

SyAM Software™

Deploying a Windows Registry Edit to a Group of Systems

Overview:

By using the Management Utility you can make registry changes to a group of System Clients that are managed by a System Area Manager.

Create the registry changes and save as a .reg file

This example shows how to modify the default time delay for the windows start menu – as users log in they will get the new default value.

Windows Registry Editor Version 5.00

[HKEY_USERS\.DEFAULT\Control Panel\Desktop]

"MenuShowDelay"="200"

Save the .reg file in the \syam\utilities\apps folder or the designated folder where you share to deploy applications from. We saved our example as **startmenudelay.reg**

Create a batch file that will be run on the target machines to install the registry edit.

The example below runs the registry across the network from the network share, no registry files are copied to the target system

```
regedit.exe /s \\192.168.200.113\c$\syam\utilities\apps\startmenudelay.reg  
exit
```

The example below copies the registry file to the target system and then runs this locally and then deletes the registry file once programmed

```
Cd \  
Copy \\192.168.200.113\c$\syam\utilities\apps\startmenudelay.reg c:\syam  
cd \syam  
regedit.exe /s startmenudelay.reg  
del startmenudelay.reg  
exit
```

****Note – The batch file must be edited to use the network shared path and files names that you have configured in your Management Utility.***

From the Management Utility, choose the Discovery Tab and set up the group that you wish to deploy the registry edits to.

The example below shows a group called Default that contains the two systems we wish to edit the registry on.

The screenshot shows the 'Discovery' tab in the Management Utility. The interface includes a navigation bar at the top with tabs: Discovery, System Client Configure, Third Party Configure, Authentication, Installation, Power Management, System Alert Matrix, and Remote Console. Below the navigation bar, there is a step indicator: 'Step 1: Select your machines. There is a hard-wired limit of 3000 machines at this time.'

The 'Domain Options' section has a checkbox for 'Scan my domain (you must be logged into the domain)' which is unchecked. Below it are fields for 'Domain:' and 'Organizational Units:' with 'Discover Domains' and 'Discover Organizational Units' buttons respectively.

The 'Network Scan' section has a checked checkbox for 'Scan IP address range'. Below it are input fields for 'Starting IP address:' (192.168.200.82) and 'Ending IP address:' (192.168.200.82). There is also a checked checkbox for 'Resolve ip address to host name' and an unchecked checkbox for 'Scan for Intel(R) AMT'.

The 'System Scan Results' section has a 'Filter By:' dropdown and a 'Scan Now' button. Below this is a table with the following data:

OU	Name	IP Address	SyAM Version	Type	AMT	Managed	On	MAC
	EQ45MF	192.168.200.82	V4.31.990-BL36...	Desktop	No	Yes	Yes	88-88-88-88-87-88

Below the table is an 'Installation List' section with a dropdown menu set to 'Default' and a 'Scan Now' button. Below this is another table with the following data:

OU	Name	IP Address	SyAM Version	Type	AMT	Managed	On	MAC
	HP-VPRO	192.168.200.81	V4.31.200-BL35...	Desktop	No	Yes	Yes	00-08-02-F5-72-A1
	EQ45MF	192.168.200.82	V4.31.990-BL36...	Desktop	No	Yes	Yes	88-88-88-88-87-88

On the right side of the interface, there are several buttons: 'Scan Now', 'Add to Install List', 'Export Results', 'Refresh List', 'Delete List', 'Remove', and 'Clear List'.

Now choose the Third Party Configure tab.

Click the Add button to choose the batch file that you wish to run, remember to check off Copy this file locally as the batch file will run on each target that you wish to edit the registry. Also remember to choose Windows as your Target Platform

The screenshot shows the 'Third Party Configure' tab in the Management Utility. The interface includes a navigation bar at the top with tabs: Discovery, System Client Configure, Third Party Configure, Authentication, Installation, Power Management, System Alert Matrix, and Remote Console. Below the navigation bar, there is a step indicator: 'Step 2: Choose installation source:'.

The 'Path' field is highlighted with a red box and contains the text: '\\192.168.200.113\c\$\SyAM\Utilities\apps\registry-edit-nocopy.bat'. Below it are fields for 'Parameters' and 'Timeout' (10). There is an 'Add...' button and 'Remove' and 'Clear List' buttons.

Below the path field, there is a checked checkbox for 'Copy this file locally to each target machine before installing (required if the above is not a network share, cannot be used with local impersonation)'. Below this is a section for 'Step 3: Choose installation parameters:'.

The 'Custom Software Parameters' section has a 'Click on the above installation source to configure parameters.' instruction. Below it is a text box: 'The install folder identified below must be a shared folder and accessible by all systems within your installation list.' Below this is an 'Install folder:' field with a dropdown menu set to '\\192.168.200.113\c\$\SyAM\u' and a 'Timeout (minutes):' field set to 10. There is also a 'Custom parameters:' field and a checkbox for 'Do not check for process completion (for BIOS updates)'.

The 'Microsoft Update Scan' section has a 'Scan' button and a dropdown menu set to 'Default'. Below it is a text box: 'This scans the systems contained within the installation list and identifies any required Microsoft updates.' Below this is a 'Download folder:' field with a dropdown menu set to '\\192.168.200.113\c\$\SyAM\u' and a 'Download Status' button.

On the right side of the interface, there is a 'Target Platform:' section with radio buttons for 'Windows', 'Mac', and 'Linux'. The 'Windows' radio button is selected and highlighted with a red box.

Remember that the authentication Tab must be configured using the Administrator level User Name and Password of the user currently logged in running the Management Utility and this user must be a valid user on the target systems.

Step 4: Authentication

Install as local system (the file must be copied to each system before installation).

Impersonation

Install impersonating this user on each target machine:

User name: Administrator

Password:

Domain: test-network

Grant this user "logon as service" permissions (required unless the account already has this privilege).

Remove "logon as service" permissions when finished (this will remove the privilege from the account, even if it was not granted by this program).

Impersonate this user locally (required if you are not logged in as the above user). This user **MUST** exist on the local system, and copying locally cannot be enabled!

Now choose the Installation tab, from the drop down menu choose the group you wish to deploy to and then press the Install Third Party button.

Current Status: Number of simultaneous installations: 2

Installation List: Last refreshed: 02/02/2010 15:40 Default

OU	Name	IP Address	SyAM Version	Type	AMT	Managed	On	MAC
	HP-VPRO	192.168.200.81	V4.31.200-BL35...	Desktop	No	Yes	Yes	00-08-02-F5-72-A1
	EQ45MF	192.168.200.82	V4.31.990-BL36...	Desktop	No	Yes	Yes	88-88-88-88-87-88

Install System Client (win) **Install Third Party (win)** Clear History

Installation History:

Time	Name	IP Address	Status	Type	File
02/02/2010 16:05	HP-VPRO	192.168.200.81	Succeeded	Third Party	registry-edit-nocopy.bat
02/02/2010 16:05	EQ45MF	192.168.200.82	Succeeded	Third Party	registry-edit-nocopy.bat

It will report the installation history as each target system has been updated.

***Note - When making registry edits you can only make current user registry edits to the user with the username that you are using in the authentication of the Management Utility.**