What’s new in ProactiveWatch - August 2010!

The ProactiveWatch August 2010 release provides:

- A technical preview of the integrated Remote Control
- Ability to schedule Windows Patch Updates for only certain days
- New ScriptCentral option to deploy and run scripts across your clients’ systems on a scheduled basis
- Additional graphing from View Metrics.

To use the new features, you will need to make sure you have the latest Explorer (v2.1.1046 or above) and updated ProactiveWatch agents (v2.1.1044 or later).

Updates for the Explorer and ProactiveWatch agents are available from the Manage Portal, or from within the Explorer from the Download menu (shown to the right).

**Integrated Remote Control**

A *technical preview* of our new integrated remote control solution based on VNC is available for your use, giving you instant remote control access to your client’s servers and workstations from the ProactiveWatch explorer. Once you have installed ProactiveWatch agents with the Remote Control (see below), you can select the row of the system, Right-Click, and you will see two Remote Control related options.

**Remote Control …**

Use this option to bring up the dialog box to enter the password, and choose Connect to initiate the remote control session. You may enable the “Remember Password” checkbox to store the password for this machine (which will then enable the Quick Connect option for future use - below).

Enable “Kill Existing Connections” if you wish to kill any other ProactiveWatch remote control sessions to that machine.

Click Connect to initiate the session. This can take 10-20 seconds if FreeMyIT was in a long idle polling state before you see the VNC status box in the top left corner.
Remote Control (Quick Connect)  (or use Function Key F6)

For one-click access, you may save the password in which case “Remote Control (Quick Connect)” will be available or just press F6!

Security
Our implementation of this remote control is secure and does not require that you open any inbound ports, but it does require that the FreeMyIT agents are installed.

Installing Remote Control

On new installations, run the ProactiveWatch Gateway or Agent installer as you normally would. You will supply a password of 8 characters or less for the remote control. You may change the password by running the ProactiveWatch Agent Manager on the target machine (choose Views, Remote Control).

For existing installations of ProactiveWatch, perform the following:

- From the ProactiveWatch Explorer, use Settings->Manage Updates and update the systems if necessary.
- Run ProactiveWatch Agent Manager on the target machine select Views->Remote Control. This will display a list of the necessary components that need to be installed (shown On Right).
- Click Install Needed Updates Now to install the Remote Control components.
  - (If an update to any of the FreeMyIT components is necessary you will need to click Install Needed Updates Now, then refresh (File->Refresh), and click Install Needed Updates Now a second time to install the Remote Control components).
- Finally set a password for the remote control for this machine.
Using Alternate Remote Control

ProactiveWatch still provides the ability to launch either LogMeIn Pro (IT Reach), LogMeIn Free or your own command line (e.g. – mstsc) when selecting Remote Control from the Tools or Right-Click menus.

To use an alternate program use Fill Cells or the Properties dialog to set the “Remote Control” column as follows:

<table>
<thead>
<tr>
<th>Remote Control Column</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>LMI</td>
<td>Runs LogMeIn Pro (assuming it is installed on the machine and the Network Console was activated/running)</td>
</tr>
<tr>
<td>lmi</td>
<td>Initiates a remote control session for LogMeIn Free. Note that you should already be logged into LogMeIn's Central website. You can also use this option to launch “Pro” without having the Network Console licensed/running.</td>
</tr>
<tr>
<td>&lt;cmd line&gt;</td>
<td>Other command line, such as MSTSC (without the angle brackets).</td>
</tr>
<tr>
<td>&lt;blank column&gt;</td>
<td>If the column is blank, it will run the ProactiveWatch Remote Control.</td>
</tr>
</tbody>
</table>

Troubleshooting

1. Ensure that Windows Firewall (or other firewall or anti-virus) is not blocking any of the ProactiveWatch or FreeMyIT components, including “Reflector” and “Reflector-Client.”

2. “Connection Closed” dialog box. The integrated VNC is not very friendly in terms of error reporting. If the password is invalid, you will get the “Connection Closed” pop-up box. You will also get the same Connection Lost pop up box if the connection is actually lost. You may also see the “Socket error” message, which also indicates an incorrect password or connection problem. Try again with the correct password.
Scheduling Windows Patch Updates for specific days

You may now set a schedule for the ProactiveWatch Windows Update mechanism in order to have updates applied only on certain days. This is done by using CRON to set a schedule for the template to be run, in conjunction with the Patch_Install_Window to control the time.

Step 1. If you are using the default “Windows Update Enhanced” template, you will need to clone it and make the changes in the new template.

1. In the Explorer, go to Settings->Monitoring Templates
2. Find the Windows Update Enhanced template, select it, right-click and choose “Clone”
3. Remember to assign it to the intended systems
4. And Unassign "Windows Update Enhanced" or the values there will continue to apply patches daily!

Next, in the ProactiveWatch Explorer, open the template you are using for the Windows Updates (step 1). Click Configure and click into the "Schedule" field to get the pop-up to enter the custom CRON which tells when the template will be "run" as shown in the screen below.

You may enter your own custom crontab schedule in the Frequency field using the format:

```
<minute(0-59)> <hour(0-23)> <day-of-month(1-31)> <month(1-12)> <day-of-week(0-6)>
```

Each "field" is separated by a single space, using commas or hyphen without a space to separate multiple entries within each "field."

As an example:  * 1-4 * * 1,5 programs the ProactiveWatch Windows Update template to be run by the agent only between 1 to 4 am on Mondays and Fridays.

Another example: * 20-23 * * 5 programs the ProactiveWatch Update mechanism to be run by the agent between 8pm-11pm only on Friday evenings

Note that it is CRITICAL that you set the Patch_Install_Window and Patch_Install_Duration to coincide with the CRON schedule or patches will not be installed:
Scheduled and Recurring Script Execution in ScriptCentral

There is a new option in ScriptCentral that allows you to schedule a script to run on one or more machines at a future scheduled time or on a recurring basis.

In the ProactiveWatch Explorer, go to the ScriptCentral tab (was previously named RemoteCommand) and log in to the ScriptCentral system.

Click the “Run Script” link to navigate to the Run Script page, and click the “Manage Scheduled Jobs” link:

Next, click the link: Schedule a New Job which will start the “Run Scheduled Script Wizard” and will display a list of your computers. Select the systems to be included in this Scheduled Job and click Next.

You will then see a list of scripts that are already “deployed” on all of the selected scripts. If necessary, choose “Show all scripts” to display all the scripts in your “My Script Library.” Select the script to be run by this job. (The script will be automatically deployed to systems as necessary.)

Set the schedule for the script. You can use one of the existing pre-defined schedules, or select “Specify in CRON format” to enter a custom schedule. (See the discussion of CRON above.)

To run the script just ONCE, enable the “Run Only One Time” checkbox and set the day and time.
Results from the script can be viewed from the Run Script page, in the same way you will view scripts run in the background:

### Additional graphing from View Metrics

As a reminder, the ProactiveWatch agents summarize and transmit the resource statistics approximately every hour, and you can view the most recently transmitted resource statistics from one or more machines in the Explorer Console. Select one or more systems, right-click and choose View->Metrics:

Select one or more rows, right-click and choose “Graph” to display a graph, where you also have the option to export the data: