed with the installation instructions.

7. Ensure the Turn on DEP for essential Windows programs and services only button is selected.
8. Click OK twice.

4 - Setting Firewall Rules

Firewall rule must allow traffic of RPC, Performance Monitoring, Named Pipes and WMI.

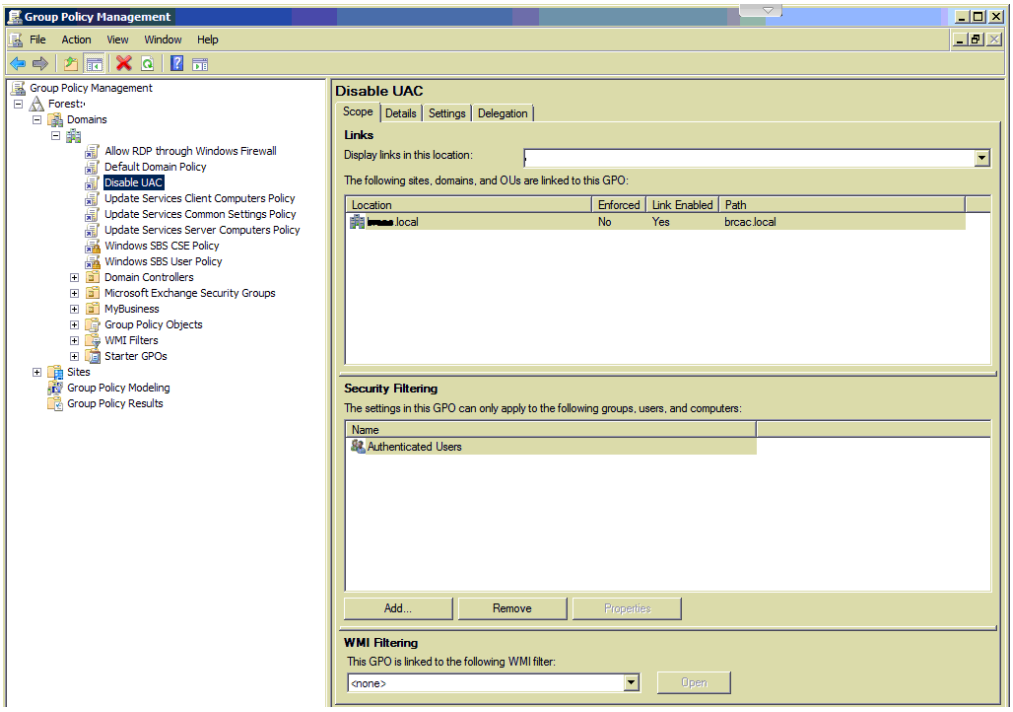
5 - Enabling Performance counters monitoring

Remote Registry Windows service must be running and its start-up type should be set to Automatic.

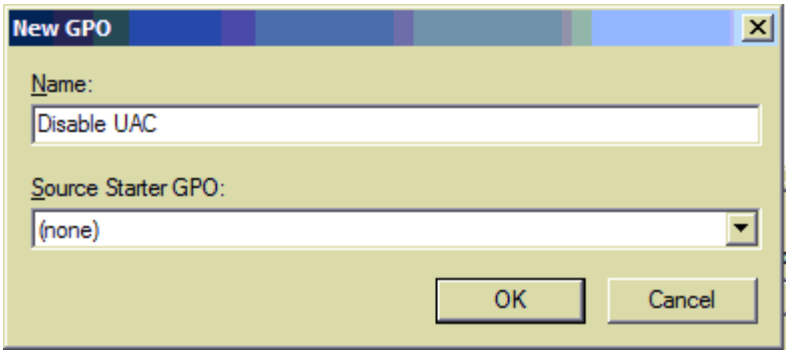
6 - Disable UAC remote restrictions

UAC prevents certain administrative tools from being run over a remote control program (like MonitorPack) because the requesting credentials is not visible to the remote user.

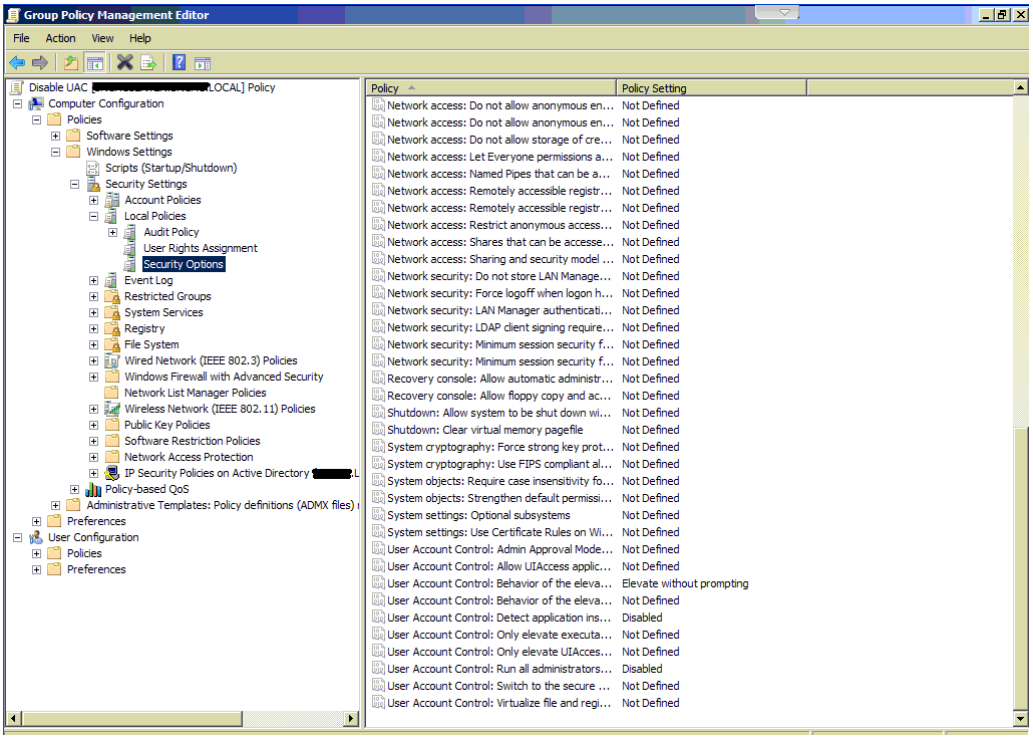
1. Login to the domain controller.
2. Open the Group Policy Management Console by typing gpmc.msc into the Search box or clicking Administrative Tools > Group Policy Management. (Ignore the fact that we already have a GPO for this in the screenshot below, simply run through this checklist to create it.)



3. Expand Forest > Domain > Domain_Name in the left-hand navigation to get a list of existing GPOs. Right-click on the domain name and select Create a GPO in this domain, and Link it here… Name the GPO “Disable UAC” and click OK.



4. The new GPO will appear in the list. Right click on it and select Edit… Expand Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options



5. Configure the following policies:
User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode: Elevate without prompting
User Account Control: Detect application installations and prompt for elevation: Disabled
User Account Control: Run all administrators in Admin Approval Mode: Disabled

6. Run gpudate /force and confirm that UAC is disabled.

7 - Update GPO to allow MonitorPack computers

The procedure below requires usage knowledge of Active Directory Users and Computers and Group Policy Management Administrative Tools

What

Group Object Policies must allow IP address of MonitorPack computer (computer(s) where MonitiorPack Guard and / or MonitorPack Asset is installed) in Active Directory forest.

Why

Microsoft security allows WMI request only from computers that are expressively declared with rights "**Allow inbound remote administration exception".**

How

1. Ensure the user account (svc_monitorpack) that is used on the **MonitorPack** computer has local administrator rights on target Computer(s), Change Credential if needed.

2. Allow for remote administration on target Computers as follow:
You can use the Group Policy editor (Gpedit.msc) to enable the Windows Firewall:
With the Group Policy editor use the following steps in the Group Policy editor (Gpedit.msc) to enable "Allow Remote Inbound Administration" on target Computers.

Note: in workgroup use gpedit.exe.

How with GPMC

GPMC could be installed on Windows Server 2003 or Windows XP Professional
Run GPMC with an account which has sufficient rights to modify Group Policy Objects
a - Under the Local Computer Policy heading, double-click Computer Configuration.
b - Double-click Administrative Templates, Network, Network Connections, and then Windows Firewall.
c - If the computer is in the domain, then double-click Domain Profile; otherwise, double-click

Standard Profile.
d - Click Windows Firewall: "**Allow inbound remote administration exception".**
e - On the Action menu, select Properties.
f - Click Enable, provide the IP address of the **MonitorPack** computer(s) and then click OK.
g- In order to update the GPO use the command **Gpupdate /Force**

8 - Remote performance counters local groups

Why

Since Windows 2008 versions, Microsoft has increase the security for Windows Management Instrumentation requests, MonitorPack Guard Windows service account used for MonitorPack Engine Service "svc_monitorpack" must be also embed in "Performance Log Users" (PLU) group or in PMU "Performance Monitor users" group of each Windows Server 2008 or higher monitored, this can be done Server by Server or from Windows domain GPO.

9 - Windows 10 rights limitation on folders

What

After installation of MonitorPack Guard or MonitorPack Asset on Windows 10 versions, Microsoft has again increase security, once installed you need to give to the "MyMachine\users" local group write rights on the MonitorPack Guard or/and MonitorPack Asset folder.

We stay at your disposal as follow:

- E-mail: support@monitorpack.com
- Online knowledge base: Online knowledge base
- By form Support request