Network Inventory Professional 5

Table of Contents

Chapter 1: Introduction

Network Inventory Professional is an award-winning network inventory software for organizations of any sizes. It offers features for remote audit of every PC in your network without having to install client modules. By using Network Inventory Professional you can get detailed hardware, software inventory and licensing information from all remote PCs within seconds. Powerful reporting module helps you save a lot of time for preparing network PC inventory and network audit reports.

How much time do you spend on network inventory? How accurate and detailed your audit information is? Do you know what is your actual configuration now? Network Inventory is network audit software created to provide you by actual hardware and software audit information with no efforts from your side.

How this network audit solution can be helpful for you? First of all, it is able to make remote audit in automatic mode and collect information about hardware and software assets from remote computers in a few moments. It means that you always have up-to-date network inventory database with all assets, their settings and specification. This database can be used to generate audit reports and answer questions like:

- Which desktops lack free space on their hard drives?
- Which have Windows XP and have less than 1 Gb RAM?

Main Features

Network Inventory is a tool that helps you automatically collect up-to-date information about all hardware and software assets from all remote PCs in your network into audit database and use it to quickly find required inventory information and build network inventory reports. With this network inventory tool you can get detailed network audit information in just few mouse clicks without any network environment configuration tricks, logon script or WMI manipulation or client installation to remote computers.

PC Inventory

Collect complete hardware and software audit information from all remote PCs in few minutes without physically attending them. Use modern network inventory scan approach, which doesn't require complicated configuration or client installation to remote PCs and is able to work in different environments.

- Unattended Remote PC Inventory
- Clientless Remote PC Audit
- Large Networks Audit
- Fast Remote PC Inventory Scan

Software Inventory

Make remote audit of installed software to get a high-level overview of used applications, guarantee licenses compliance and optimize software purchases and upgrades. Get software report for particular PC or entire network. Identify forbidden applications and resources on remote PCs.

- OS and System Information for Every PC
- Installed Software Inventory

       3

Hardware Inventory

Perform automatic network audit and get general overview of all hardware assets installed on remote PCs. Get information about configuration of each particular PCs. Easily find where particular hardware component is installed. Simplify hardware upgrades and optimize your purchases.

- Remote Unattended Hardware Audit

- Hardware Inventory Information for Every PC

- Detailed Assets Specification

- Aggregated Hardware Assets Overview

Inventory Report

Generate detailed network inventory reports based on collected network audit information using a set of clear, accurate and nice-looking inventory templates. Save produced reports in one of popular formats. Customize existing or design own reports. Integrate your application with network inventory system.

- Automatic Inventory Report Generation

- Hardware and Software Inventory Reports

- Easy Reports Customization

Chapter 2: User Interface Overview

The main application screen **Pic 1** is divided on two parts. At the left side you can find **Machine Management** area that displays the network tree and asset groups. Management toolbar **A** is used to execute main actions, for example, scan network or update inventory information. The full set of actions is available from the context menu on the tree.
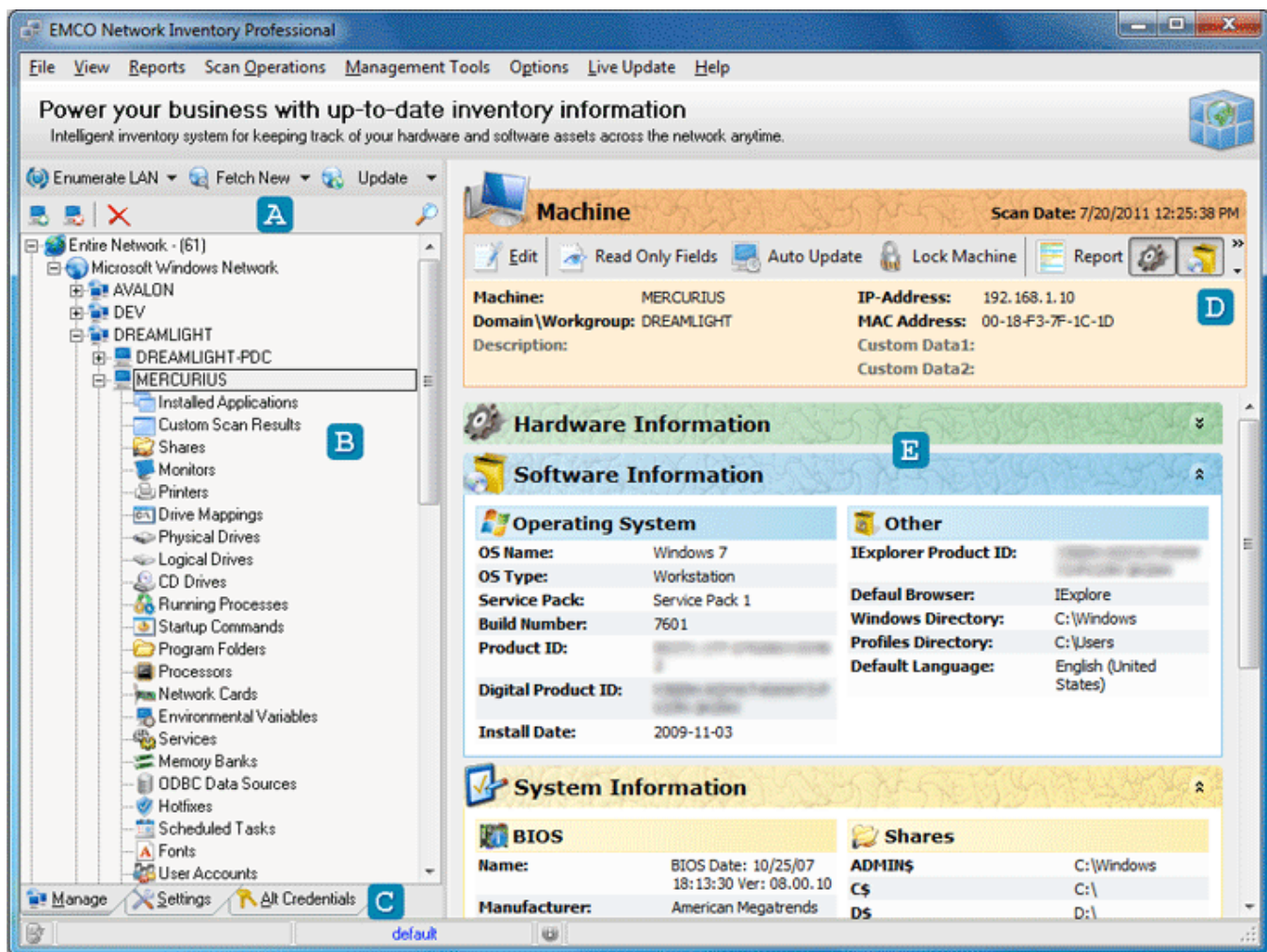
Pic 1. The main application screen

The **Machine Tree** is located under the management toolbar and contains asset information that can be represented by two ways. The **Entire Network** node **B** displays PCs found in the network, grouped by domains and workgroups. When some node under the **Entire Network** is selected, on the right side you can see related inventory information. For example, if you select particular PC, you can see its hardware and software assets summary. If you want to learn more about concrete asset, for example processors on particular PC, you can select **Processors** under PC's node in the tree and get detailed information.

Other nodes in the **Machine Tree** represent particular asset category for all computers in the network. Thus, if you need to check monitors information only, you can expand **Monitors** root node in the tree and select domain/workgroup or particular PC to get information for them.

In order to manage application settings you can switch tabs located under the **Machine Tree**. **C** The **Settings** tab allows you to manage information extracted from remote PCs, so you can enable or skip some parameters. The **Alt Credentials** tab is used to set administrative credentials applied to access remote PCs. If your account doesn't have administrative permissions on remote PCs you need to set administrative account on this tab.

Information displayed on the right side of the main screen depends on the node, selected in the **Machine Tree**. For example, if PC node is selected, at the right side you can see **Machine Summary** information. Management toolbar **D** is located at the top of the summary and provides a quick access to the most frequent actions, such as report generation, locking and update functions. Under the toolbar **E** you can find **Hardware**, **Software** and **System Information** boxes with the correspondent information about PC.

Chapter 3: Getting Started

This chapter is a starting point for everyone, who would like to see how to make software and hardware audit of remote computers with the Network Inventory Professional. If you are making first steps with the application, this tutorial will help you to quickly familiarize with main features of the product.

Any company and organization needs to have hardware and software inventory information in order to plan upgrades or hardware/software purchases. This information gives you an overview how many and what exact hardware and software assets do you have and helps to identify what assets you need to add or replace.

Today every PC has tens applications installed and consists of dozen components, including CPU, memory, motherboard, hard drive, etc. Manual collecting inventory information from one PC can take up to ten minutes. How long does it take to make inventory of tens, hundreds and thousands PCs in your network? Also consider the fact that to be useful inventory information should be up-to-date. It's not enough to collect assets information at the purchasing time, because afterwards configuration can be changed - administrators can replace or remove some hardware, users can install new applications, etc.

Is there an effective way to make the software and hardware audit? Network Inventory Professional allows automatic collecting hardware and software assets information from remote PCs and gives you few advantages:

- Fast automatic collection of asset information that significantly reduces your time and efforts

- Always up-to-date inventory information helps you to make decisions easier

What's Inside

Collect Hardware and Software Information from Remote PCs

Browse, Filter and Analyze Inventory Information

Prepare Inventory Report

Detect Licensing or Policies Violations on Remote PCs

Collect Hardware and Software Information from Remote PCs

As you may know, Network Inventory allows you to make hardware and software inventory of remote PCs without installation of any agents on client computers. It simplifies the process, because in order to prepare to the remote inventory you just need to check only two things. First, you need to have administrative access to remote PCs. If your current account doesn't have administrative permissions, you need to go to the **Alt Credentials** tab and setup credentials there. Second, you need to switch to the **Settings** tab and check what data will be collected from remote PCs. Please note that some data is collected through the Windows Management Instrumentation (WMI), so this service should be enabled on remote Pcs.

Collection of inventory information is activated by the **Enumerate LAN** button located on the management toolbar. This button launches the network enumeration to detect PCs in all available domains and workgroups within the local network. Inventory information is extracted from all remote PCs and stored in the local database. If you would like to reduce the range of scanned PCs, you can choose other options, like a scan by IP range, available from the **Enumerate LAN** pop-up menu.
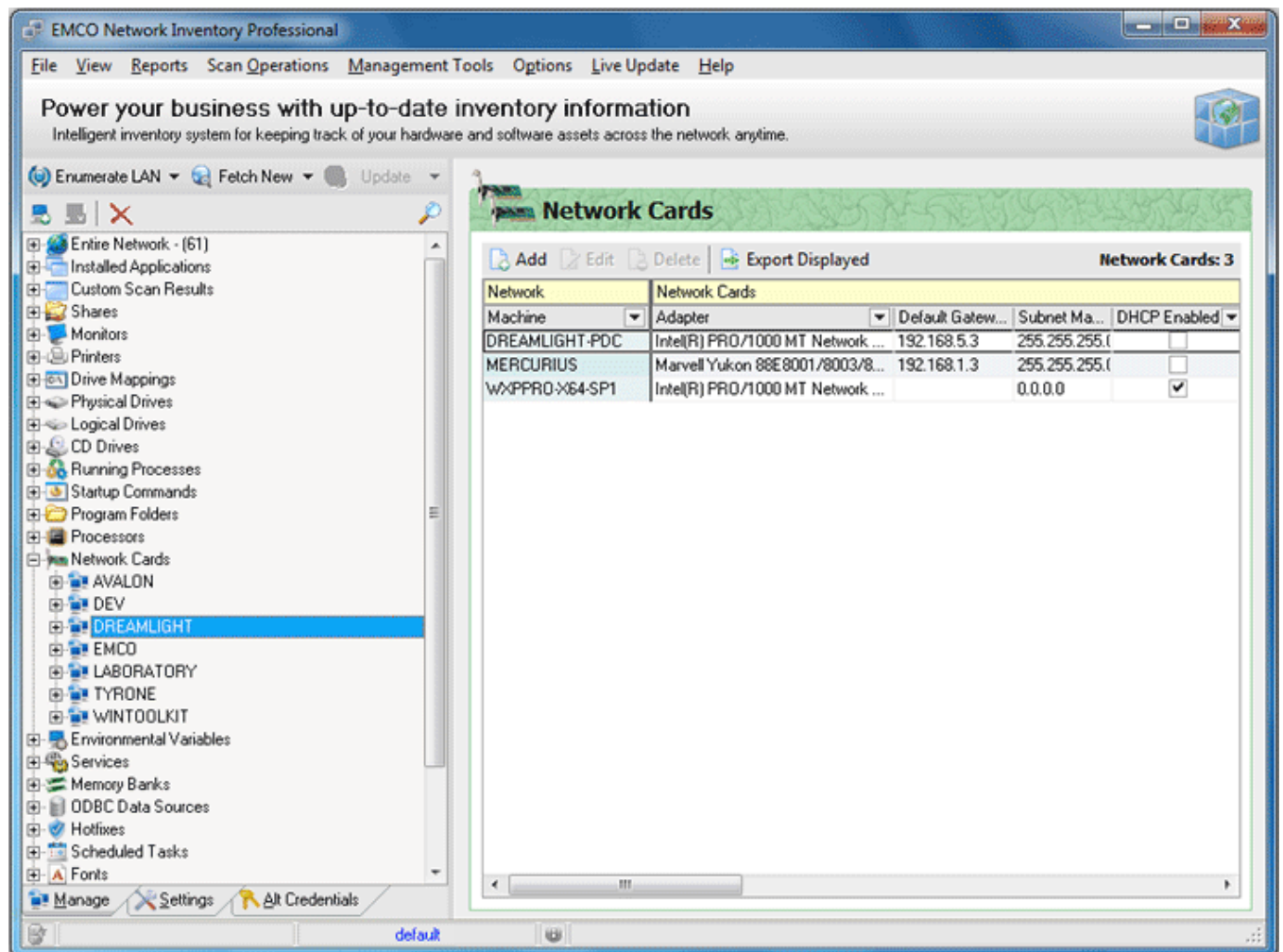
`Pic  1`
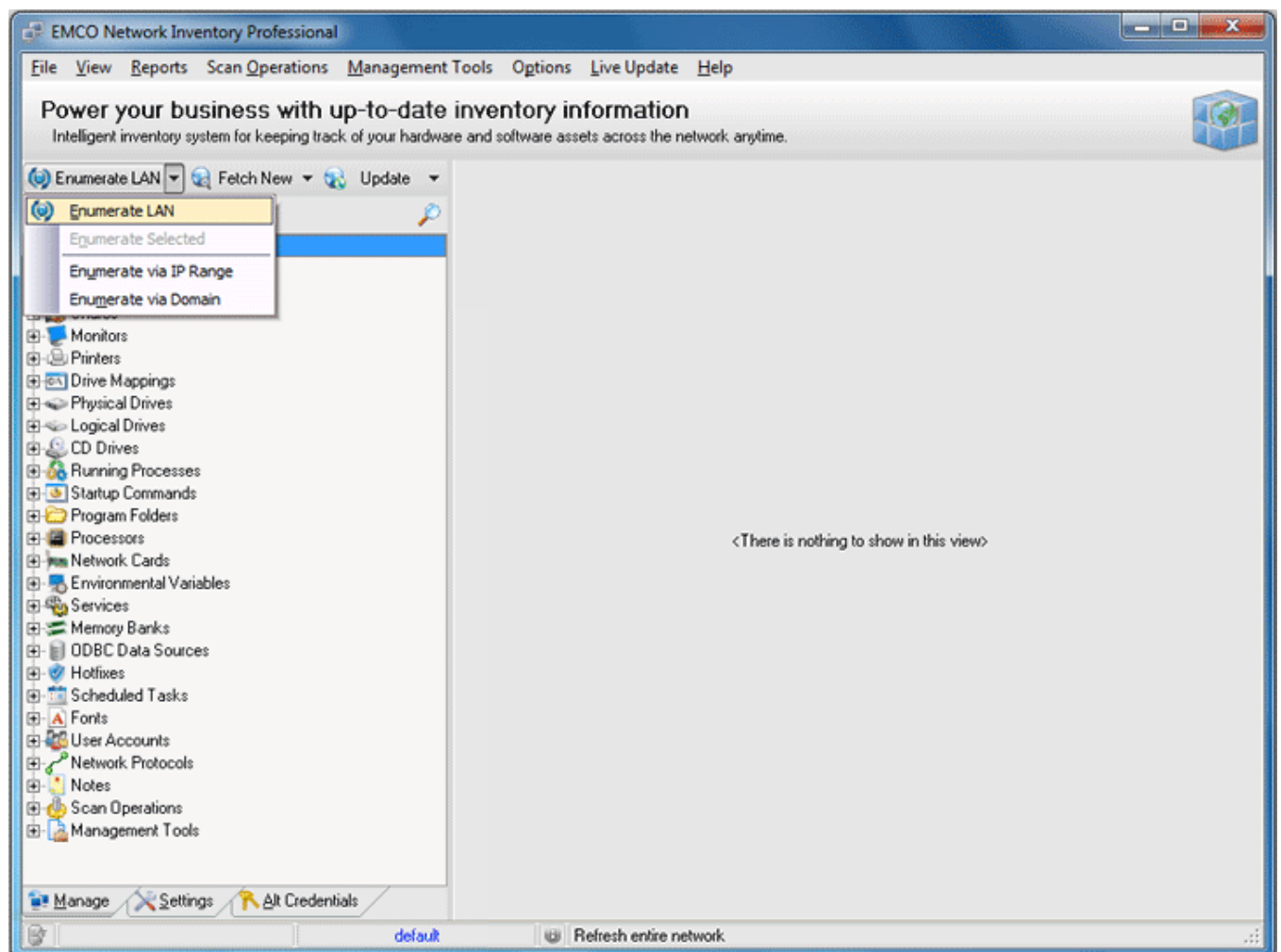
Pic 1. Enumerate LAN options

After a scan the **Machine Tree** displays detected PCs grouped by domains and workgroups. You can browse the tree to see inventory information for the selected tree node. Thus, you can see asset information for workgroup/domain or PC or components of particular PC, etc. `Pic 2`


Pic 2. Inventory scan results

When you make the first scan, the **Machine Tree** is filled by the collected data. Next time, when you need to make an inventory, you can choose to collect information from the new PCs available in the network, or to update information on existing PCs in the tree. In this case you need to use **Fetch New** or **Update** buttons on the management toolbar. If you make **Enumerate LAN**, then the network scan and the data collection procedure will be repeated again and your current data will be replaced by the new one.

## Browse, Filter and Analyze Inventory Information

When collection of inventory information is finished, you can browse it by selecting required nodes in the **Machine Tree**. By this way you can get inventory information for each particular PC or the general overview for particular asset across the network. But if you have hundreds or thousands PCs in the network, it's hard to find required information.

Network Inventory can help you to easily manage and narrow information by applying filters. For example, let's detect problematic PCs, which have a lack of memory. In order to find them, select the domain or workgroup under the **Entire Network** node in the tree. Summary information about PCs in this domain or workgroup is displayed on the right side. This information includes **Physical Mem** field, so we can apply filter by this field to display only problematic PCs. Click on the down button on the field's caption and in appeared menu select **(Custom...)** item. On the **Custom AutoFilter** dialog select is less than option and enter *512* value to display only those PCs, which have less than 512MB of memory. `Pic 1`
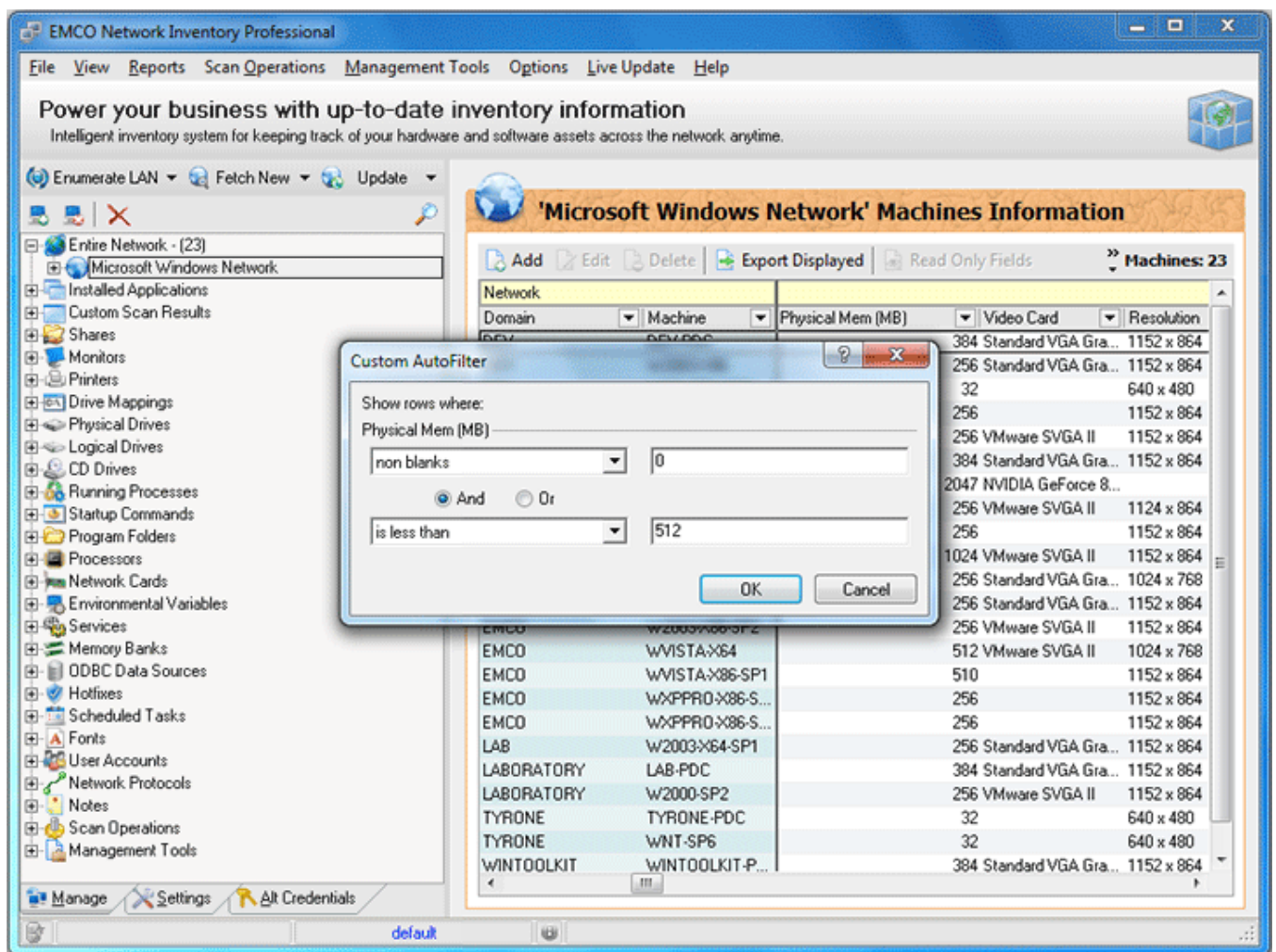
Pic 1. Custom AutoFilter dialog

After applying the filter the displayed data will be updated to show only those PCs that fulfill the filter condition. **Pic 2**
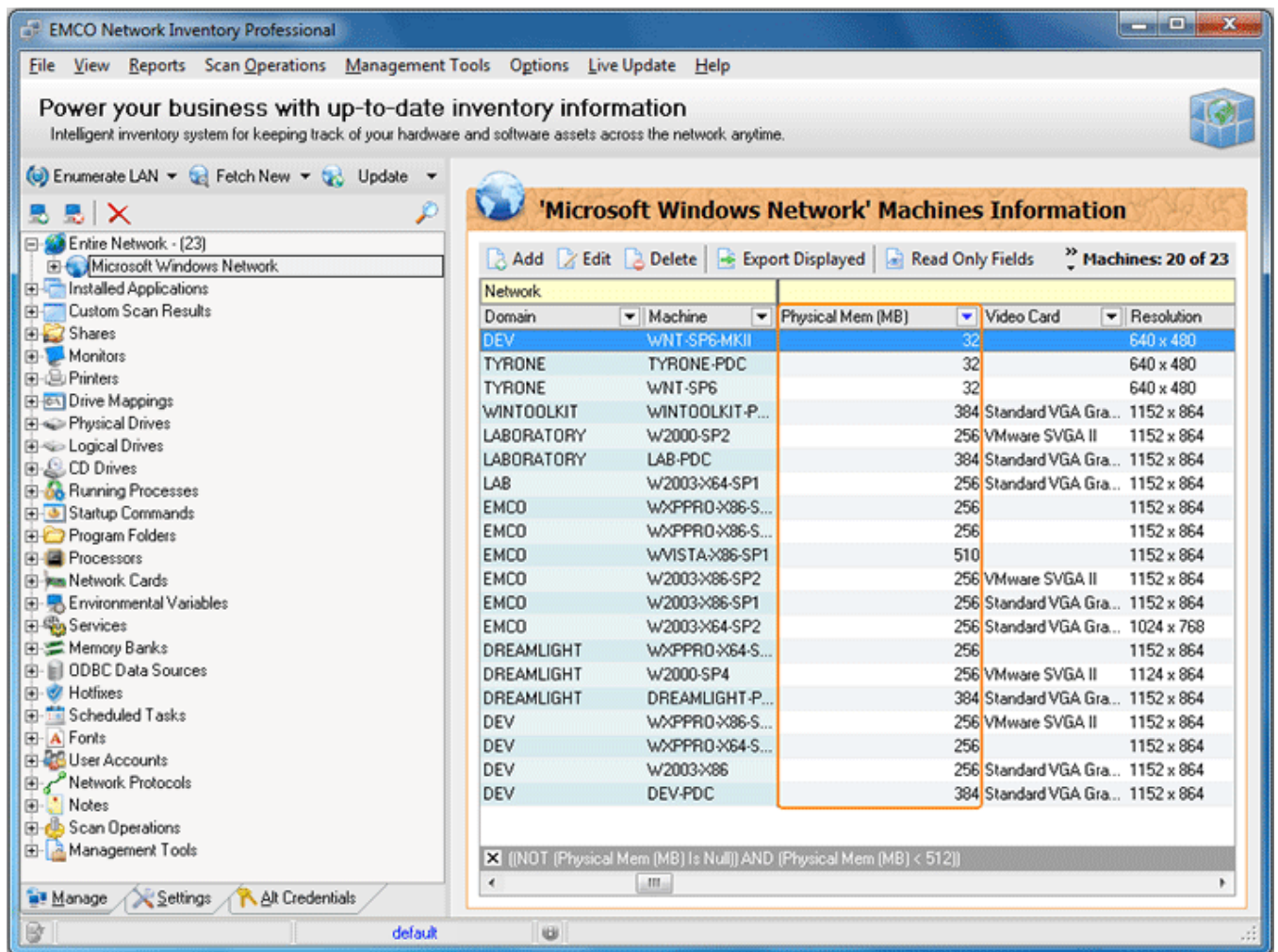
**Pic 2. Scan results with applied filter**

Note that you can apply multiple filters at once, for example to detect PCs that have Windows Vista and a low memory.

Prepare Inventory Report

Collecting information from remote computers is only a part of inventory task. Usually, the asset information should be composed into printable reports for the management or further reference by IT team. Network Inventory provides few easy ways to prepare reports. First, you can save information displayed on screen in various formats if you click on the **Export Displayed** button. Second, you can generate a set of detailed predefined reports. Third, you can your own custom reports.

All reports are customizable. It means that you can change the title page and put your name and company logo to it. To customize report select **File > Preferences...** item from the main menu and go to the **Report** tab. Change report Title, Description and set Author and Company Logo. **Pic 1** Press **OK** button to apply settings.
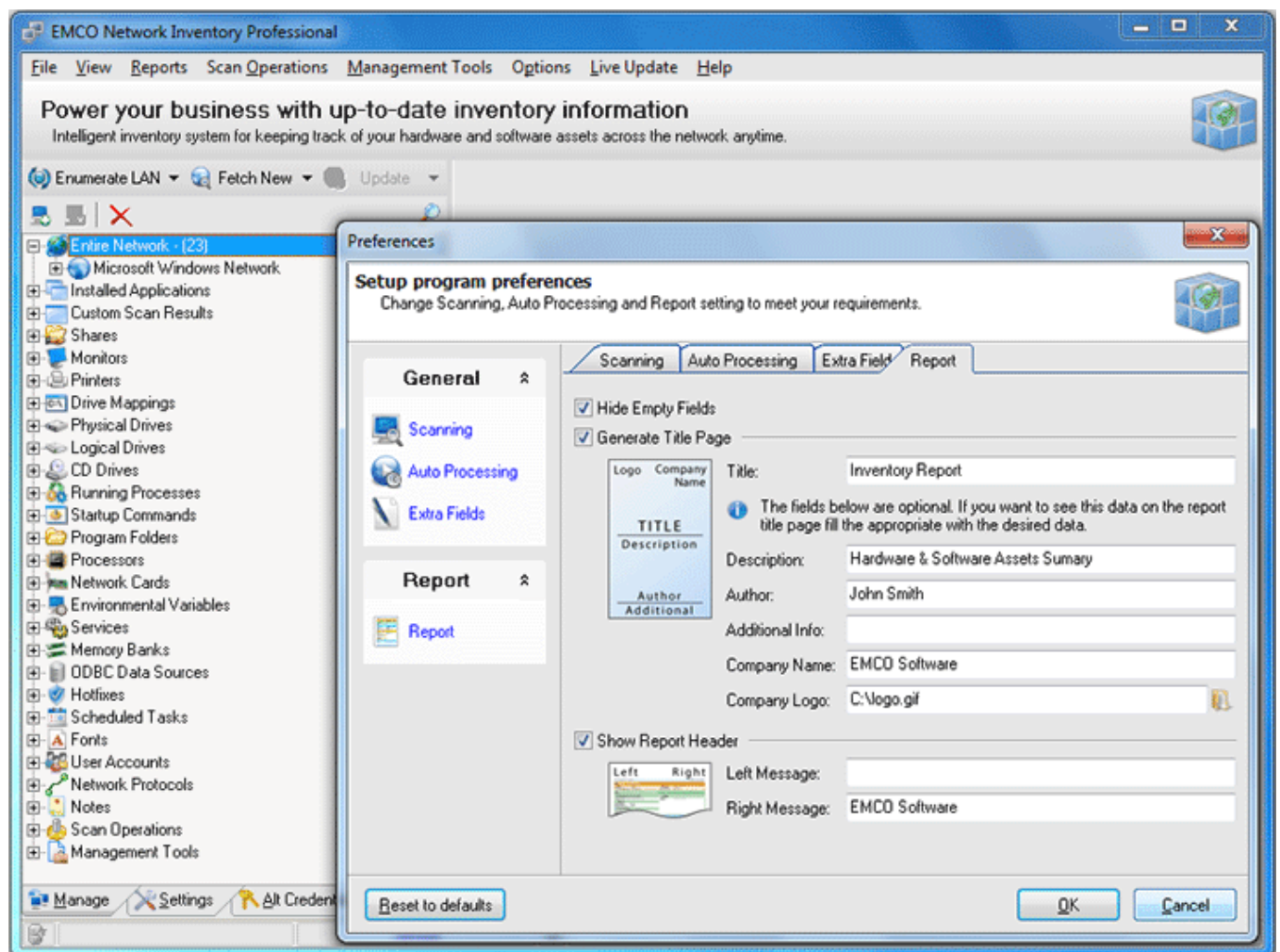

Pic 1. Report customization options

Let's create inventory report in PDF format for all PC. To generate the report select **Reports > Machine Data > Export to File > All** item from the main menu. On the appeared **Field Output Selection** dialog you can choose what data should be included into the report. Pic 2
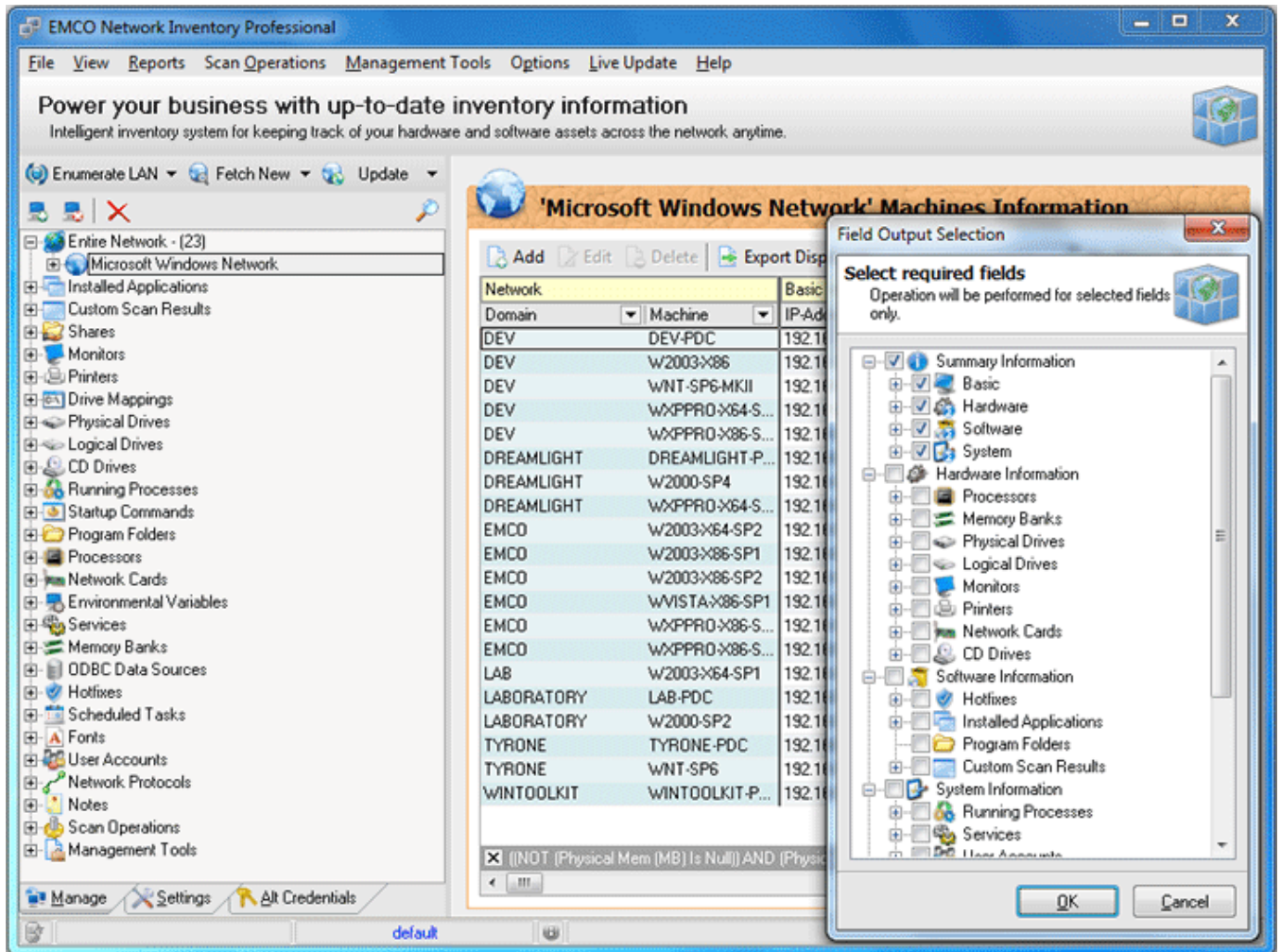

Pic 2. Field Output Selection dialog

Make you selection, press **OK** and proceed to the **Save As** dialog where you need to enter the file name and choose **Adobe Acrobat Document** as output format. Press **Save** button to generate the report and open it in the Acrobat Reader. You can see logo and customized captions on the title page. Pic 3
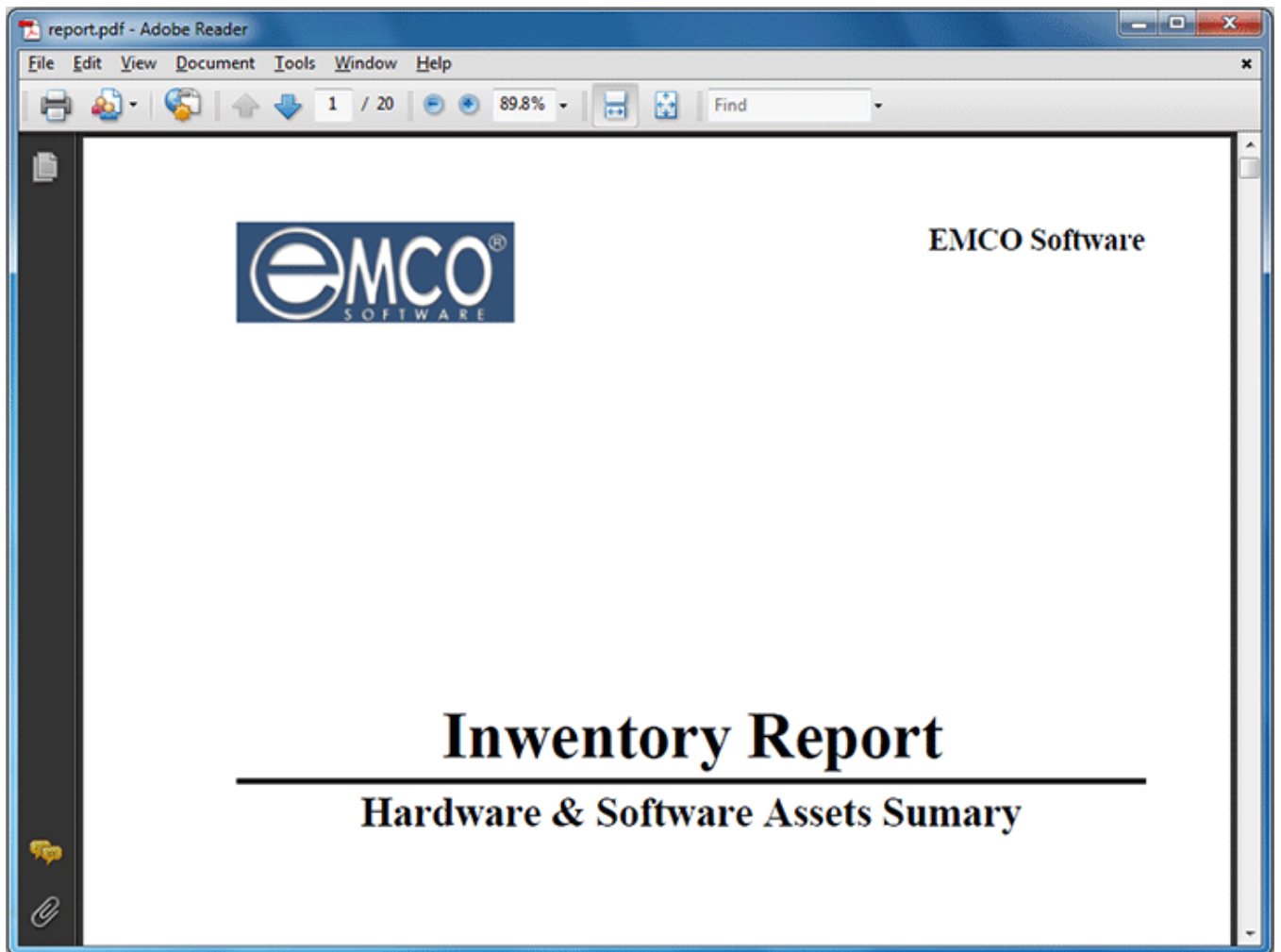
Pic 3. Report title page

Other pages contain information selected for inclusion into the report. **Pic 4**
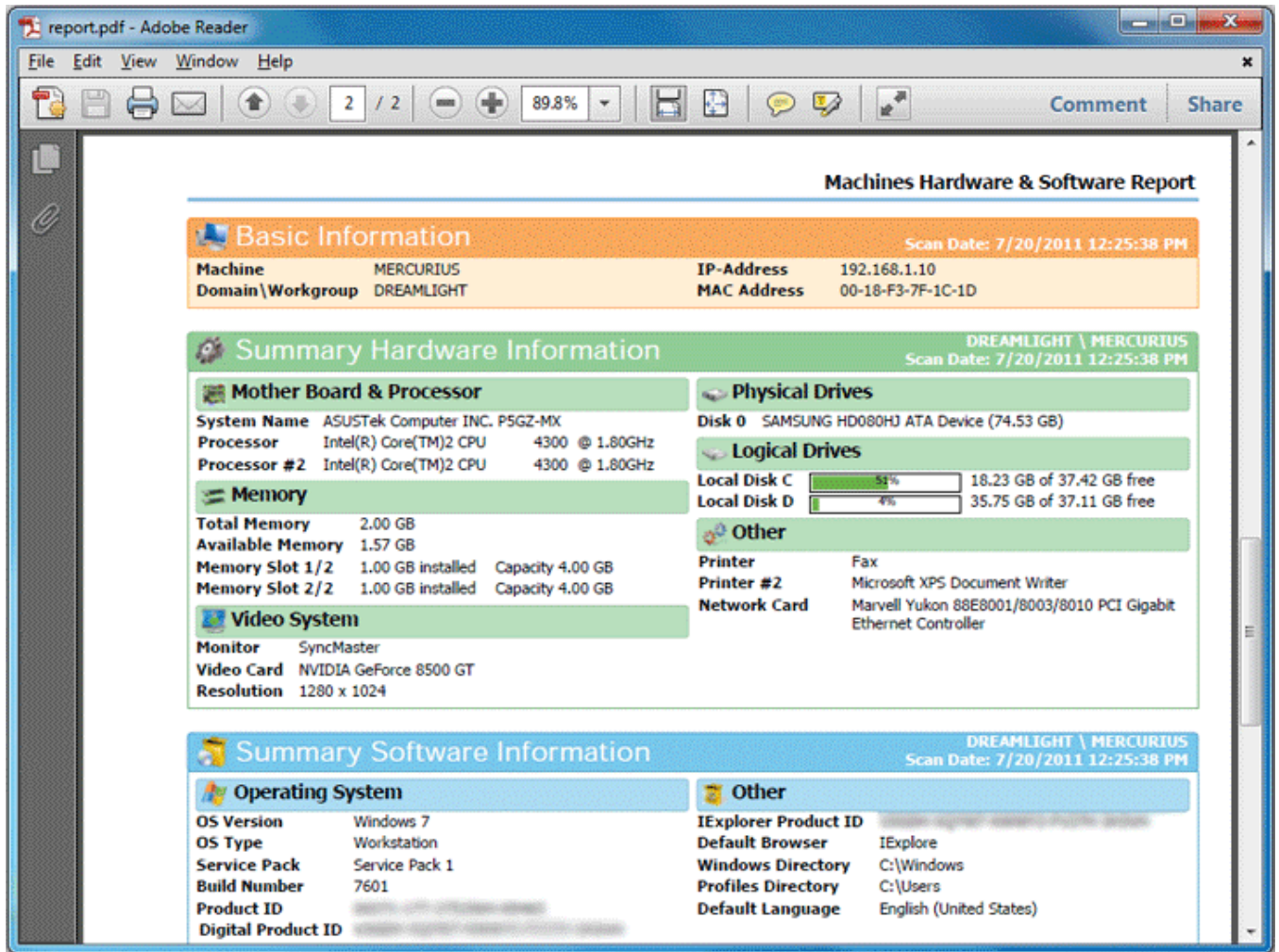

Pic 4. PC Summary report

Now you are familiar with a sample of building a report and configuring the report presentation and can create inventory reports fast and easy.

Detect Licensing or Policies Violations on Remote PCs

Network Inventory has an ability to make a custom search on remote computers. You can define specific conditions to search resources on the file system and registry. This feature is useful in various cases, for example, to detect remote PCs with specific resources, settings or viruses, etc. It can help also to detect licensing or company policies violations. For example, let's detect PCs that have MP3 files on hard drives.

Remote search options are available under the **Scan Operations** node in the **Machine Tree**. To make a files scan select **File System Scan** node and press **Add** button to configure a new scan task. On the appeared **Add Scan Task** dialog enter scan task name and description. Pic 1
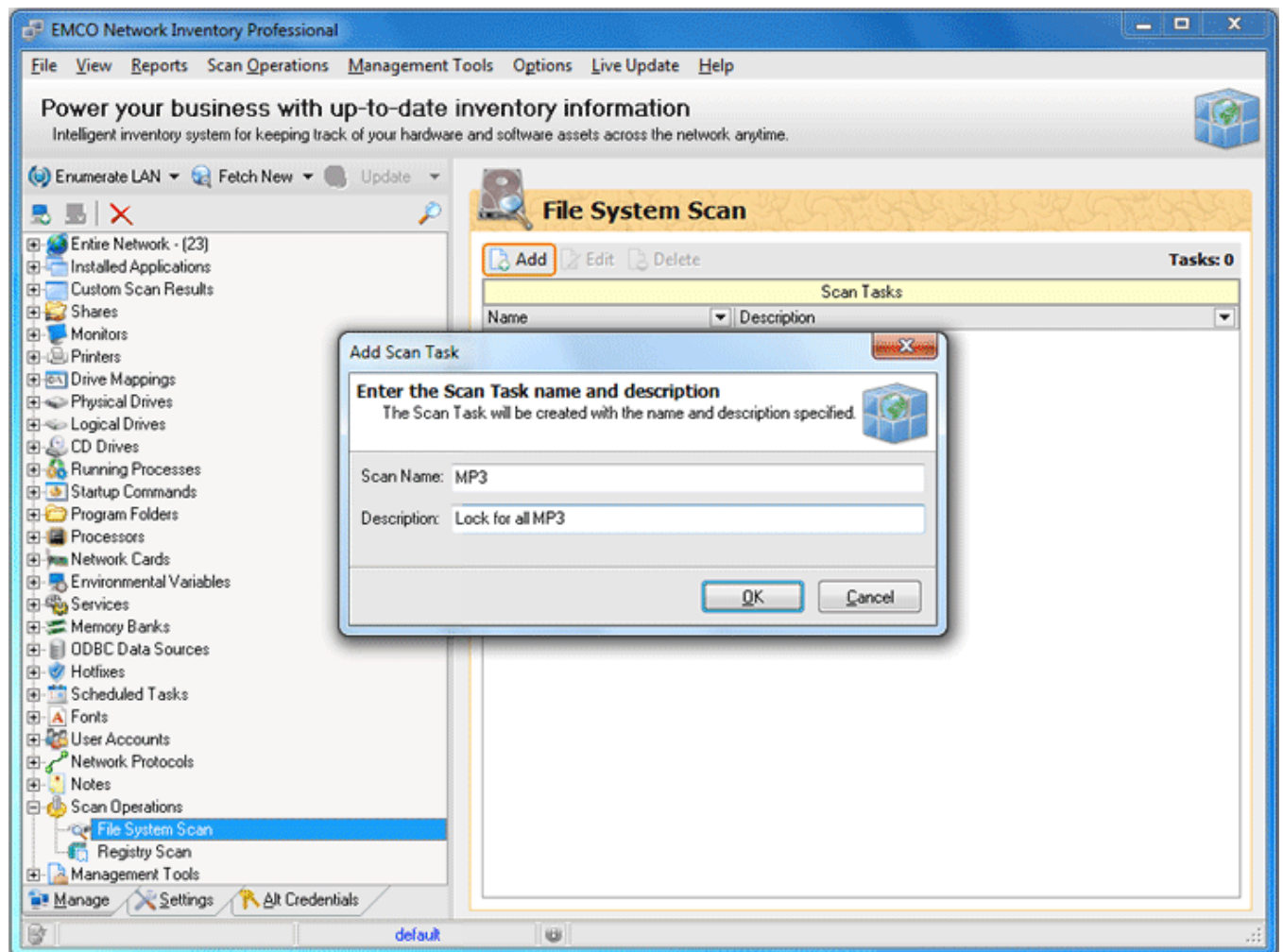


Pic 1. Add Scan Task dialog

New scan task will appear in the tree and you can select it to configure conditions. Click on the **Add** button on the toolbar and on the **Add Scan Criteria** dialog `Pic 2` enter file mask *.mp3* and select *%All Drives%* as a search criteria to look for MP3 files on all available drives. Press **OK** button to finish.
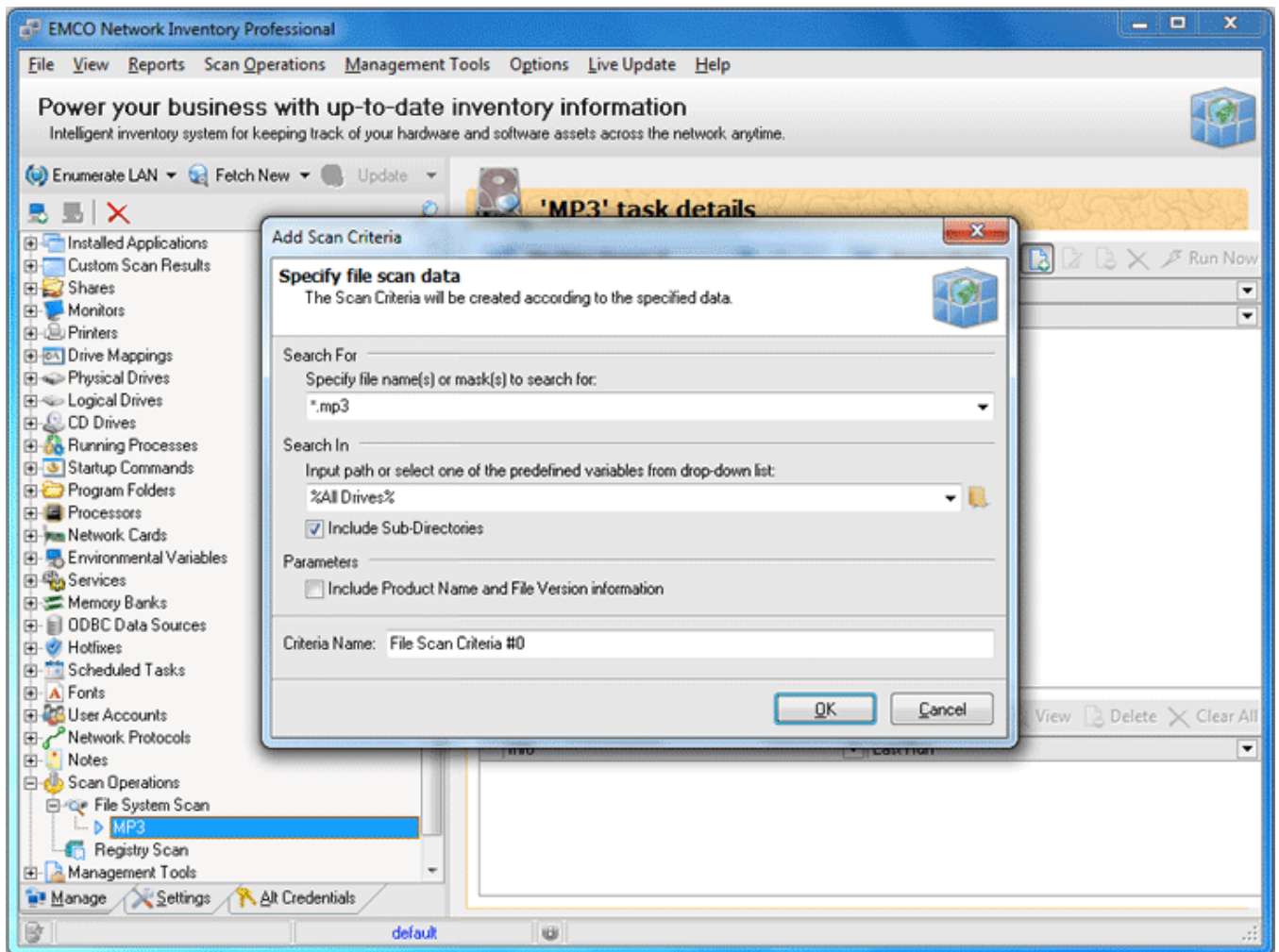
**Pic 2. Add Scan Criteria dialog**

Next, we need to configure the search scope, so click on the **Include Machine** button located on the **Machine Queue** toolbar. On the appeared **Add Machines to Queue** dialog `Pic 3` you can choose domains/workgroups or individual PCs where search should be performed and press **OK** button to fill the **Machine Queue**.
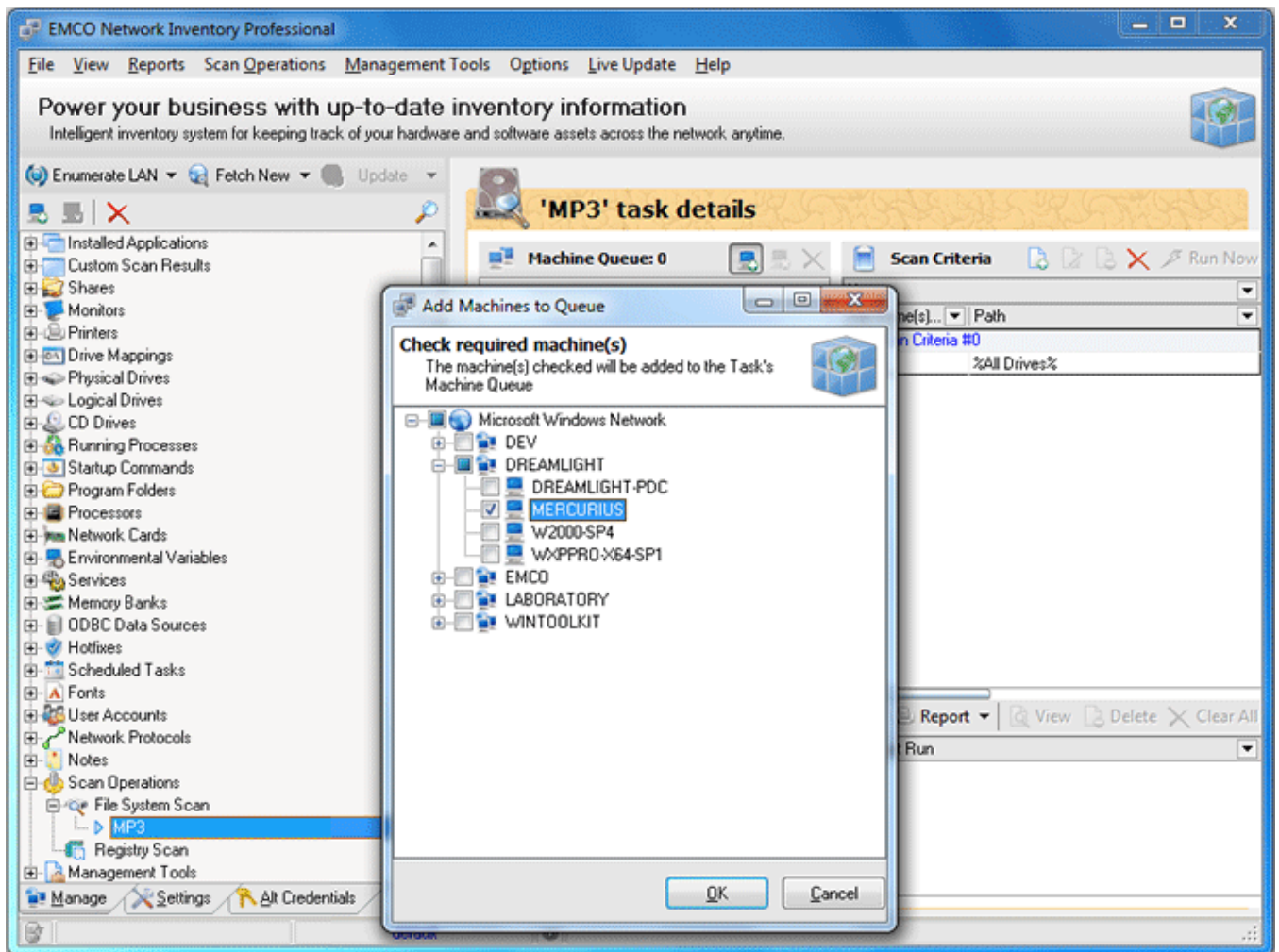
Pic 3. Add Machines to Queue dialog

When search conditions and **Machine Queue** are configured, you can launch the search by pressing **Run Now** button on the toolbar. After scan completion you can see search results below. `Pic 4` To get a detailed report about resources found, you can click on the row in the search results.
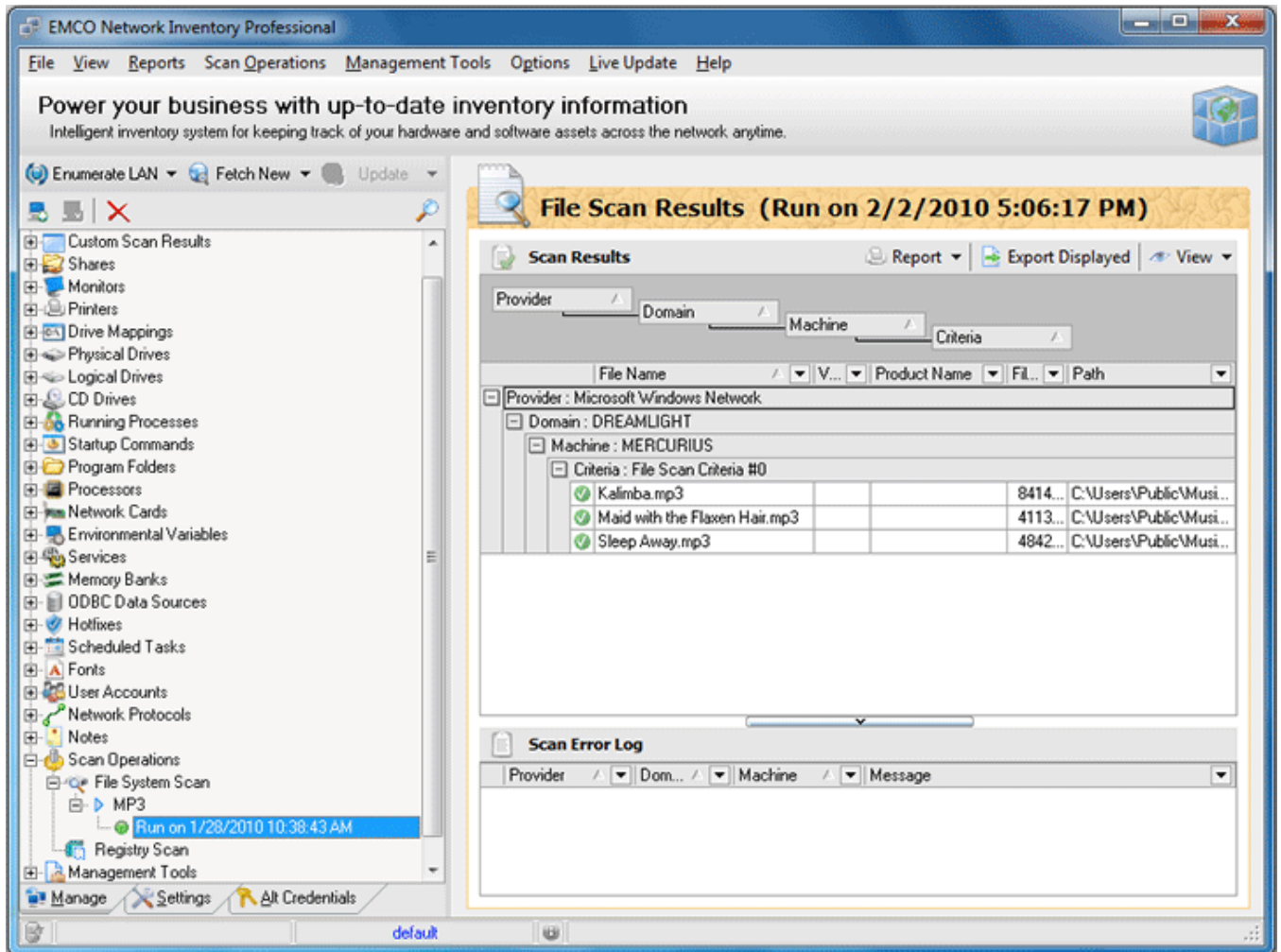
Pic 4. File System Scan results

Now you are familiar with **File System Scan** and you can use it any way and any time you need.

Chapter 4: Network Management

Network Inventory interaction with network is designed in a way that makes it fast and easy to search for Machines all over the network and collect inventory information for them. Network Inventory saves the network structure in its database along with inventory data and represents it in a form of a tree.

This chapter's target is to get you know how to review the information from this representation, manage it and what can be done over network elements available for you from the **Machine Tree**.

What's Inside

Machine Tree

Enumerating Network Automatically

Fetching new Machines

Adding Machines Manually

Machine Tree

The **Machine Tree** is located on the left of the main application screen under the **Manage** tab and consists of grouping nodes that allow you to browse inventory information fast and easy. The main node that contains all the information inside is the **Entire Network** node. It contains the Machines found during the Enumeration, fetched or added manually. The child nodes of each Machine are the nodes representing inventory information about this Machine. Pic 1
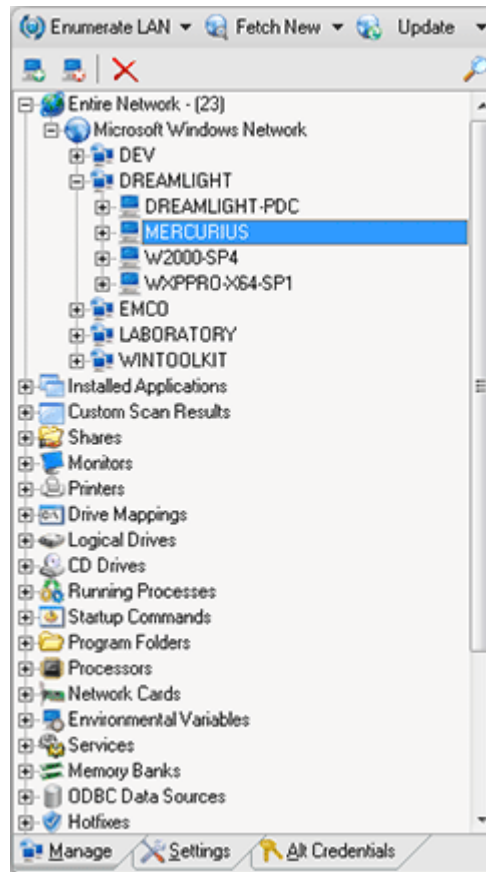
Pic 1. Machine Tree

It is not always comfortable to see all inventory information under each Machine that is why the other grouping nodes, except the **Entire Network**, are also present to show the individual accept of the data collected for each Machine. For example, selecting the Machine under the **Monitors** node gives you the same information as selecting the **Monitors** node under this Machine within the **Entire Network** node. This is very useful feature if you want to browse just particular inventory information for all the Machines.

There are also additional management nodes in the **Machine Tree** to be used for **Custom Scan** functionality and _Management Tools_ node containing the short cuts to the installed applications exclude list and the error log.

Enumerating Network Automatically

Network Inventory comes with a built-in network scan engine that allows you to scan an entire network for available Machines with just one click. It is possible to enumerate domain or workgroup, just some IP range from a group or the whole network. There are four possible ways of enumeration and all of them are described in this chapter.

> 💡 Enumeration means full rescan of the specified enumeration scope (network or group) so the Machines not found during re-enumeration are deleted from the **Machine Tree** along with there data. If you have already enumerated the network and just want to add more Machines that are now available on the network but not available in Network Inventory use **Fetch New** feature.

Enumerate All

Enumerate All means scanning whole network for the available Machines. To start such a enumeration process press **Enumerate LAN** button on the tool bar above the **Machine Tree**. When the enumeration completes the Machines found are displayed in the **Machine Tree** grouped by workgroups and domains. `Pic 1`
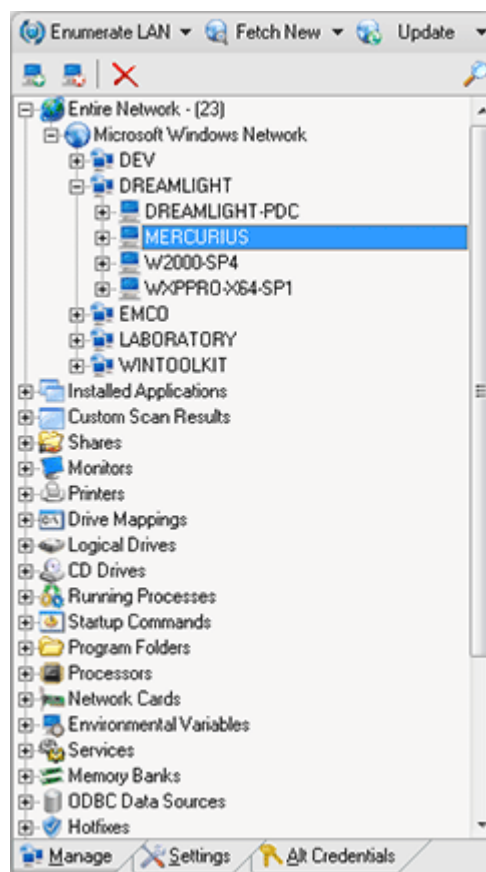
**Pic 1. Enumeration results for the whole network**

Enumerate Selected

Enumerate Selected feature should be used to rescan for Machines only the selected group. To perform such enumeration select the group within the **Machine Tree** and select **Enumerate Selected** from the drop-down options of **Enumerate LAN** button on the tool bar above the **Machine Tree**.
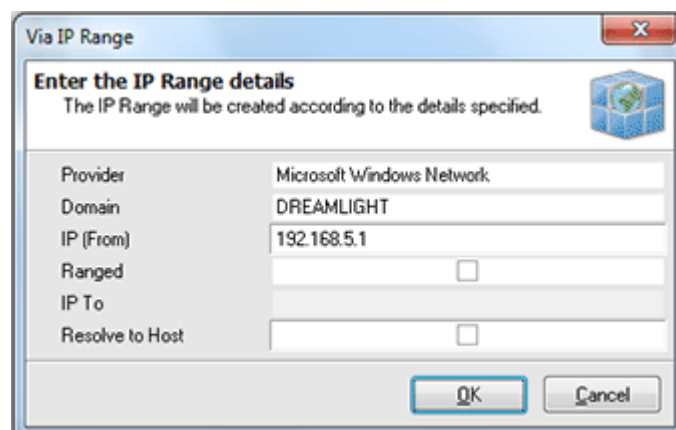
Enumerate via IP Range

If the target is to retrieve only the Machines with a specific IP addresses from a workgroup or domain the **Enumerate via IP Range** feature should be used. To enumerate a specific range select **Enumerate via IP Range** option from the drop-down options of **Enumerate LAN** button on the tool bar above the **Machine Tree**. The **Enum Via IP Range** dialog will appear on the screen. `Pic 2`
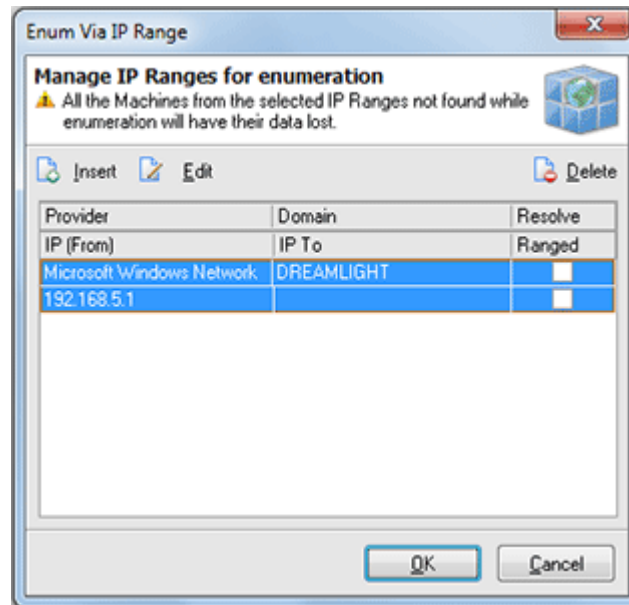
Pic 2. Specifying IP Ranges to enumerate

Within the **Enum Via IP Range** dialog you are to specify the IP Ranges to be used for enumeration. To add an IP Range press **Insert** button on the tool bar over the ranges list. The **Via IP Range** dialog will appear on the screen. `Pic 3`


Pic 3. Specifying enumeration settings for an individual IP Range

The **Via IP Range** dialog allows you to specify the domain or workgroup the IP range belongs to along with the Network Provider and the starting IP address. You can specify if the IP addresses to process is ranged and if so than provide the ending IP. It is also possible to resolve the IP addresses to host names. Press **OK** button to add the range.

You can add as many ranges as you want and then press **OK** button to proceed with enumeration.

Enumerate via Domain

With Network Inventory it is also possible to scan only a specific domain or workgroup for Machines. This goal can be reached using the **Enumerate via Domain** functionality. To proceed with such enumeration choose **Enumerate via Domain** option from the drop-down options of **Enumerate LAN** button on the tool bar above the **Machine Tree**. The **Enumerate via Domain** dialog will appear on the screen. `Pic 4`
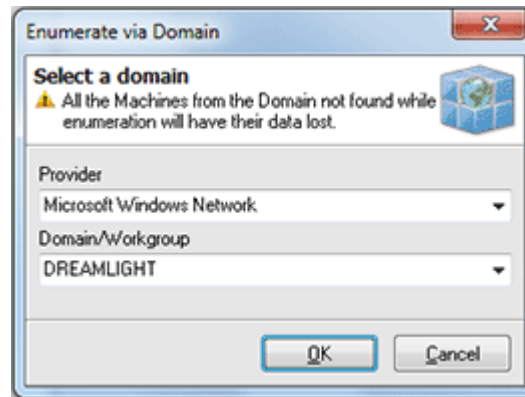
Pic 4. Specifying the group to enumerate

In the **Enumerate via Domain** dialog you are to specify the group to enumerate along with the network provider it belongs to. After you have specified the required information press **OK** button to proceed.
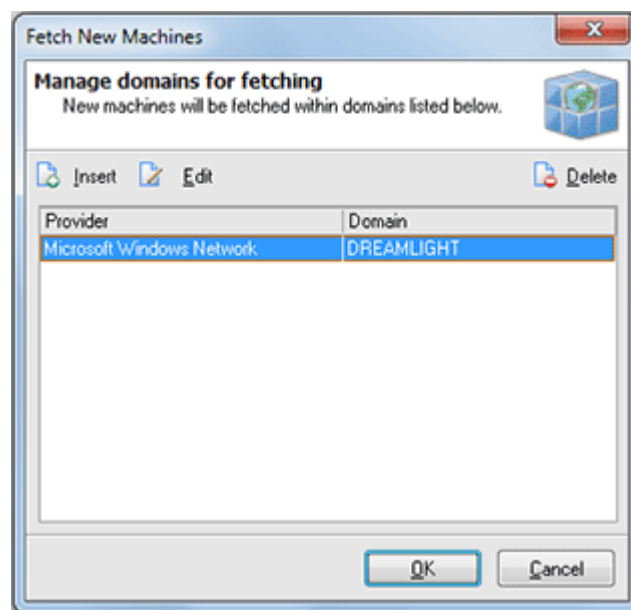
Fetching new Machines

Network Inventory along with the network enumeration provides you with an ability of scanning the whole network or specific groups for the newly added Machines, those that are not available in the **Machine Tree**, without loosing inventory information on the Machines that are not reachable now. This approach is reached using the **Fetch New** feature. You can always review the latest fetched machines using the appropriate node in the **Machine Tree**. There are two possible ways of searching for new Machines and both of them are described in this chapter.
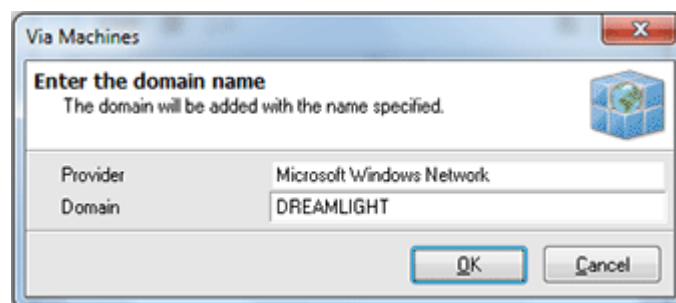
Fetch New

The **Fetch New** option allows you to search for new Machines within specific groups. To perform such kind of a search press **Fetch New** button on the tool bar above the **Machine Tree**. The **Fetch New Machines** dialog will appear on the screen. `Pic 1`

Pic 1. Specifying the groups to fetch new Machines from

In the **Fetch New Machines** dialog it is possible to specify the groups to fetch new Machines from. To add a group to scan press **Insert** button on the tool bar above the groups list. The **Via Machines** dialog will appear on the screen. `Pic 2`


Pic 2. Adding a group to fetch new Machines from

A group name along with a network provider are to be specified to add a new group into fetching process. After the required data is specified press **OK** button to proceed. The group is now added to the list of groups to fetch new Machines from. You can add as many groups as you want. When you are done press **OK** button to proceed with fetching.

After the fetch process is complete the Machines fetched will be available in the **Machine Tree**.

Fetch New via IP Range

Sometimes you face the situation when you do not need to fetch all the Machines from the network but only some of them. In such a case you can use **Fetch New via IP Range** feature. To use such kind of search choose **Fetch New via IP Range** option from the drop-down options of **Fetch New** button on the tool bar above the **Machine Tree**. The **Fetch New via IP Range** dialog will appear on the screen to specify the ranges to use. Pic 3
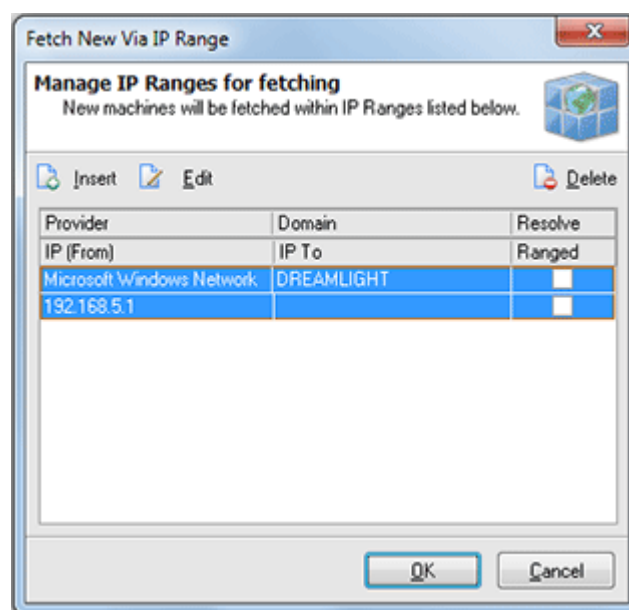
Pic 3. Specifying the IP Ranges to be used in Machines search

In the **Fetch New via IP Range** dialog you are to specify the ranges of IP addresses to be used in search. You can add as many ranges as needed. To add a range press **Insert** button above the ranges list. The **Via IP Range** dialog will appear on the screen. Pic 4
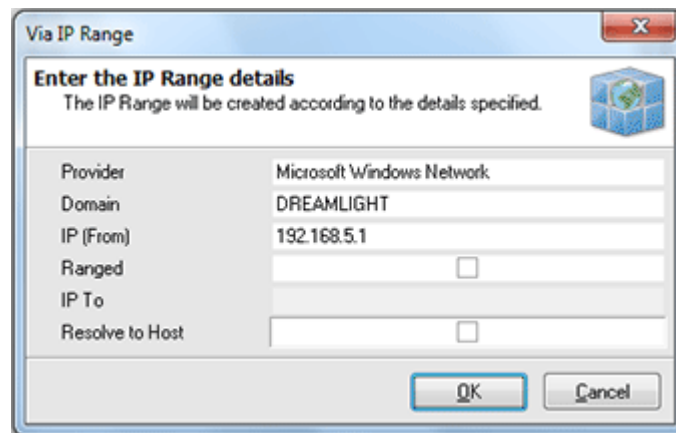

Pic 4. Specifying an individual IP Range to take part in Machines search

The **Via IP Range** dialog allows you to specify the domain or workgroup the IP range belongs to along with the Network Provider and the starting IP address. You can specify if the IP addresses to process is ranged and if so than provide the ending IP. It is also possible to resolve the IP addresses to host names. Press **OK** button to add the range.

When you have added all the ranges needed press **OK** button to proceed with the search.

Latest Fetched Machines

With Network Inventory you can always see the Machines that were fetched lately. These information is displayed within the **Latest Fetched Machines** dialog. `Pic 5` This dialog by default groups the Machines fetched by a fetching date but you can change the grouping any way you want.
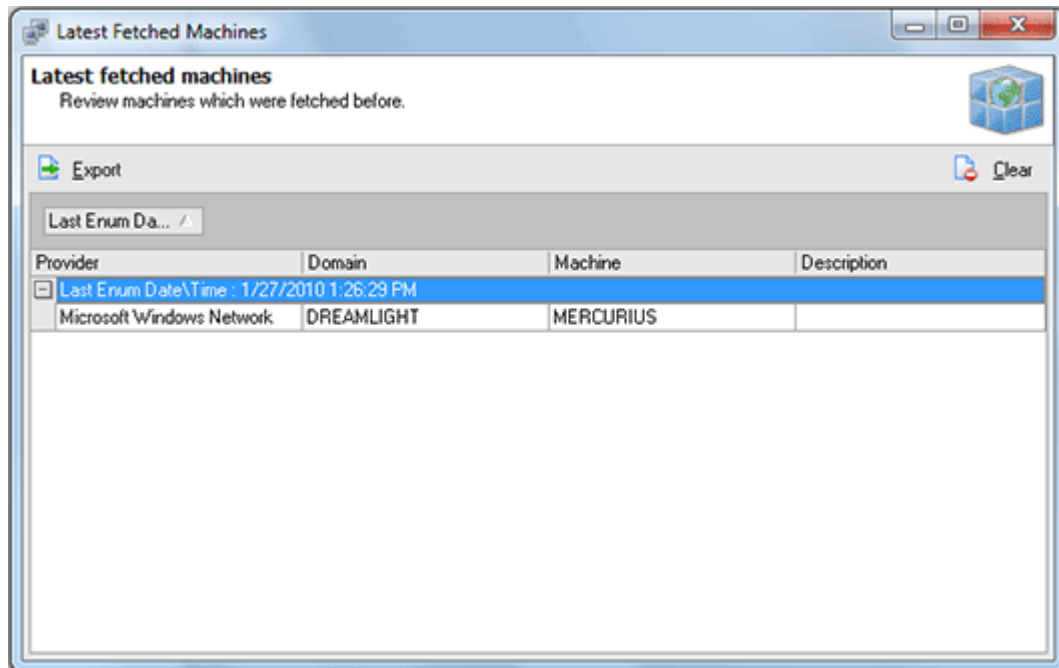

Pic 5. Latest fetched Machines

To reach the **Latest Fetched Machines** dialog you can select **Management Tools > Latest Fetched Machines** menu item from the application main menu or choosing the **Latest Fetched Machines** node in the **Machine Tree**.

Adding Machines Manually

If network scan is not a convenient way of adding Machines to the **Machine Tree** Network Inventory provides you with an ability of adding Machines manually. To add Machines in such a way press **Add Machine(s)** button from the tool bar above the **Machine Tree**. The **Add Machine(s)** dialog will appear on the screen. `Pic 1`
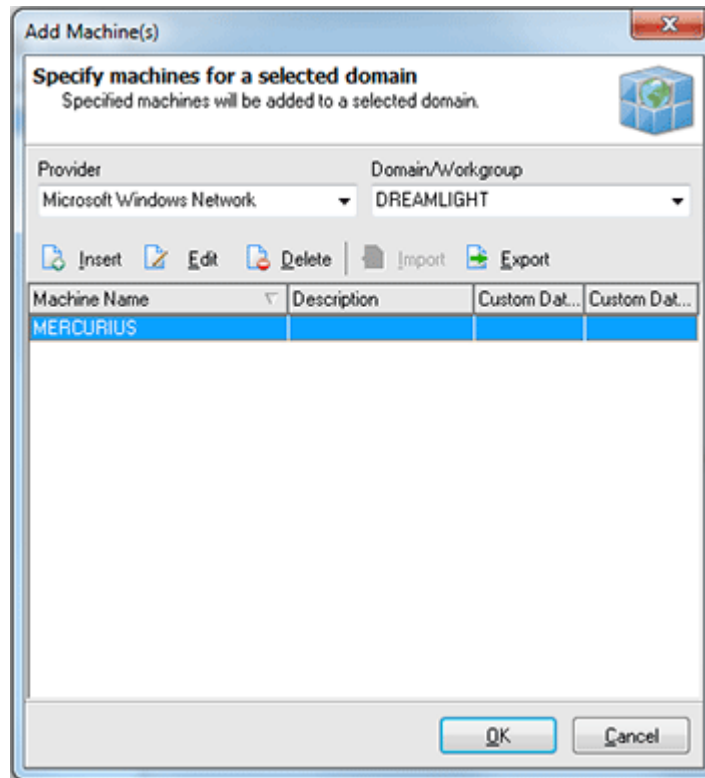
Pic 1. Adding machines manually

In the **Add Machine(s)** dialog you can add as many Machines as you wish one by one or import the list of Machines from a file to the specified group. To add a single Machine press **Insert** button above the Machines list. The **Add Machine** dialog will appear on the screen. `Pic 2`
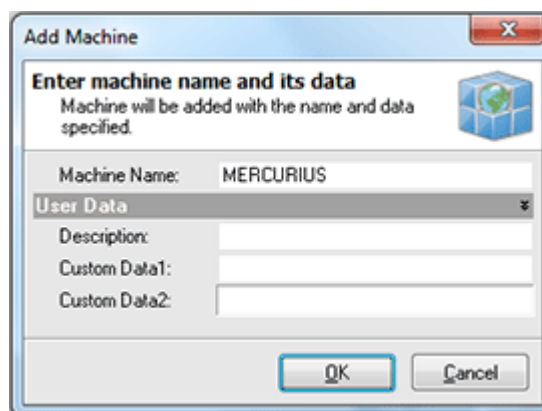
Pic 2. Adding a single Machine

The **Add Machine** dialog allows you to specify the Machine host name to add and its description.

As it was mentioned earlier the other way of adding Machines is importing from a file. To import Machines press **Import** button on the tool bar above the Machines list. The dialog will open to browse to a file with a list of Machines.

When you are ready with filling the Machines list with Machines you want to add press **OK** button to proceed. Optionally you can export this list to a file for a further import using the **Export** button on the tool bar above the Machines list.

Removing red mark from manually added Machines

As Machines are added manually they are marked with a red cross – this means that these Machines were not scanned for inventory information. To remove this mark you should update these Machines. To update select these Machines in the **Machine Tree** and select **Update Offline Only** options from the drop-down of the **Update** button on the tool bar above the **Machine Tree**.

Chapter 5: Inventory Information Management

The main goal of Network Inventory is to help you collect inventory information all over the network with least effort. With Network Inventory it is possible to retrieve both software and hardware information from remote Machines along with system information. The options defining what to collect are specified on the **Settings** tab on the left of the main application screen. This chapter is describing the range of information that can be retrieved with the example of the retrieved one for each aspect.

What's Inside

Brief Scan

Network Inventory allows to retrieve a lot of inventory information of different kind. First of all we would like to introduce to you the brief scan options that allow to collect basic software, hardware and system information. The brief scan options are available on the **Settings** tab.

The **Brief Scan Options** consists of the Machine's MAC address, basic information about the mother board, memory, video system, operating system, BIOS and other. This chapter will describe the **Brief Scan Options** in details.

What's Inside

Basic Information

Basic information is Machine's name, MAC and IP addresses along with the group name the Machine belongs to. Optionally while editing the basic information it is possible to specify two custom fields and description for the Machine that can help you while the inventory process. To retrieve basic information about the Machine first of all check the **Basic Information** option on the **Settings** tab under the **Machine Information Scan Options**. Then select the Machines you want to retrieve basic info for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the basic information for the Machine by selecting it in the **Machine Tree**. Pic 1
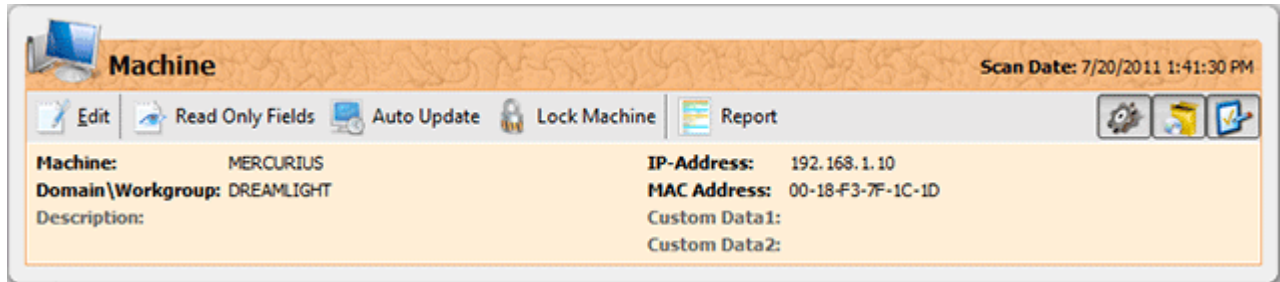
Pic 1. Basic information about the Machine

The basic information is displayed in an orange part of the Machine information area. You can edit this information using the **Edit** button on the management tool bar or create a report containing this information. While editing the basic information it is possible to specify two custom fields that can help you while the inventory process.

Summary Hardware Information

Summary Hardware information consists of basic mother board, memory and video system information. To retrieve basic hardware information about the Machine first of all check the **Summary Information** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve summary hardware information for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the summary hardware information for the Machine by selecting it in the **Machine Tree**. **Pic 1**

Pic 1. Summary hardware information about the Machine

The basic hardware information is displayed in a green part of the Machine information area. You can edit this information using the **Edit** button on the management tool bar or create a report containing this information.

It is also possible to expand and collapse this part using the glyph on its header or hide this part using the **Hide Hardware Information** button on the management tool bar.

Summary Software Information

Summary Software information consists of operating system information such as OS name, version, product key, language, default programs, etc. To retrieve basic software information about the Machine first of all check the **Summary Information** option on the **Settings** tab under the **Software Information Scan Options**. Then select the Machines you want to retrieve summary software information for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the summary software information for the Machine by selecting it in the **Machine Tree**. **Pic 1**
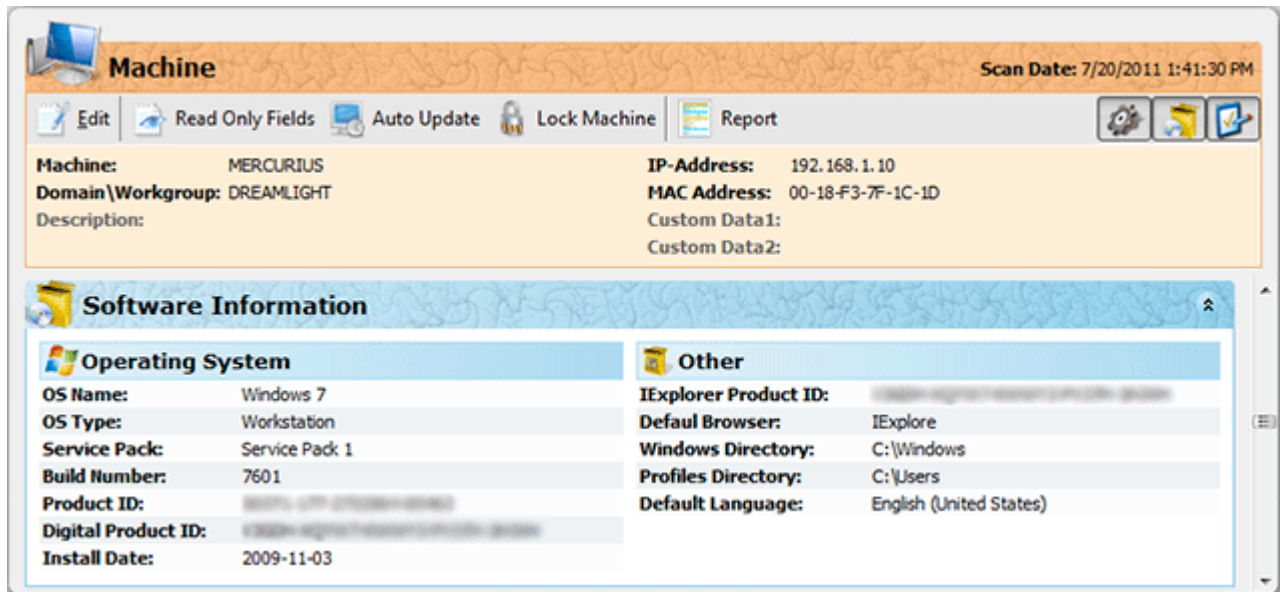

Pic 1. Summary software information about the Machine

The basic software information is displayed in a blue part of the Machine information area. You can edit this information using the **Edit** button on the management tool bar or create a report containing this information.

It is also possible to expand and collapse this part using the glyph on its header or hide this part using the **Hide Software Information** button on the management tool bar.

Summary System Information

Summary System information consists of BIOS information, information about the currently logged on user, if any, auto admin settings, etc. To retrieve basic system information about the Machine first of all check the **Summary Information** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve summary system information for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the Machine Tree. As soon as the update process completes you are about to see the summary system information for the Machine by selecting it in the **Machine Tree**.

Pic 1

Pic 1. Summary system information about the Machine

The basic system information is displayed in a peachy part of the Machine information area. You can edit this information using the **Edit** button on the management tool bar or create a report containing this information.

It is also possible to expand and collapse this part using the glyph on its header or hide this part using the **Hide System Information** button on the management tool bar.

Detailed Scan

Frequently basic information is not enough for inventory reports and EMCO fully understand this. That is why Network Inventory comes with a wide range of detailed scan options that allow you to collect almost everything about the software and hardware installed on remote Machines along with their configuration. All detailed scan options are located on the **Settings** tab. This part of the manual is to describe the range of detailed scan options and show you how much information can you include in your inventory reports without any serious effort.

What's Inside

Installed Applications

Application Updates

Shares

Monitors

Printers

Drive Mappings

Physical Drives

Logical Drives

CD Drives

Running Processes

Startup Commands

Program Folders

Processors

Network Cards

Environment Variables

Services

Memory Banks

ODBC Data Sources

Scheduled Tasks

Fonts

User Accounts

Network Protocols

Installed Applications

Network Inventory allows you to collect information on the applications installed on any Machine so you do not need to rewrite the whole list of applications from the Add/Remove Programs section of the Operating System during the inventory. To get a list of installed applications first of all check the **Installed Applications** option on the **Settings** tab under the **Software Information Scan Options**. Then select the Machines you want to retrieve installed applications list for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the installed applications list for the Machine by selecting its **Installed Applications** child node in the **Machine Tree**. Pic 1
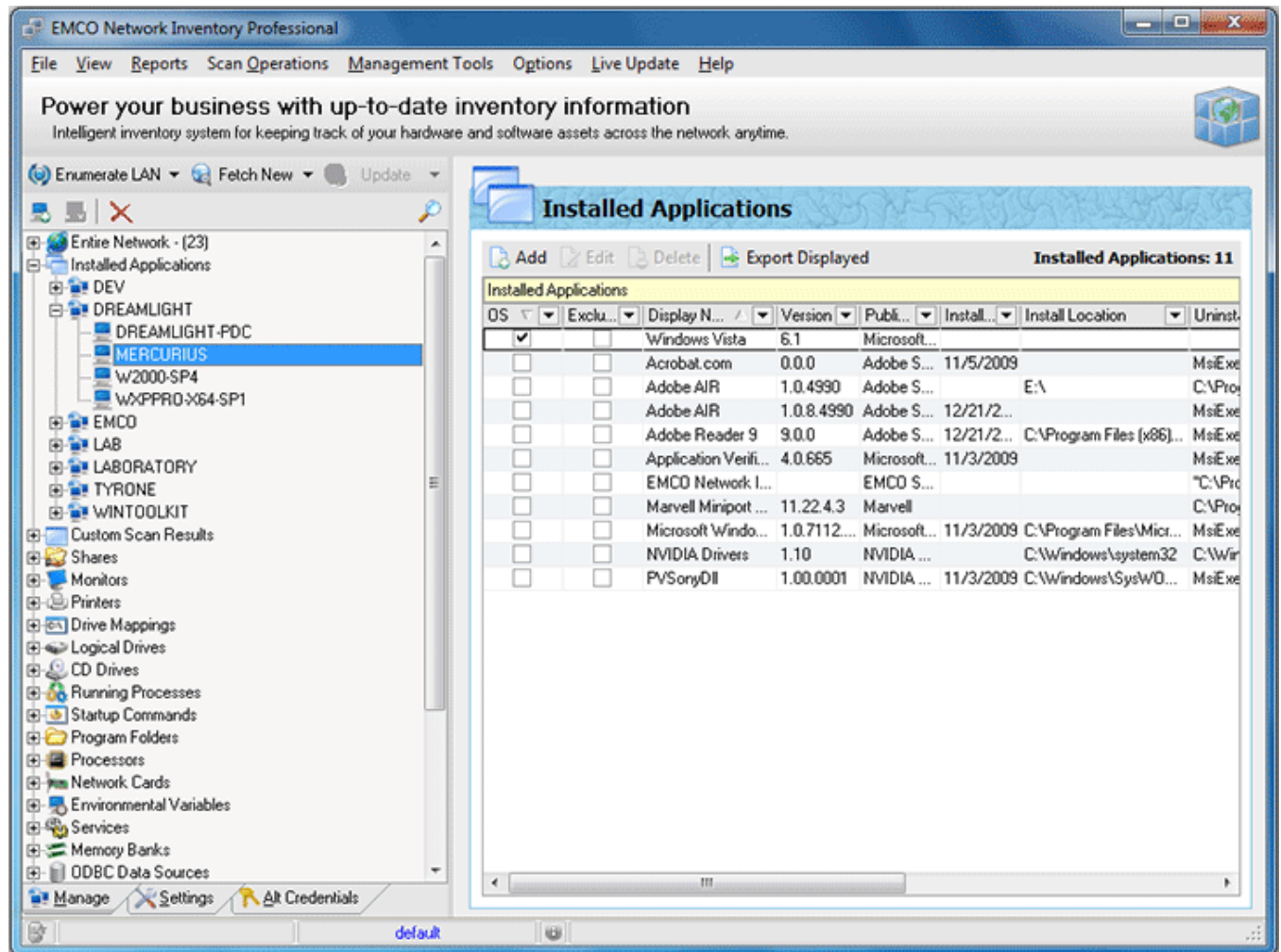
Pic 1. The list of installed applications for the Machine

You can add applications to this list manually, remove the applications from this list, edit each application info, export this list to any format or create a report containing this information.

Application Updates

Network Inventory allows you to collect information on the application updates installed on any Machine. To get a list of application updates first of all check the **Application Updates** option on the **Settings** tab under the **Software Information Scan Options**. Then select the Machines you want to retrieve a list of application updates for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the application updates list for the Machine by selecting its **Application Updates** child node in the **Machine Tree**. **Pic 1**
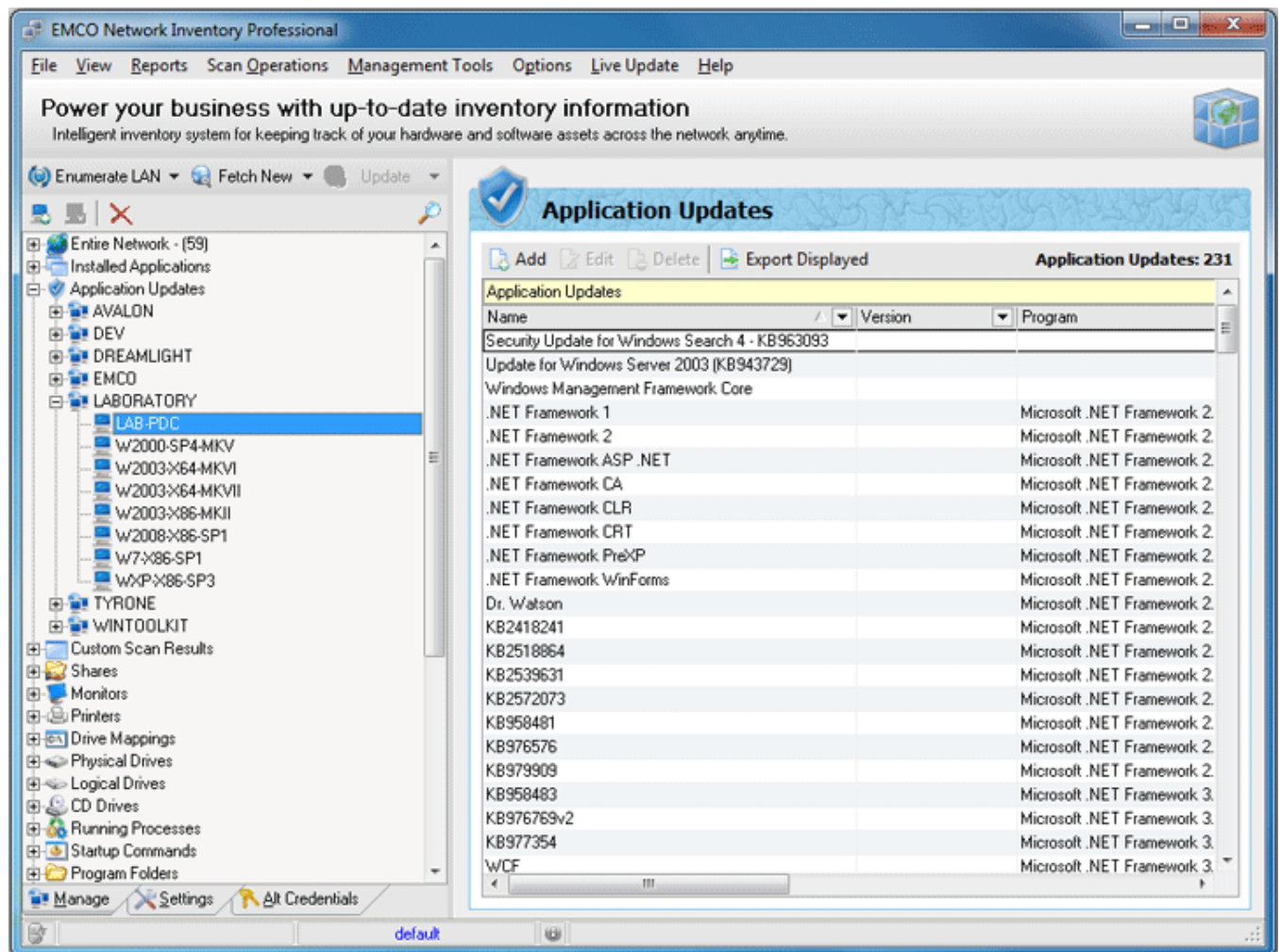
Pic 1. The list of application updates for the Machine

You can add a application update to this list manually, remove the application update from this list, edit application update info, export this list to any format or create a report containing this information.

Shares

Network Inventory allows you to collect information on the shares available on any Machine. To get a list of shares first of all check the **Shares** option on the **Settings** tab under the **System Information Scan Options** (optionally you can also check **Include Share Access** to retrieve access rights). Then select the Machines you want to retrieve shares list for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the shares list for the Machine by selecting its **Shares** child node in the **Machine Tree**. Pic 1

Pic 1. The list of shares for the Machine

You can add a share to this list manually, remove the share from this list, edit each share info, export this list to any format or create a report containing this information.

Monitors

Network Inventory allows you to collect information on the monitors available on any Machine. To get a list of monitors first of all check the **Monitors** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve monitors list for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the monitors list for the Machine by selecting its **Monitors** child node in the **Machine Tree**. Pic 1
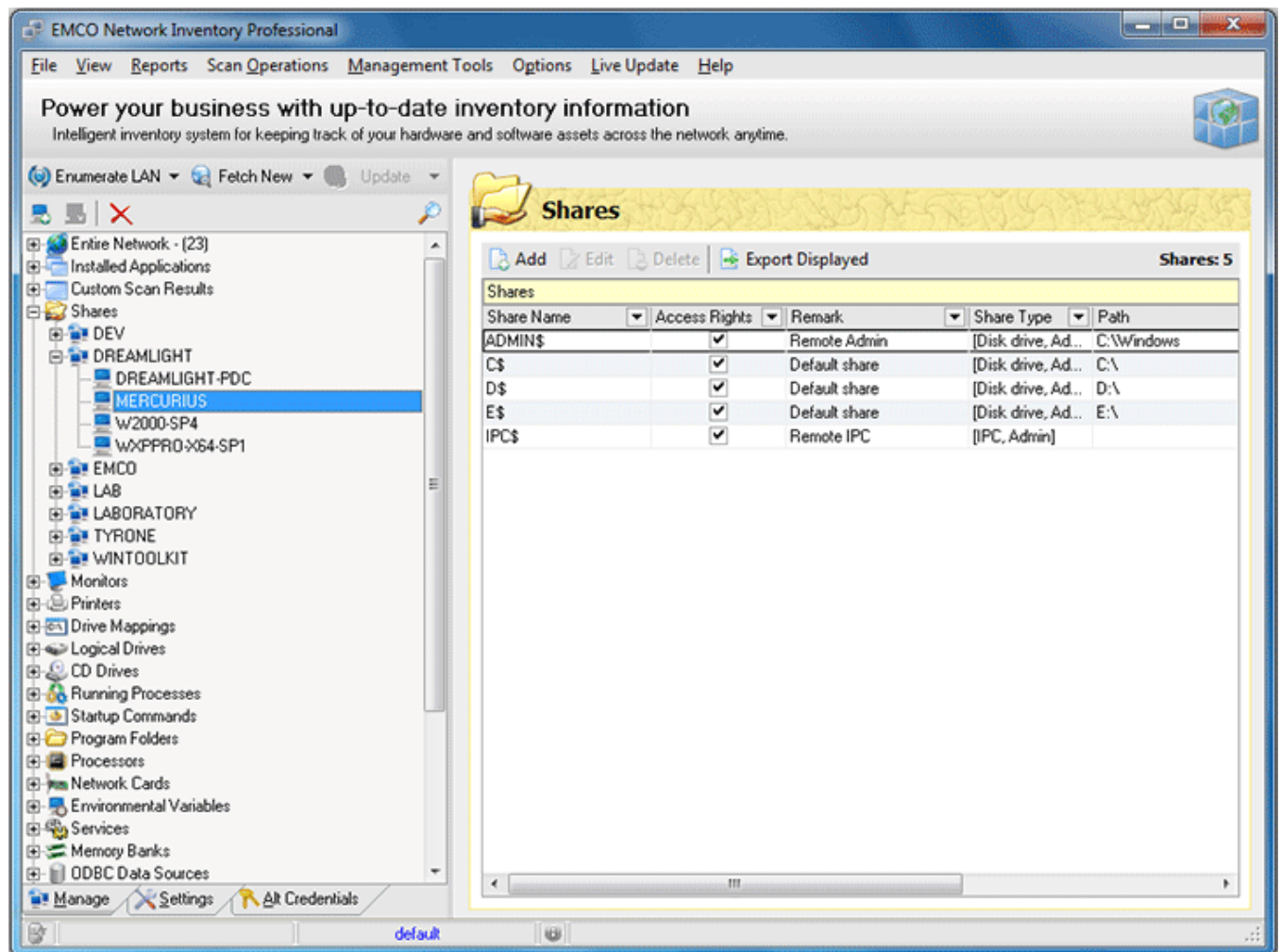

Pic 1. The list of monitors for the Machine

You can add a monitor to this list manually, remove the monitor from this list, edit each monitor info, export this list to any format or create a report containing this information.

Printers

Network Inventory allows you to collect information on the printers available on any Machine. To get a list of printers first of all check the **Printers** option on the **Settings** tab under the **Hardware Information Scan Options**. If you would like to include network printers to the inventory check **Include Network Printers** option. Then select the Machines you want to retrieve printers list for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the printers list for the Machine by selecting its **Printers** child node in the **Machine Tree**. Pic 1
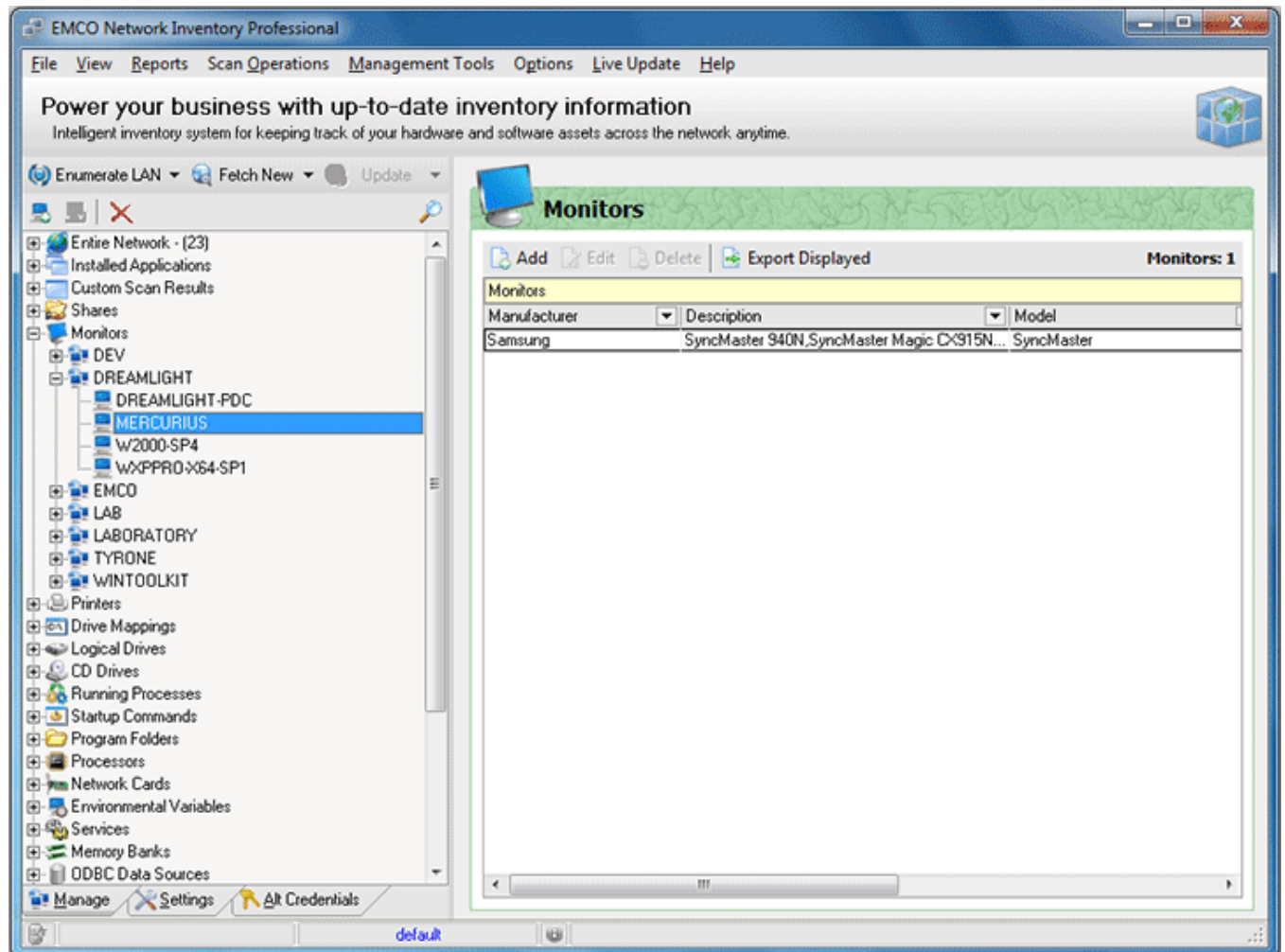

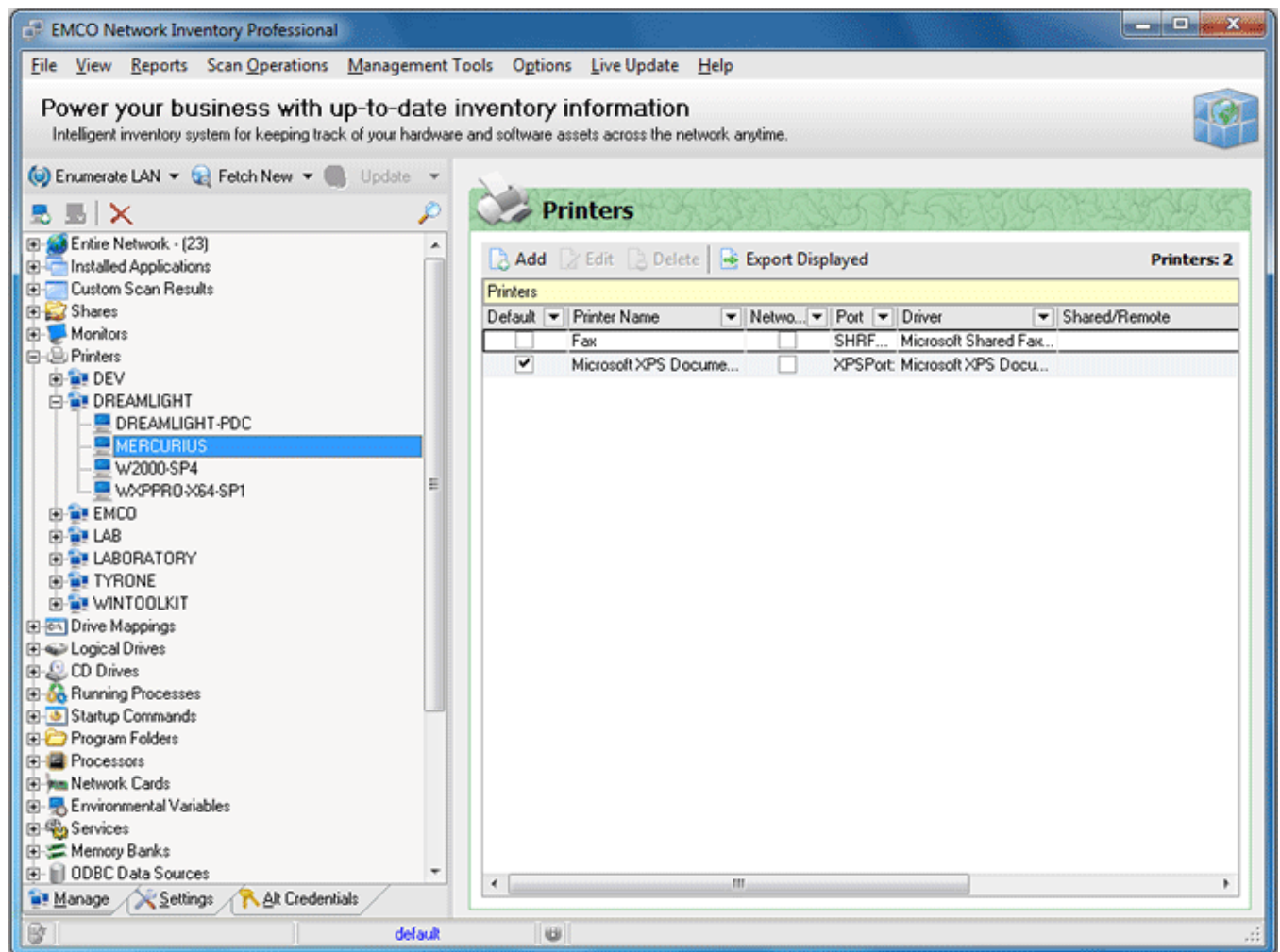**Pic 1. The list of printers for the Machine**

You can add a printer to this list manually, remove the printer from this list, edit each printer info, export this list to any format or create a report containing this information.

Drive Mappings

Network Inventory allows you to collect information on the drive mappings available on any Machine. To get a list of mapped network drives first of all check the **Drive Mappings** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of mapped drives for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the mapped drives list for the Machine by selecting its **Drive Mappings** child node in the **Machine Tree**. Pic 1

Pic 1. The list of mapped drives for the Machine

You can add a mapped drive to this list manually, remove the mapped drive from this list, edit each drive info, export this list to any format or create a report containing this information.

Physical Drives

Network Inventory allows you to collect information on the physical drives available on any Machine. To get a list of physical drives first of all check the **Physical Drives** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve a list of physical drives for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the physical drives list for the Machine by selecting its **Physical Drives** child node in the **Machine Tree**. **Pic 1**
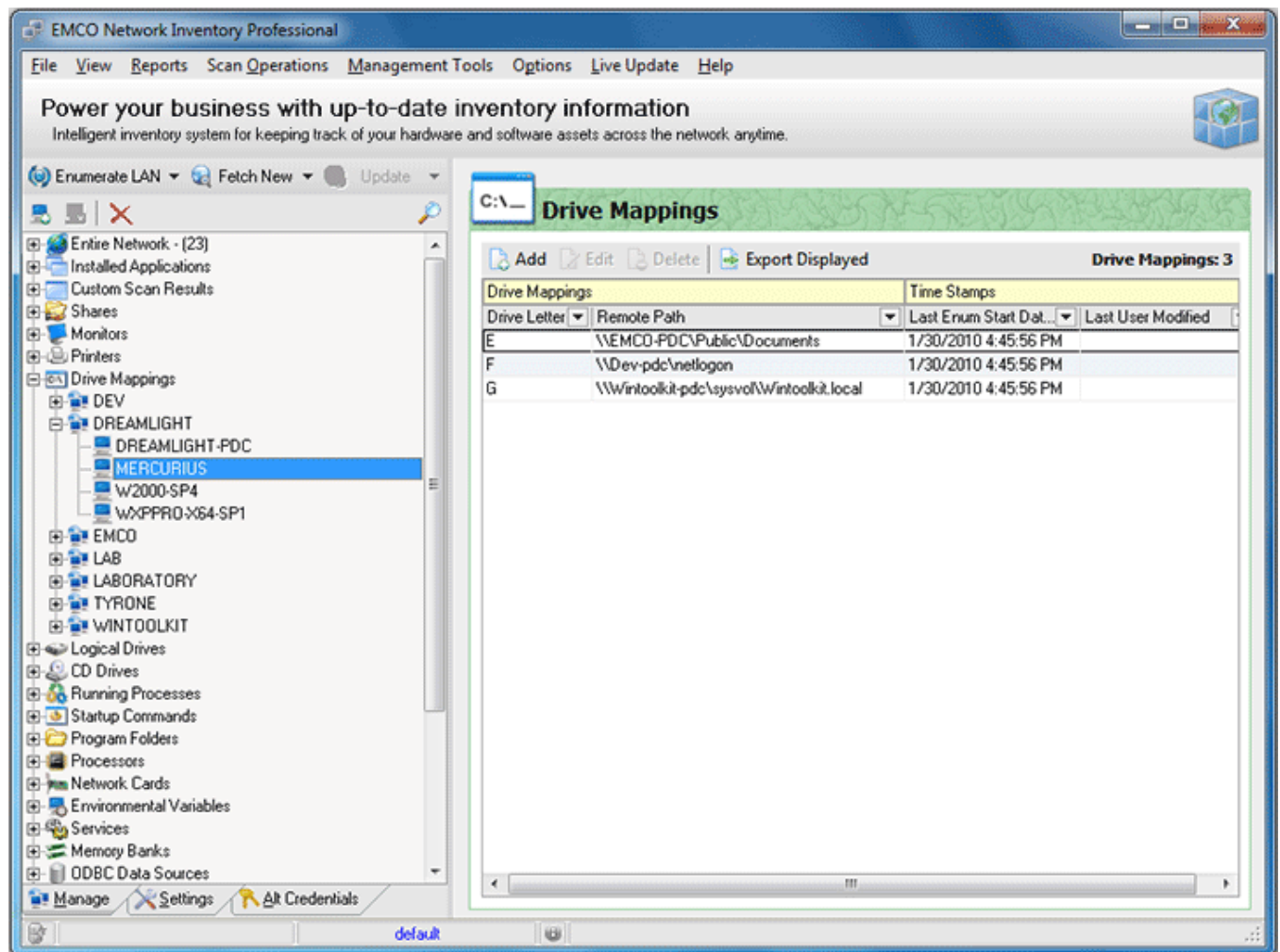

Pic 1. The list of Physical drives for the Machine

You can add a physical drive to this list manually, remove the physical drive from this list, edit each drive info, export this list to any format or create a report containing this information.

Logical Drives

Network Inventory allows you to collect information on the logical drives available on any Machine. To get a list of logical drives first of all check the **Logical Drives** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve a list of logical drives for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the Machine Tree. As soon as the update process completes you are about to see the logical drives list for the Machine by selecting its **Logical Drives** child node in the **Machine Tree**. Pic 1
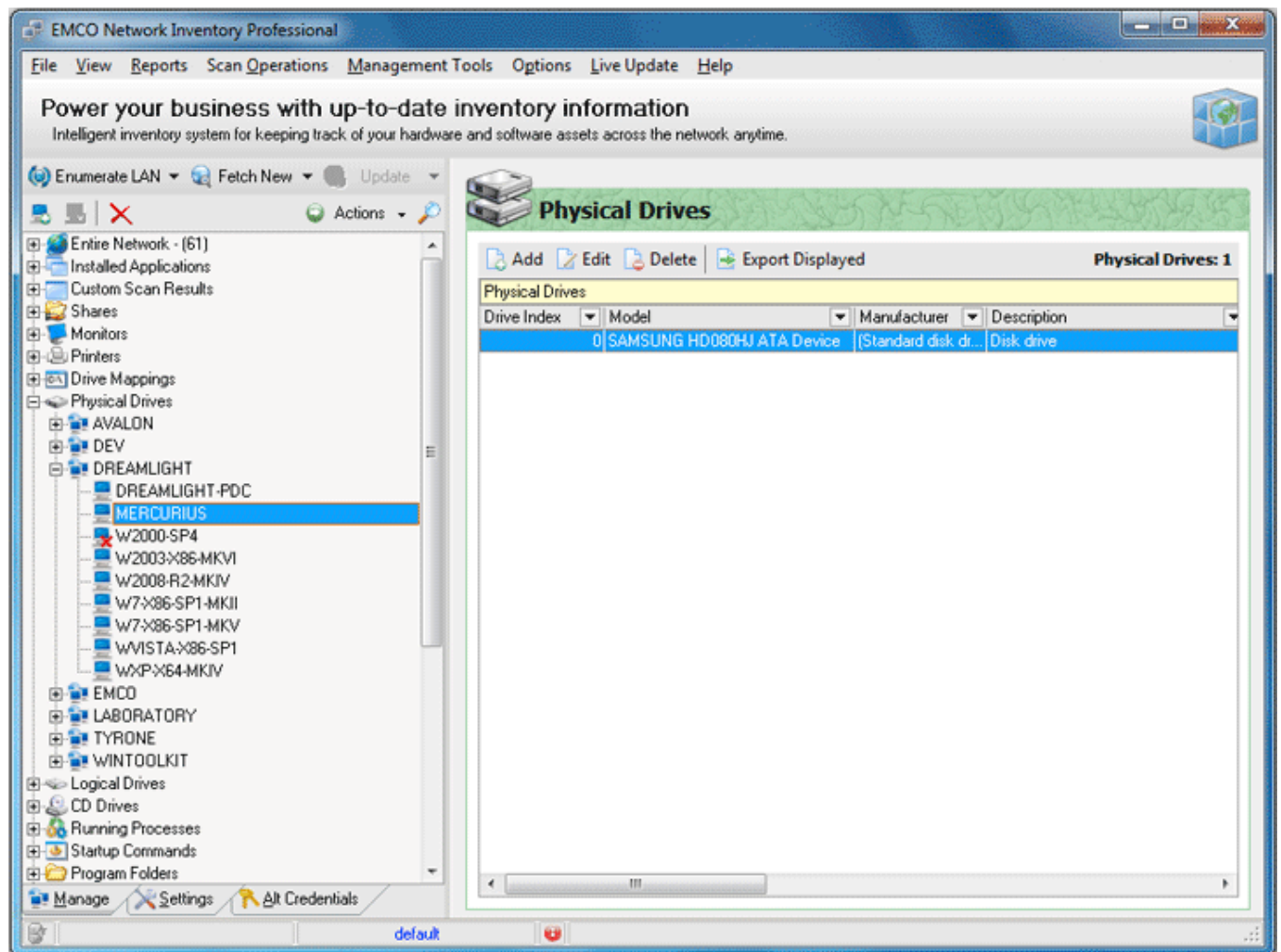

Pic 1. The list of logical drives for the Machine

You can add a logical drive to this list manually, remove the logical drive from this list, edit each drive info, export this list to any format or create a report containing this information.

CD Drives

Network Inventory allows you to collect information on the CD drives available on any Machine. To get a list of CD drives first of all check the **CD Drives** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve a list of CD drives for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the CD drives list for the Machine by selecting its **CD Drives** child node in the **Machine Tree**.
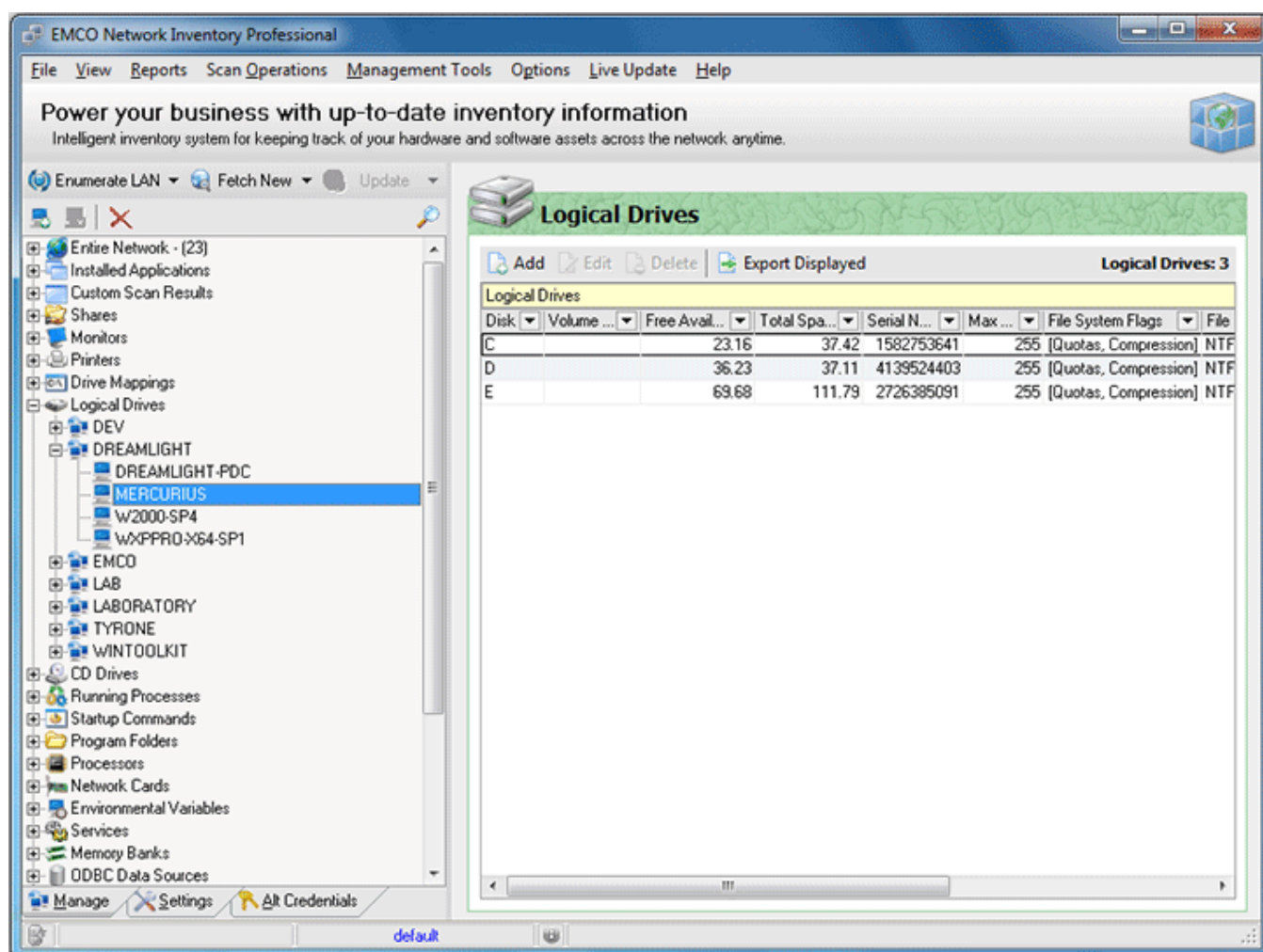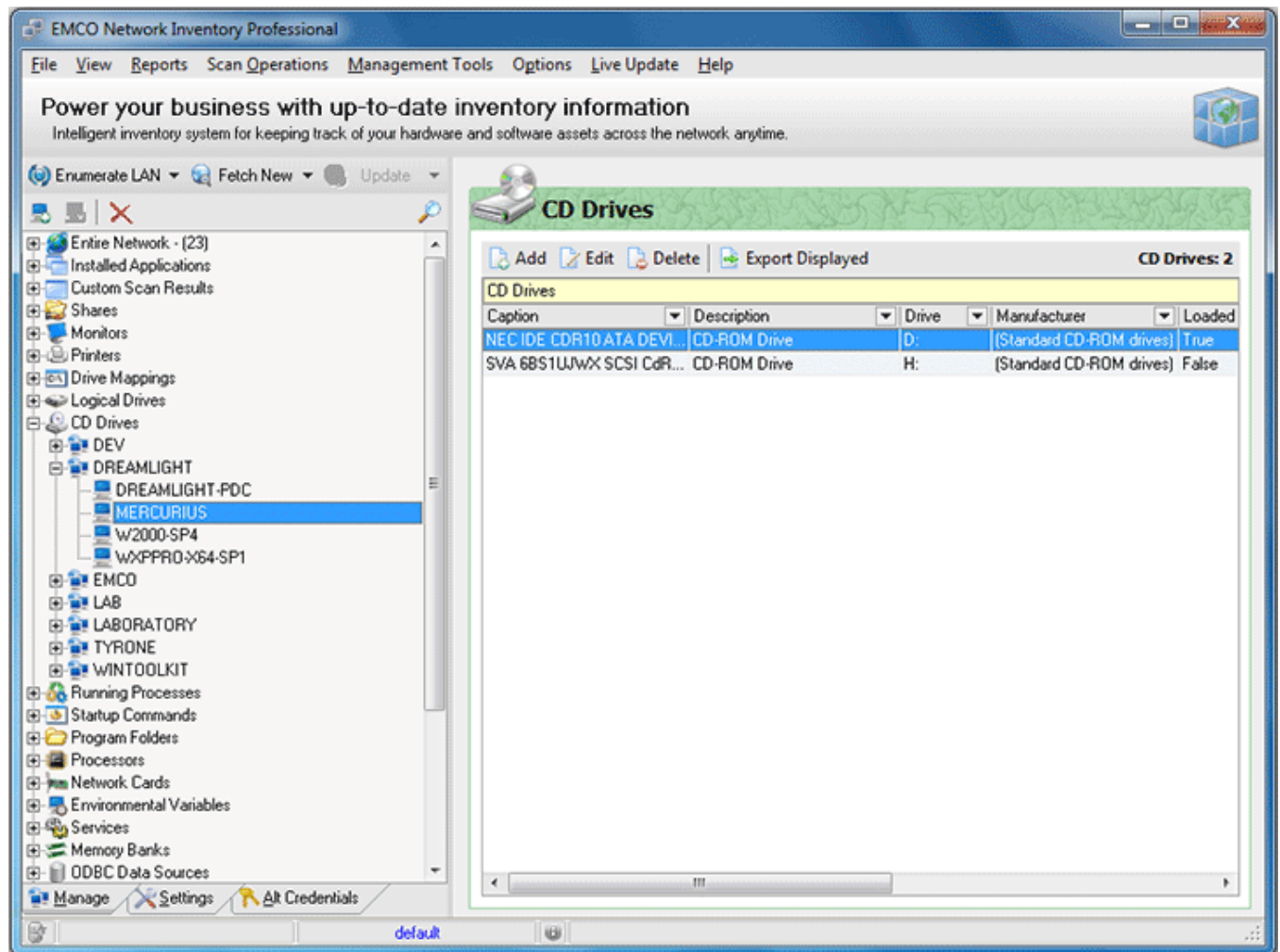**Pic 1**

Pic 1. The list of CD drives for the Machine

You can add a CD drive to this list manually, remove the CD drive from this list, edit each drive info, export this list to any format or create a report containing this information.

Running Processes

Network Inventory allows you to collect information on the processes running now on any Machine as you've made a screen shot with the Task Manager of the Operating System during the inventory. To get a list of running processes first of all check the **Processes** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of running processes for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the processes list for the Machine by selecting its **Running Processes** child node in the **Machine Tree**. `Pic 1`
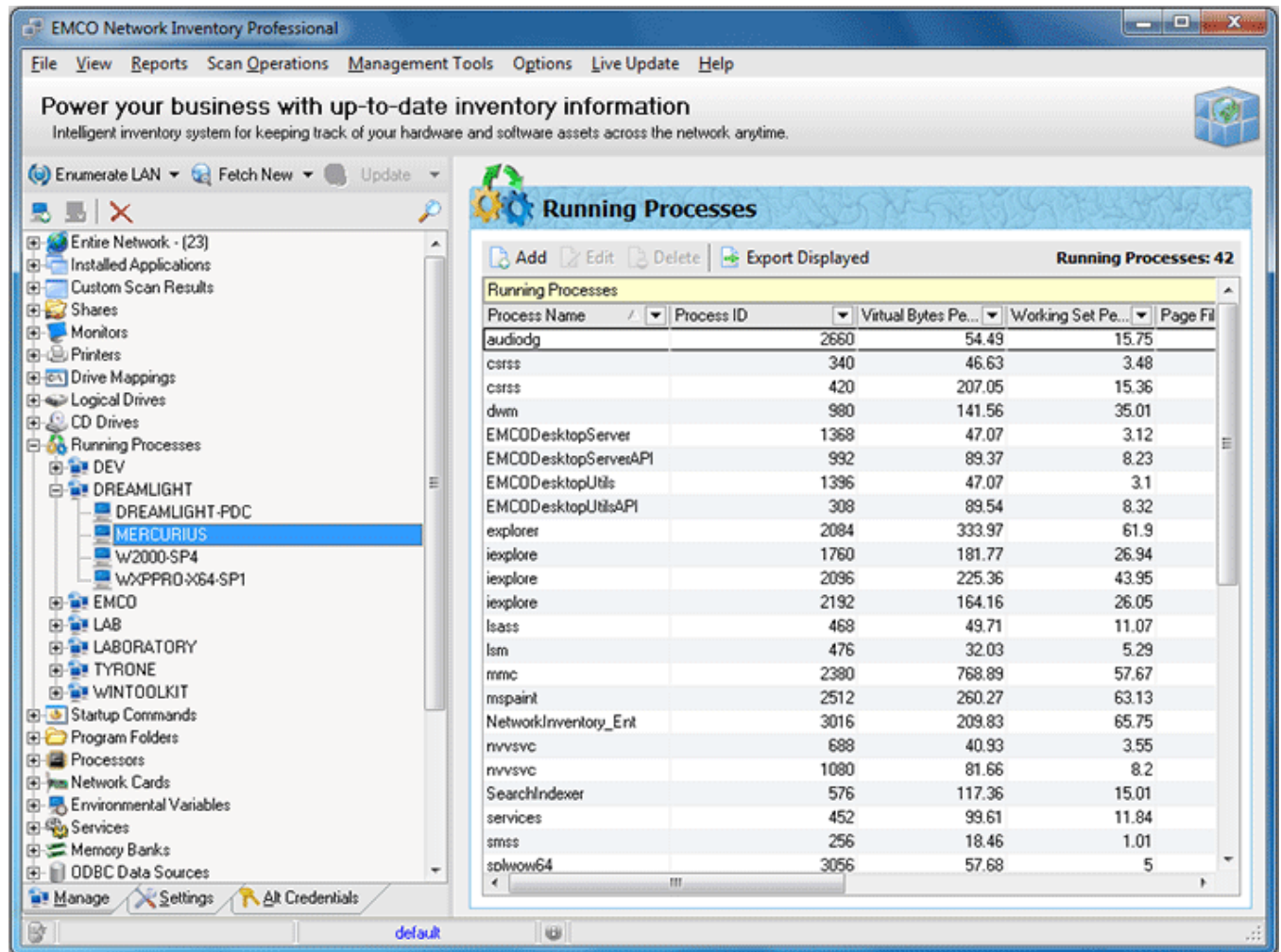
Pic 1. The list of running processes for the Machine

You can add a process to this list manually, remove the processes from this list, edit each each process info, export this list to any format or create a report containing this information.

Startup Commands

Network Inventory allows you to collect the commands to be run on the Operating System start up for any Machine. To get a list of startup commands first of all check the **Startup Commands** option on the **Settings** tab under the **System Information Scan Options**. If you also want to collect the information on the commands to be run for the currently logged on user, you should check **Current User** option under the **Startup Commands** one. Then select the Machines you want to retrieve a list of startup commands for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the startup commands list for the Machine by selecting its **Startup Commands** child node in the **Machine Tree**. Pic 1
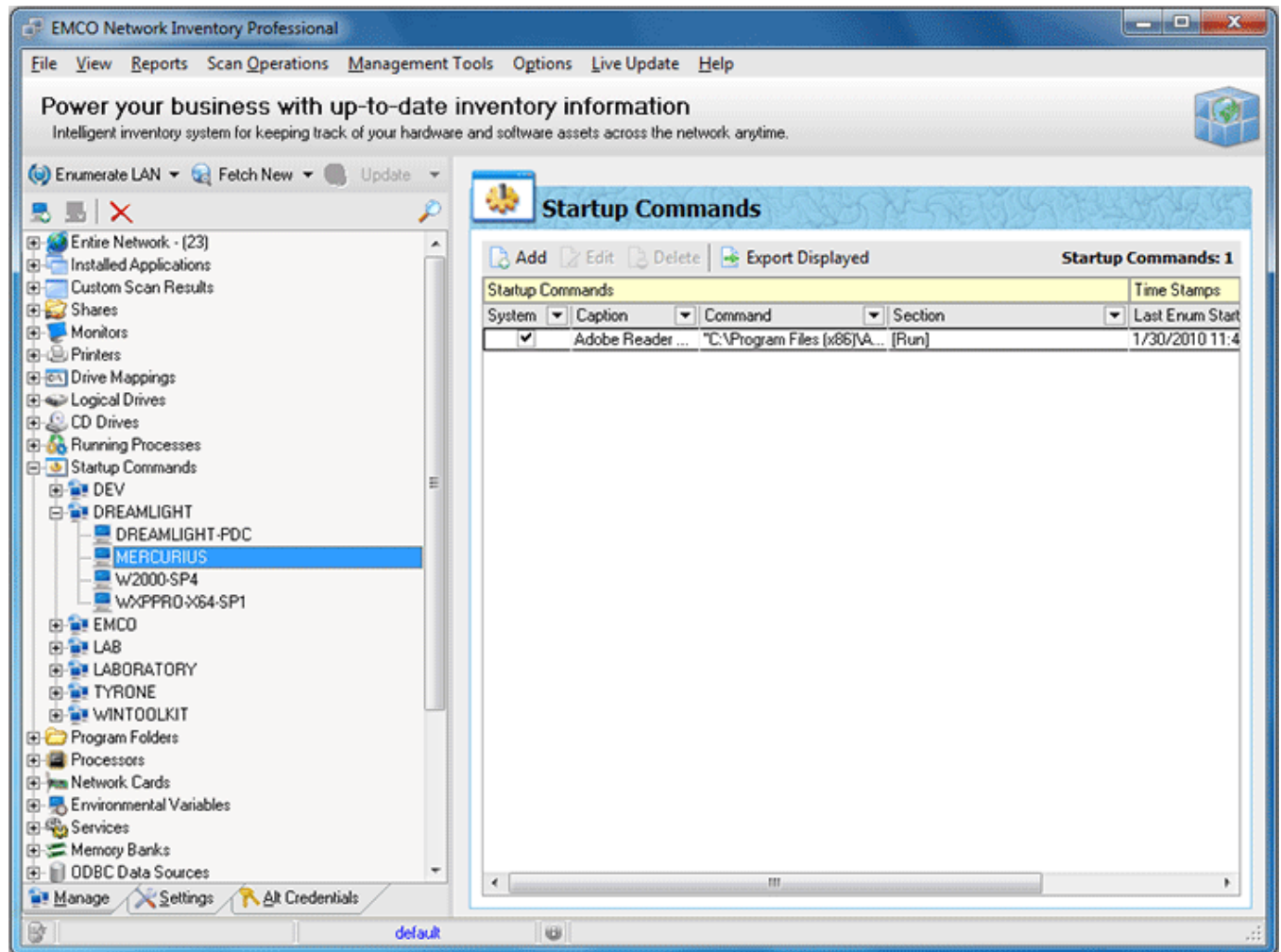

Pic 1. The list of startup commands for the Machine

You can add a startup command to this list manually, remove the startup command from this list, edit each command, export this list to any format or create a report containing this information.

Program Folders

Network Inventory allows you to collect information on the folders available from the Program Files folder of the operating system on any Machine. To get a list of program folders first of all check the **Program Folders** option on the **Settings** tab under the **Software Information Scan Options**. Then select the Machines you want to retrieve a list of program folders for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the program folders list for the Machine by selecting its **Program Folders** child node in the **Machine Tree**. Pic 1

Pic 1. The list of program folders for the Machine

You can add a folder to this list manually, remove the folder from this list, edit each program folder, export this list to any format or create a report containing this information.

Processors

Network Inventory allows you to collect information on the processors available on any Machine. To get a list of processors first of all check the **Processors** option on the **Settings** tab under the**Hardware Information Scan Options**. Then select the Machines you want to retrieve a list of processors for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the Machine Tree. As soon as the update process completes you are about to see the processors list for the Machine by selecting its **Processors** child node in the **Machine Tree**. Pic 1

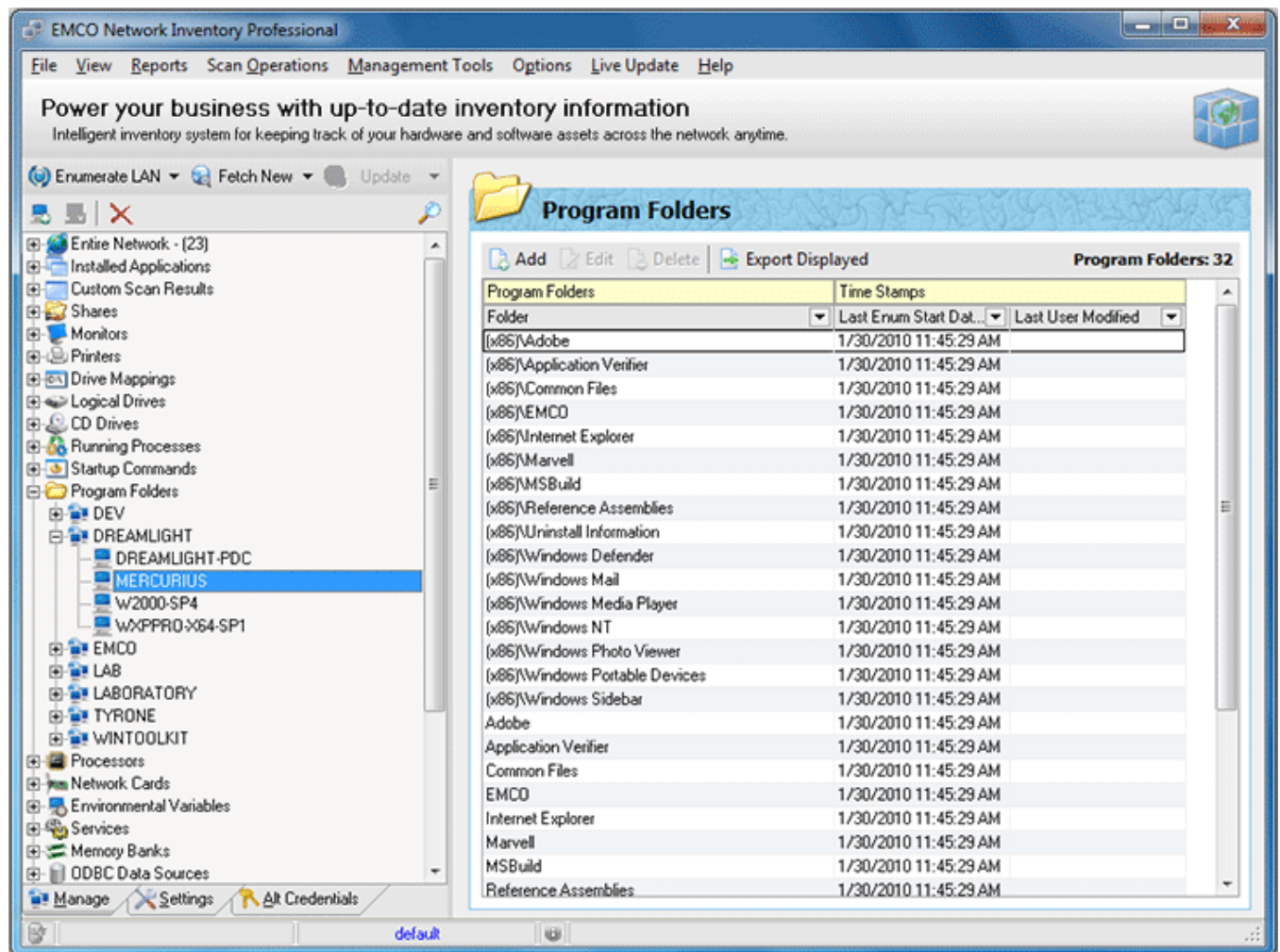**Pic 1. The list of processors for the Machine**

You can add a processor to this list manually, remove the processor from this list, edit processor info, export this list to any format or create a report containing this information.

Network Cards

Network Inventory allows you to collect information on the network cards available on any Machine. To get a list of network cards first of all check the **Network Cards** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve a list of network cards for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the network cards list for the Machine by selecting its **Network Cards** child node in the **Machine Tree**. `Pic 1`
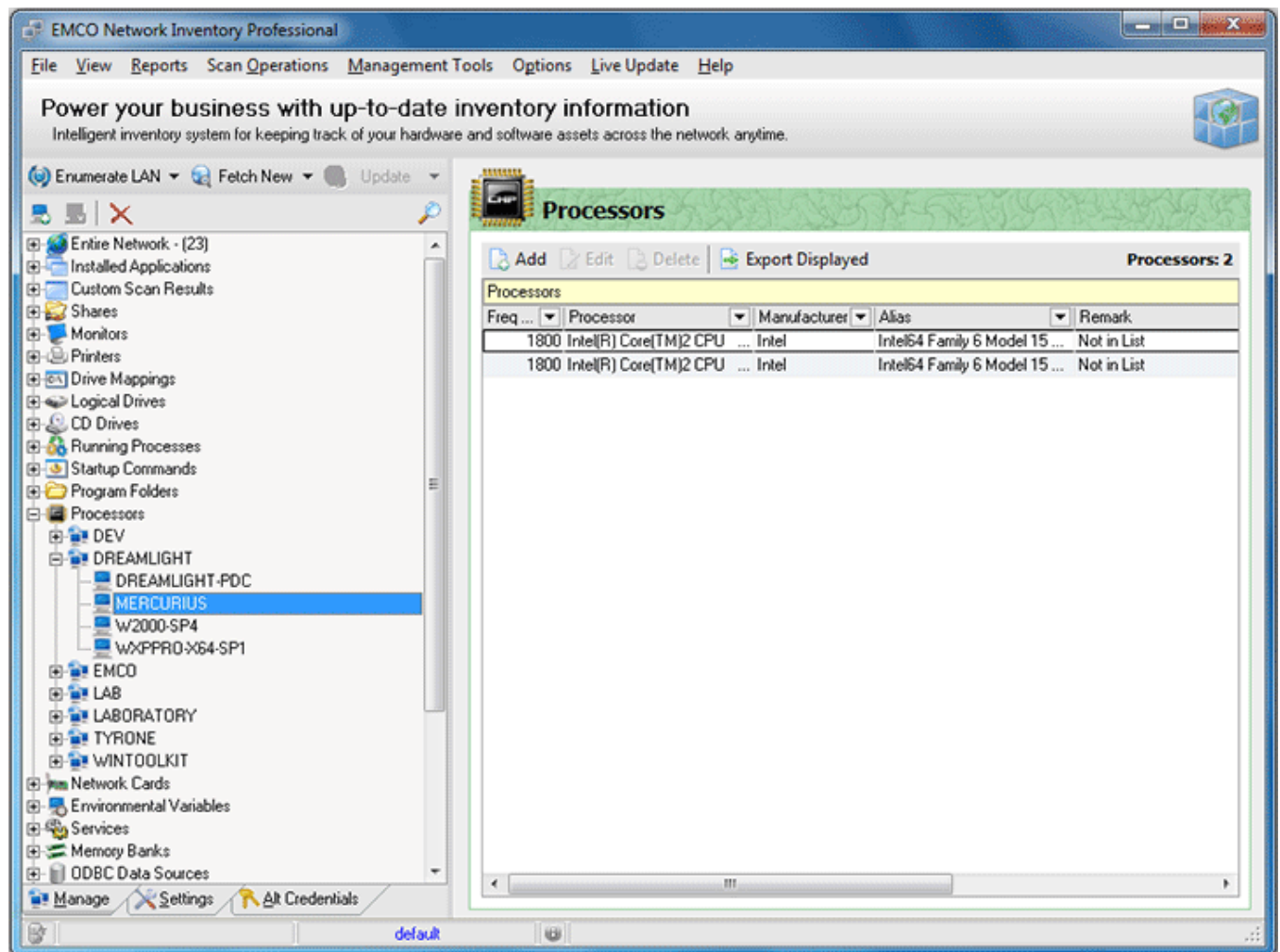

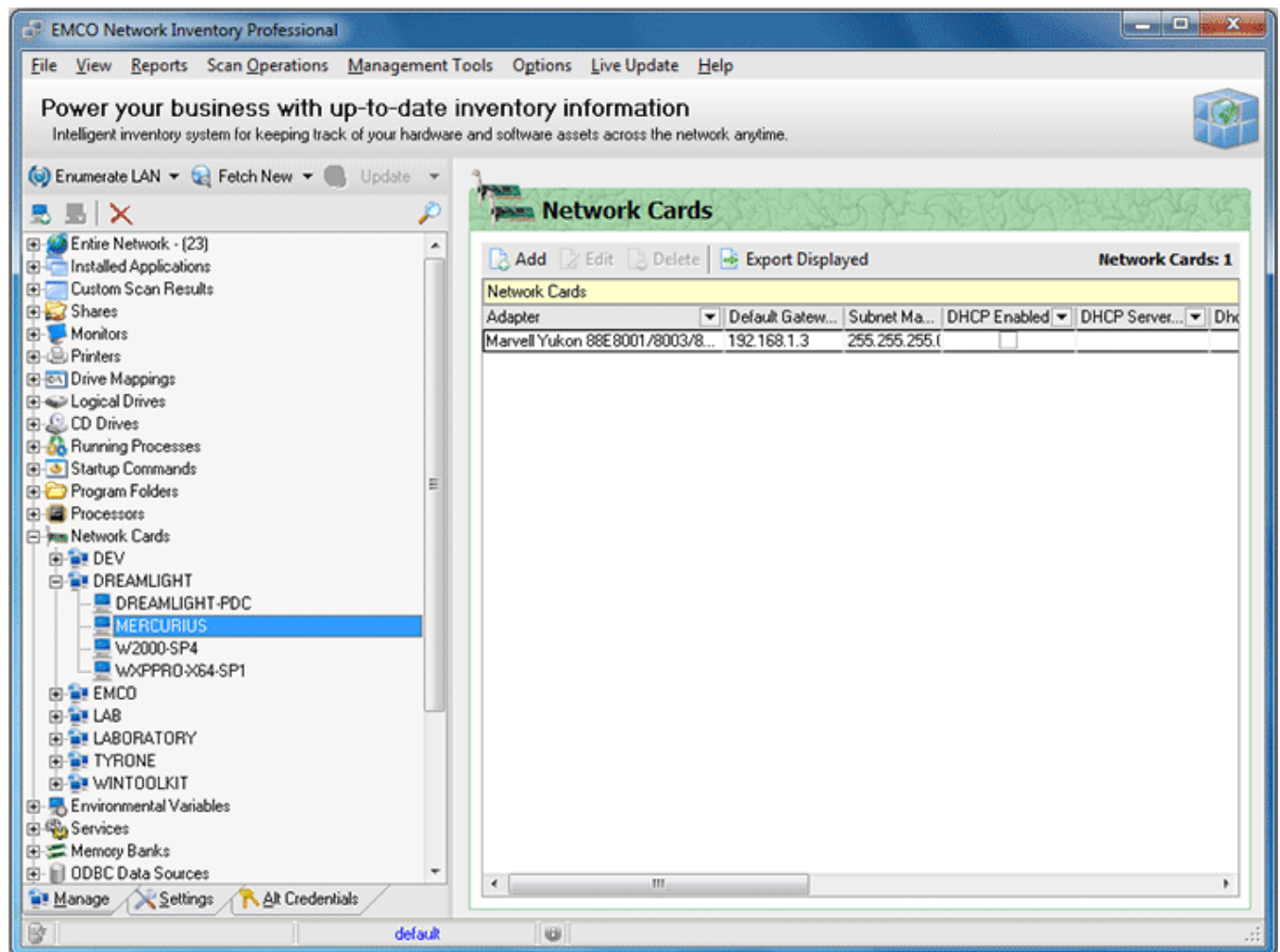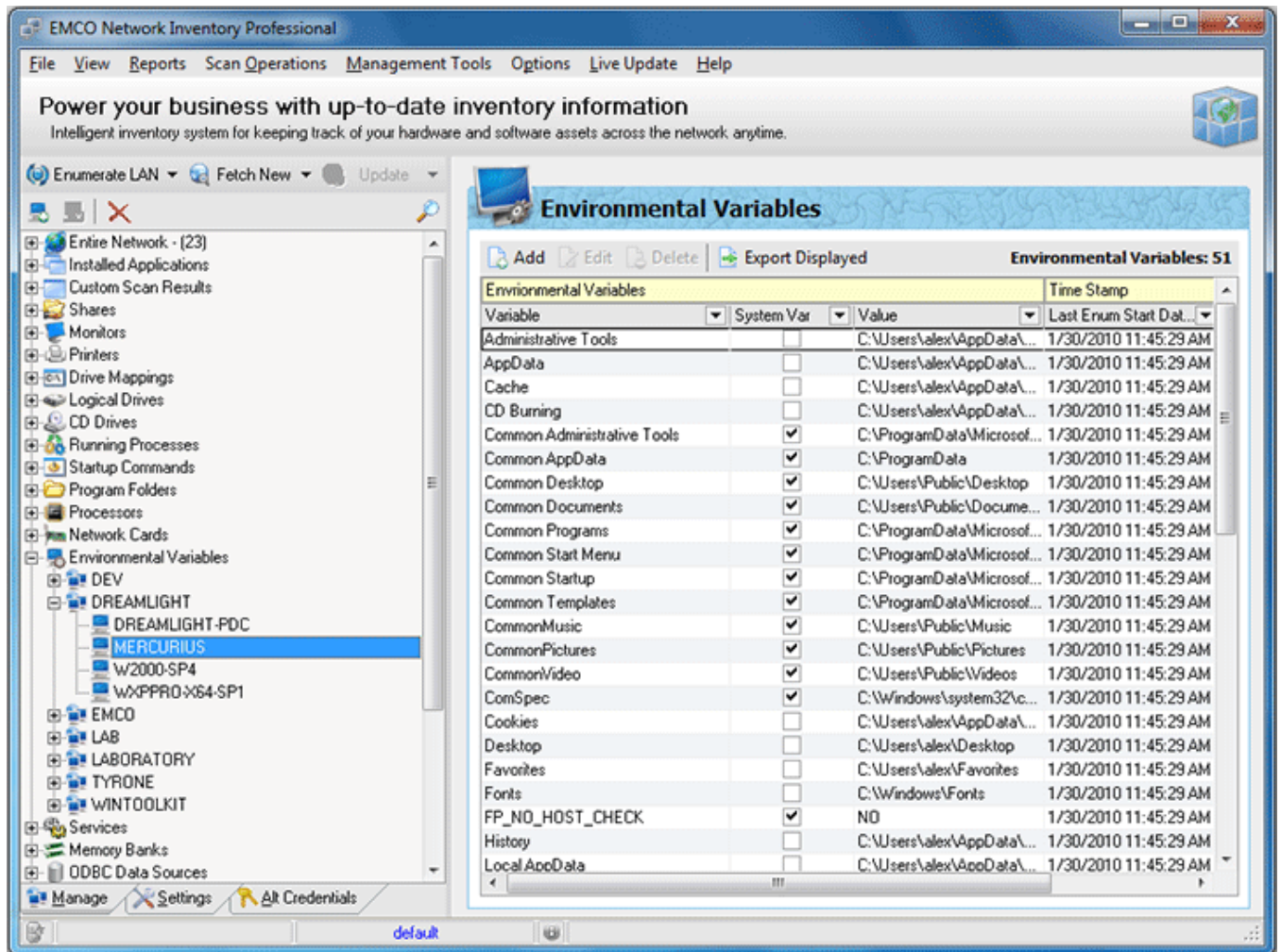
Pic 1. The list of network cards for the Machine

You can add a network card to this list manually, remove the network card from this list, edit network card info, export this list to any format or create a report containing this information.

Environment Variables

Network Inventory allows you to collect information on the environmental variables registered in the Operating System on any Machine. To get a list of environmental variables first of all check the **Environmental Variables** option on the **Settings** tab under the **System Information Scan Options**. If you want to collect also the variables for the currently logged on user and shell folders select the following options under the **Environmental Variables** one. Then select the Machines you want to retrieve a list of environmental variables for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the environmental variables list for the Machine by selecting its **Environmental Variables** child node in the **Machine Tree**. Pic 1


Pic 1. The list of environmental variables for the Machine

You can add a environmental variable to this list manually, remove the environmental variable from this list, edit each variable, export this list to any format or create a report containing this information.

Services

Network Inventory allows you to collect information on the services registered in the Operating System on any Machine. To get a list of services first of all check the **Services** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of services for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the services list for the Machine by selecting its **Services** child node in the **Machine Tree**. `Pic 1`
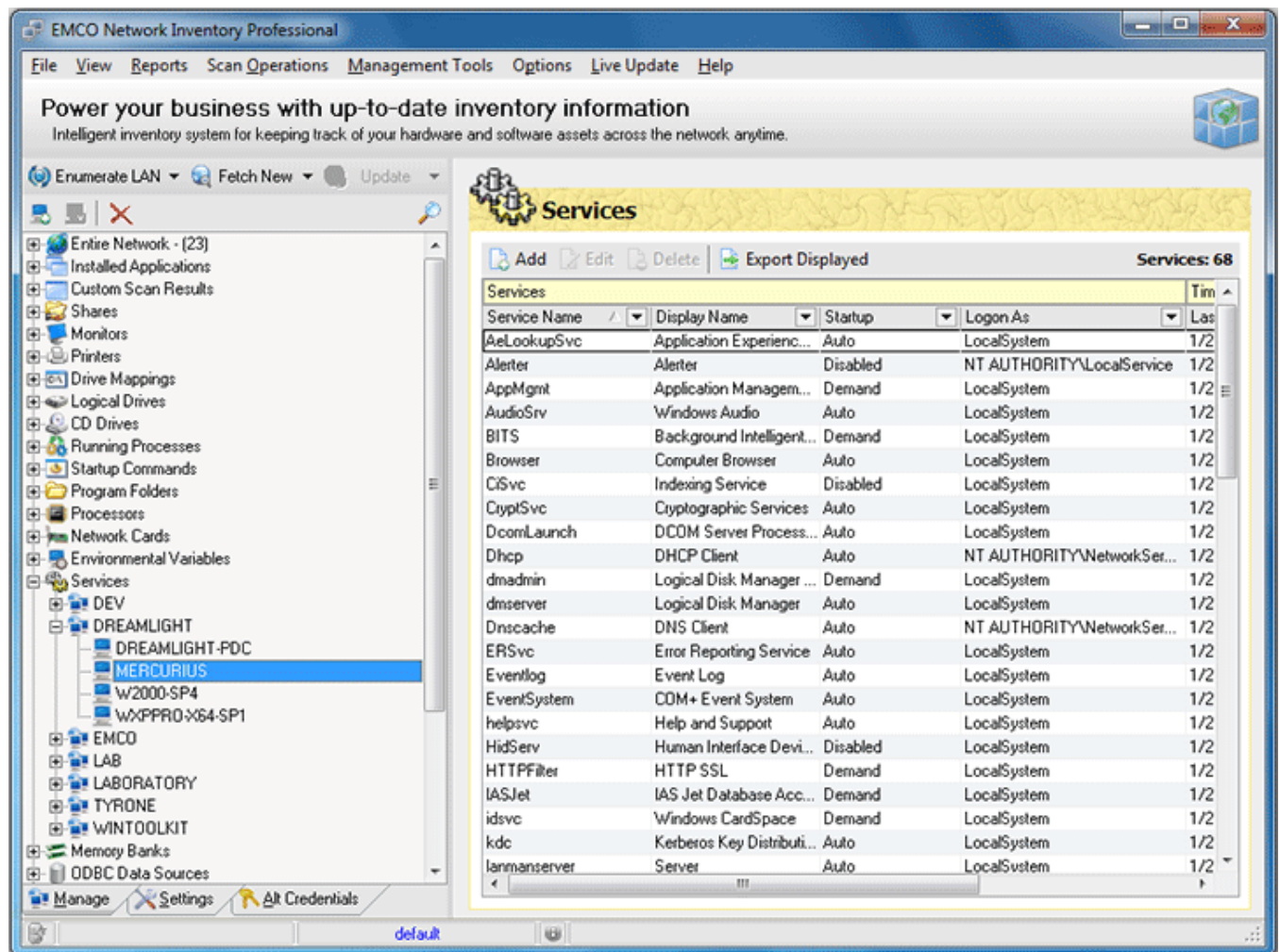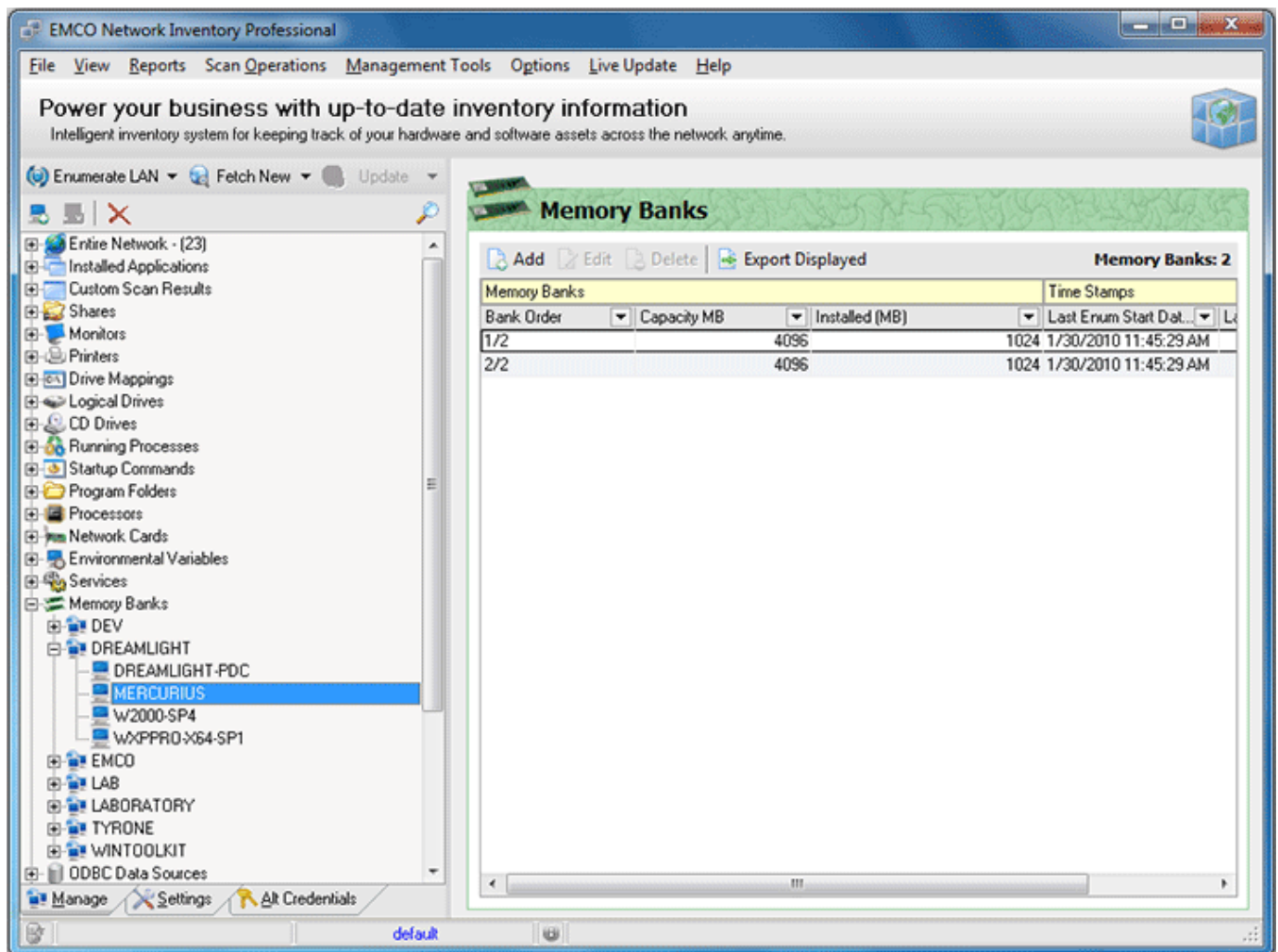

Pic 1. The list of services for the Machine

You can add a service to this list manually, remove the service from this list, edit each service info, export this list to any format or create a report containing this information.

Memory Banks

Network Inventory allows you to collect information on the memory banks available on any Machine. To get a list of memory banks first of all check the **Memory Banks Info** option on the **Settings** tab under the **Hardware Information Scan Options**. Then select the Machines you want to retrieve a list of memory banks for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the memory banks list for the Machine by selecting its **Memory Banks** child node in the **Machine Tree**. `Pic 1`
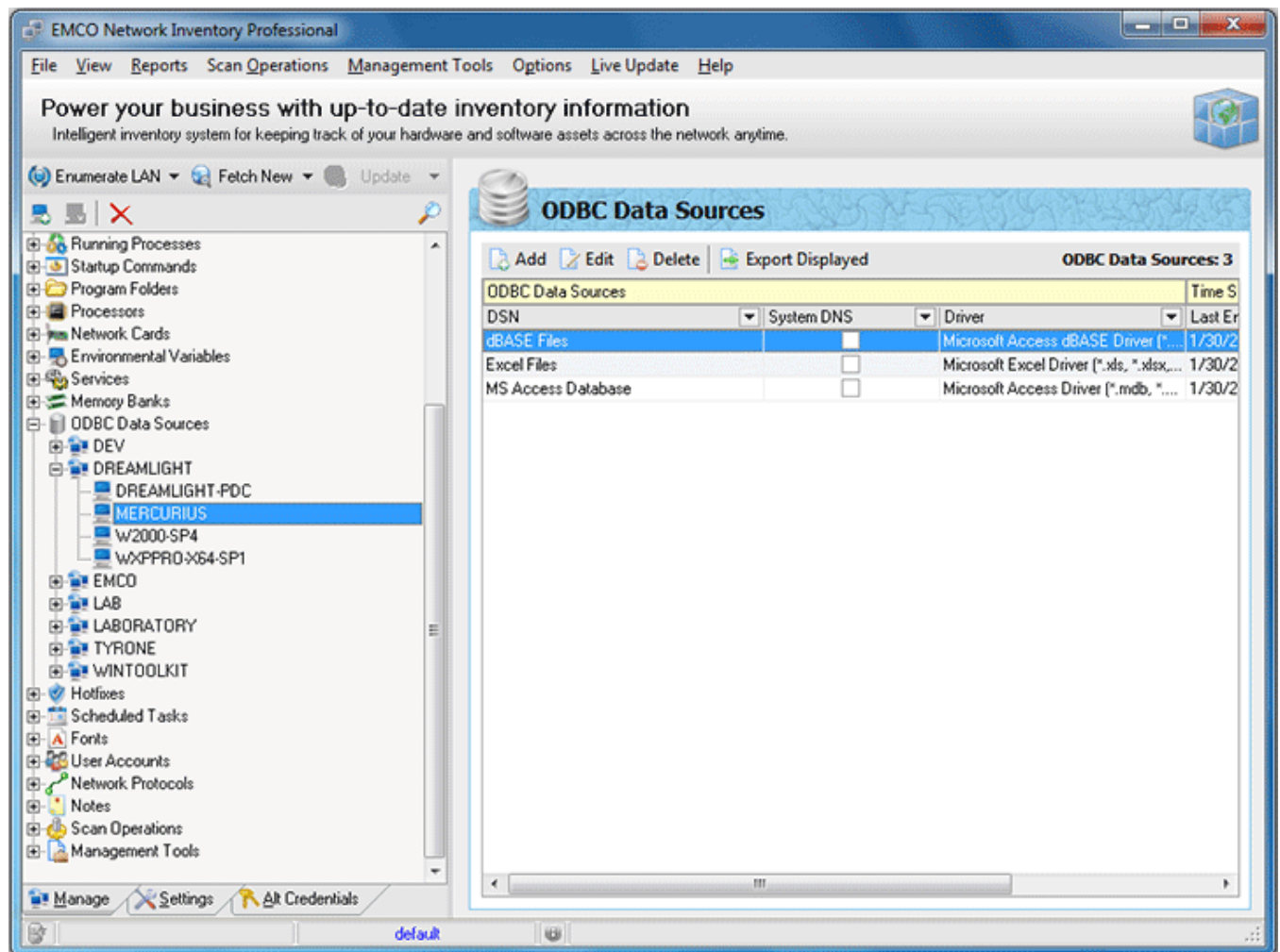

Pic 1. The list of memory banks for the Machine

You can add a memory bank to this list manually, remove the memory bank from this list, edit memory bank info, export this list to any format or create a report containing this information.

ODBC Data Sources

Network Inventory allows you to collect information on the ODBC data sources available on any Machine. To get a list of ODBC data sources first of all check the **ODBC Data Sources** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of data sources for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the data sources list for the Machine by selecting its **ODBC Data Sources** child node in the **Machine Tree**. `Pic 1`


Pic 1. The list of ODBC Data Sources for the Machine

You can add an ODBC data source to this list manually, remove the ODBC data source from this list, edit data source info, export this list to any format or create a report containing this information.

Scheduled Tasks

Network Inventory allows you to collect information on the tasks being scheduled in the Operating System on any Machine. To get a list of scheduled tasks first of all check the **Scheduled Tasks** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of scheduled tasks for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the tasks list for the Machine by selecting its **Scheduled Tasks** child node in the **Machine Tree**. `Pic 1`
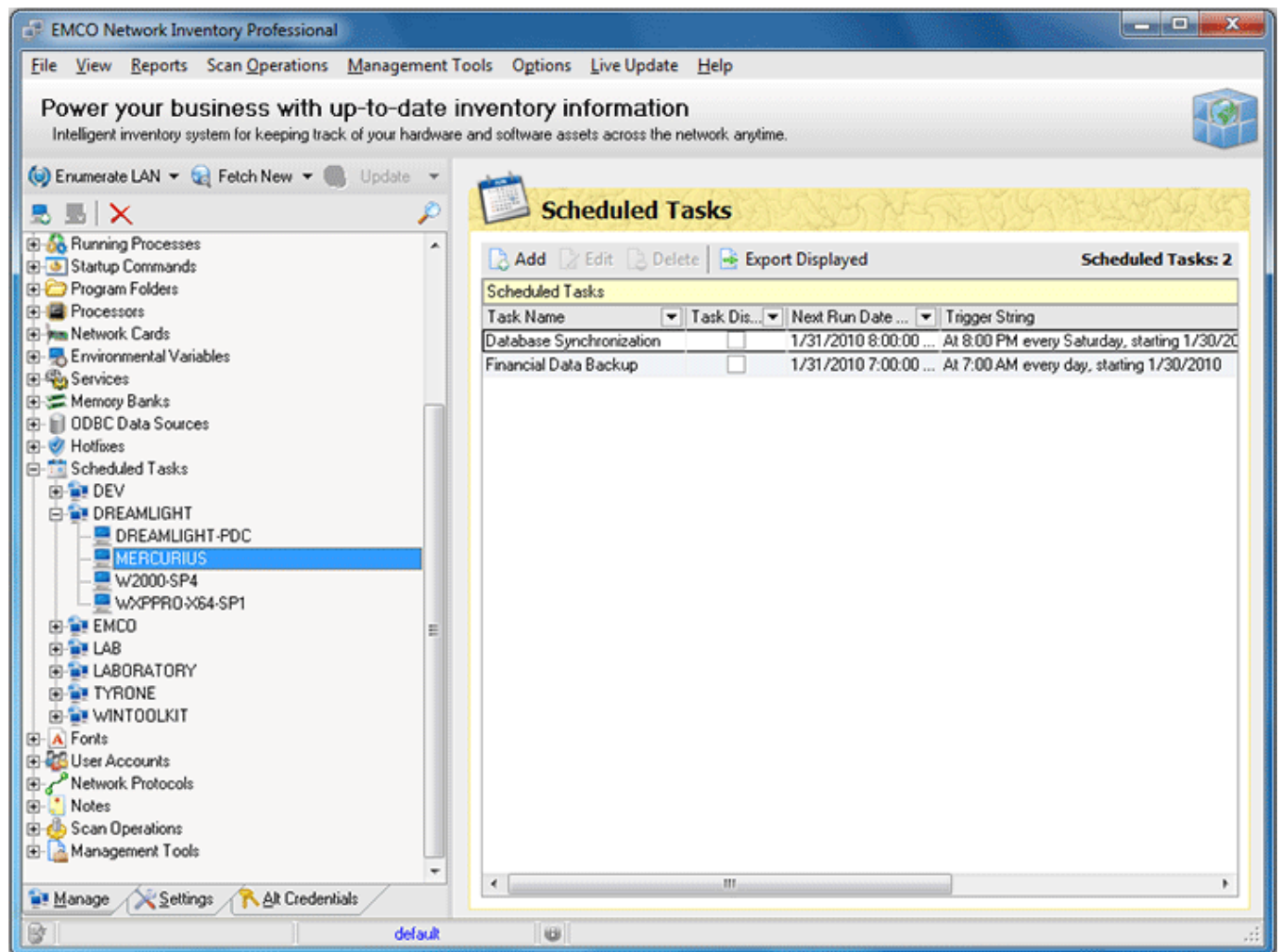

Pic 1. The list of scheduled tasks for the Machine

You can add a scheduled task to this list manually, remove the scheduled task from this list, edit each task info, export this list to any format or create a report containing this information.

Fonts

Network Inventory allows you to collect information on the fonts installed in the Operating System on any Machine. To get a list of fonts first of all check the **Fonts** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of fonts for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the fonts list for the Machine by selecting its **Fonts** child node in the **Machine Tree**. Pic 1
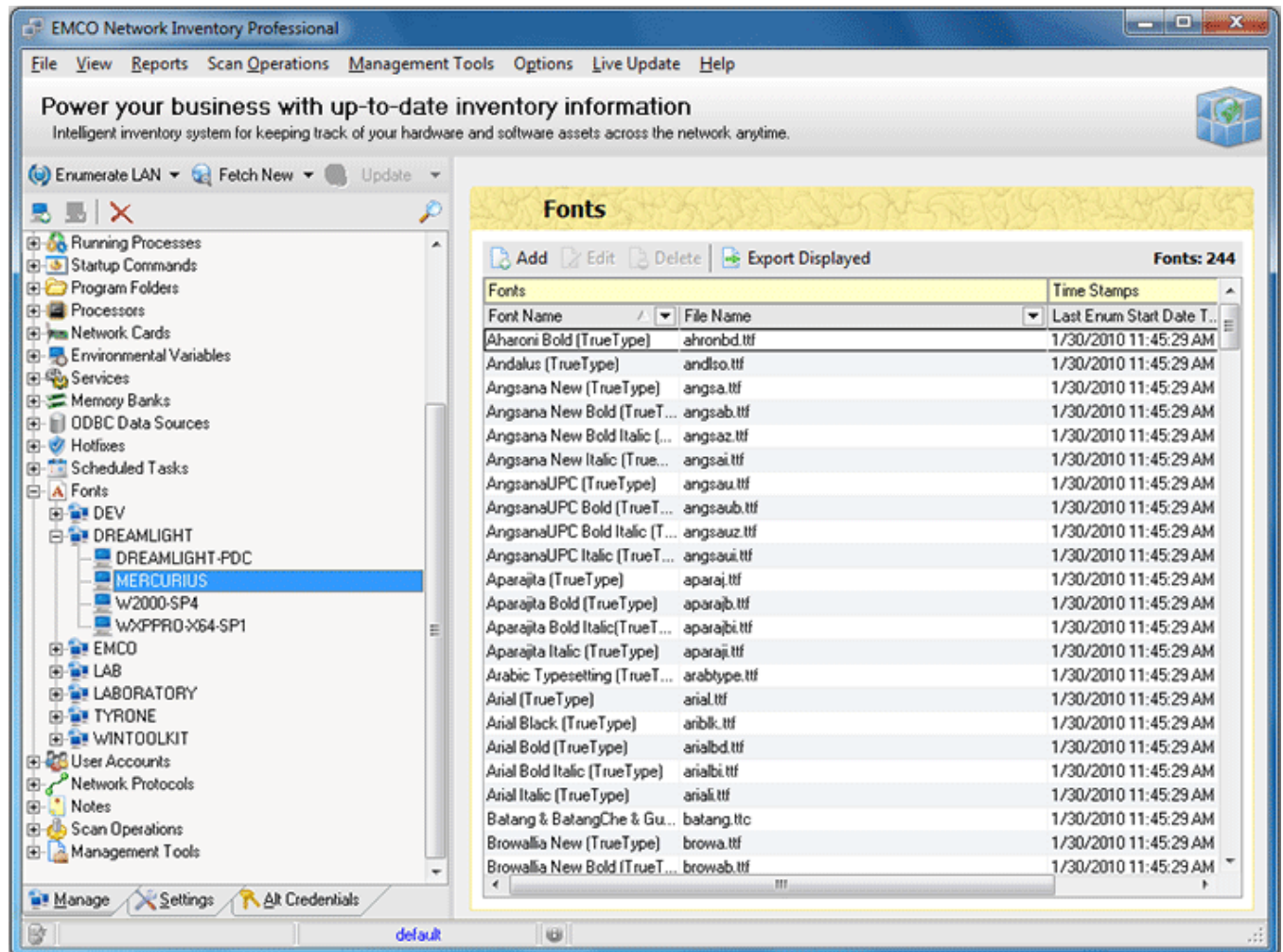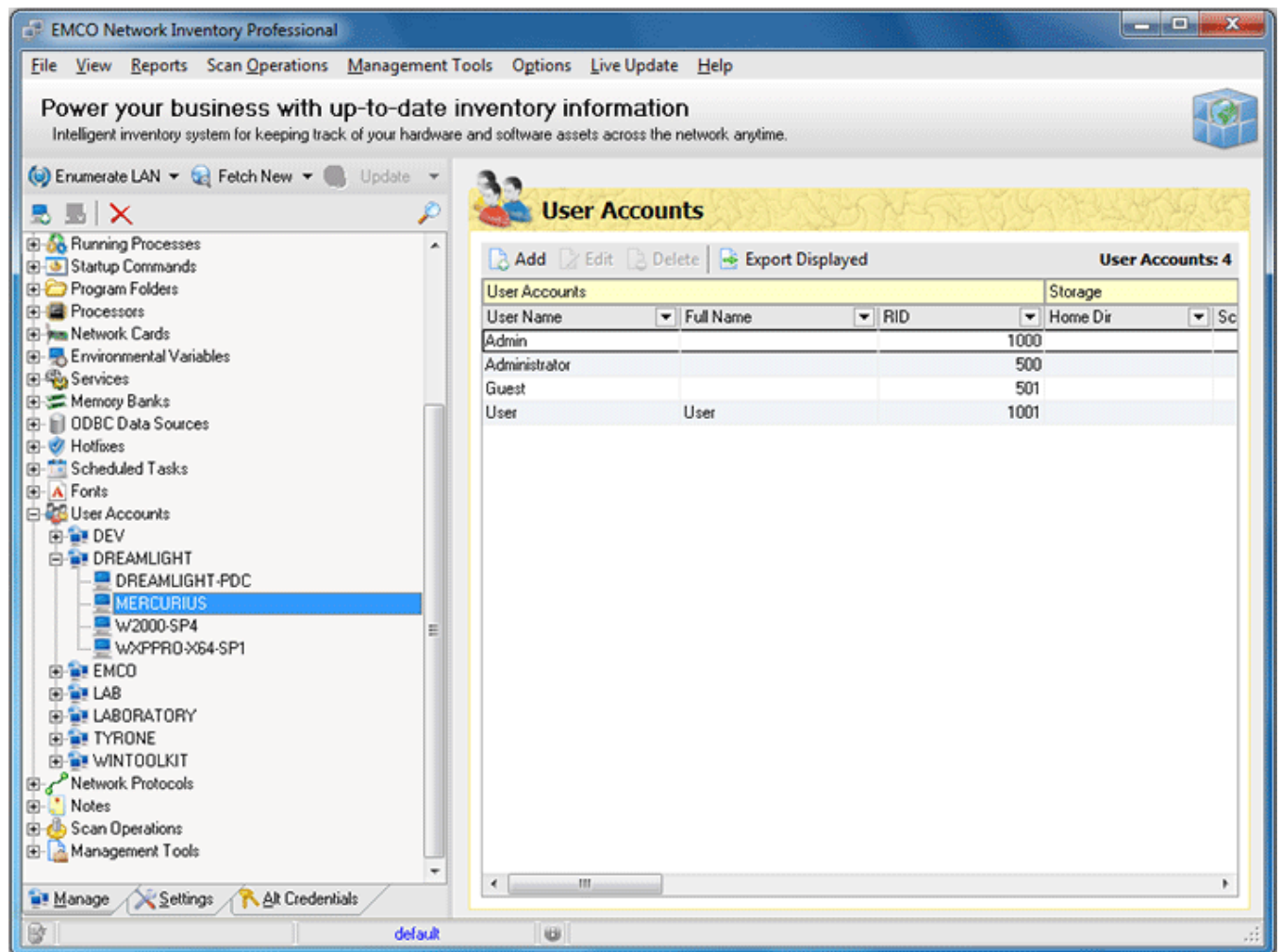

Pic 1. The list of fonts for the Machine

You can add a font to this list manually, remove the font from this list, edit font info, export this list to any format or create a report containing this information.

User Accounts

Network Inventory allows you to collect information on the user accounts known by the Operating System on any Machine. To get a list of user accounts first of all check the **User Accounts** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of accounts for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the user accounts list for the Machine by selecting its **User Accounts** child node in the **Machine Tree**. Pic 1

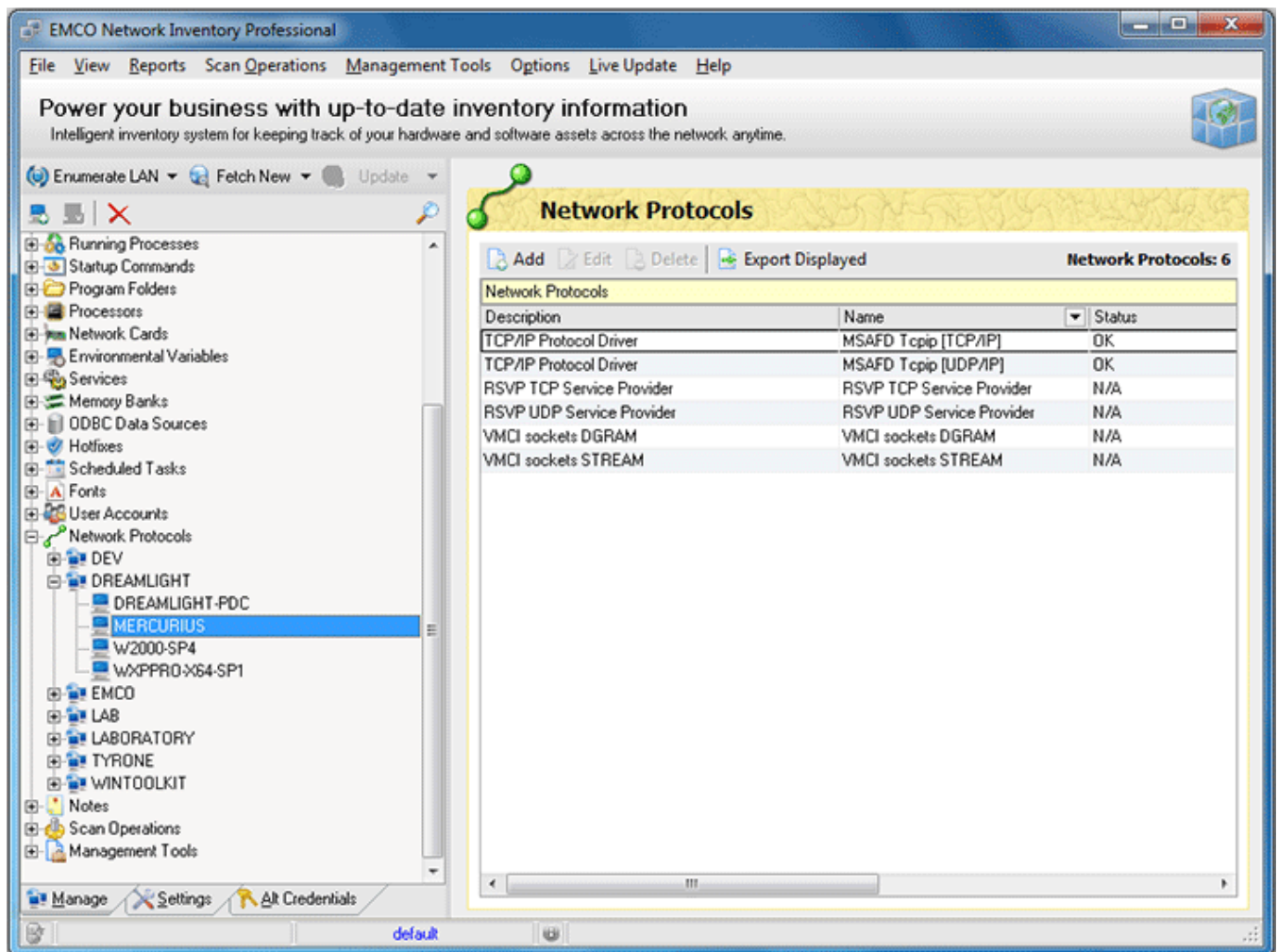**Pic 1. The list of user accounts for the Machine**

You can add a user account to this list manually, remove the user account from this list, edit account info, export this list to any format or create a report containing this information.

Network Protocols

Network Inventory allows you to collect information on the network protocols available on any Machine. To get a list of network protocols first of all check the **Network Protocols** option on the **Settings** tab under the **System Information Scan Options**. Then select the Machines you want to retrieve a list of protocols for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the network protocols list for the Machine by selecting its **Network Protocols** child node in the **Machine Tree**. `Pic 1`

Pic 1. The list of network protocols for the Machine

You can add a network protocol to this list manually, remove the network protocol from this list, edit protocol info, export this list to any format or create a report containing this information.

Custom Scan

Along with the **Brief Scan** and **Detailed Scan** Network Inventory provides you with an ability of running custom **File System** and **Registry** scans. Such scans allow you to find the file system and registry items that match the defined criteria on any Machine.

Custom scans can be really useful if you are going to detect policy violations, for example using some portable hacked programs at work place or storing entertainment data on the Machines. This chapter will guide you through the process of creating and executing custom scans.

What's Inside

File System Scan

Registry Scan

Custom Scan Criteria

File System Scan

File system scan feature of Network Inventory provides you with an ability of searching for the file system items matching a defined criteria any time you want. File system scan capabilities can be accessed by selecting the **File System Scan** node under the **Scan Operations** node of the **Machine Tree**. The **File System Scan** area will appear on the right of the application screen showing you the list of scan tasks. **Pic 1** This part will guide you through creating, configuring and executing custom **File System Scans**.
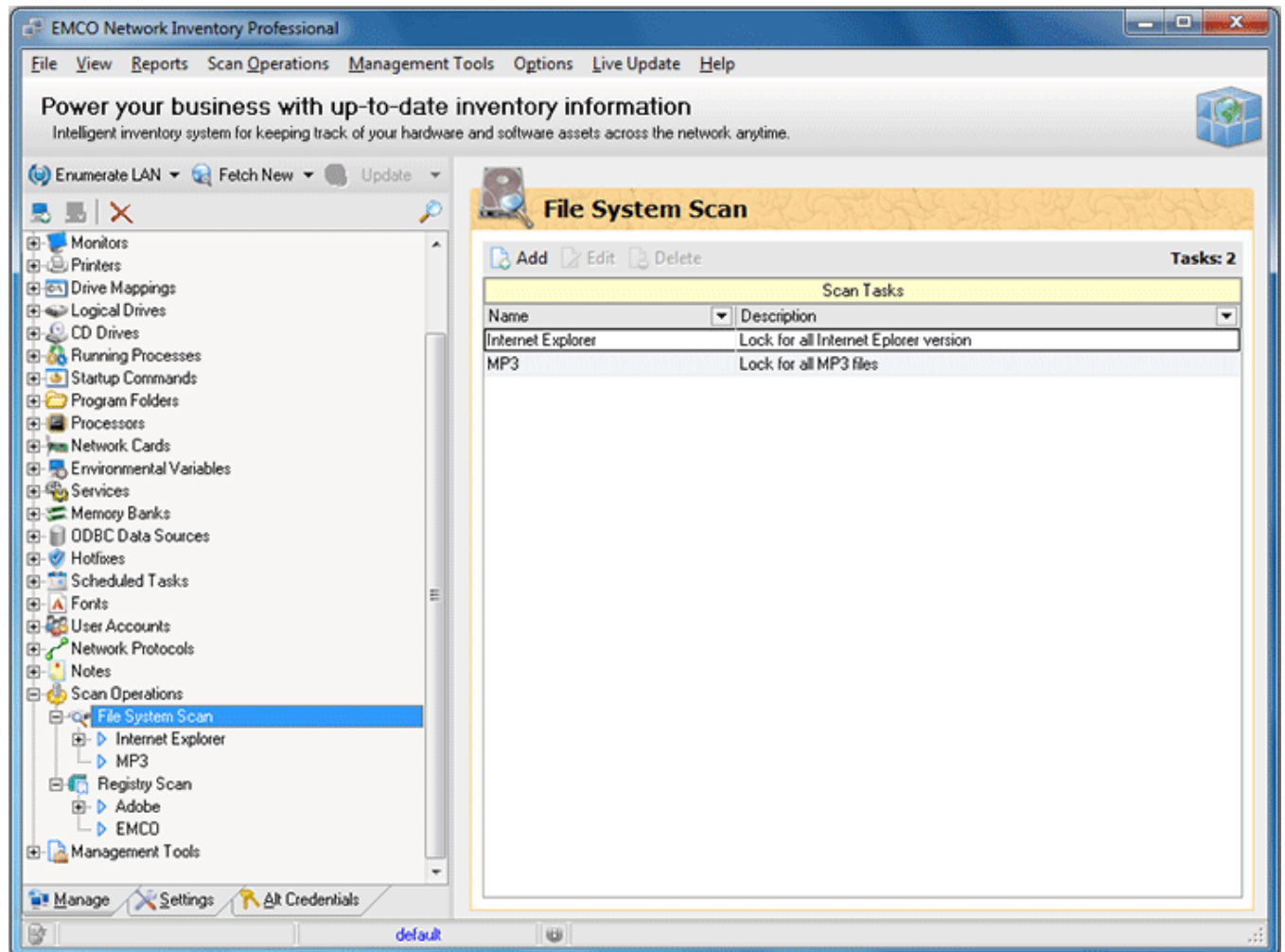
Pic 1. File system scan tasks list

Creating a File System Scan

To create a new file system scan select **File System Scan** node under the **Scan Operations** node of the **Machine Tree** and press **Add** button on the tool bar of the **File System Scan** area. The **Add Scan Task** dialog will appear on the screen. `Pic 2`
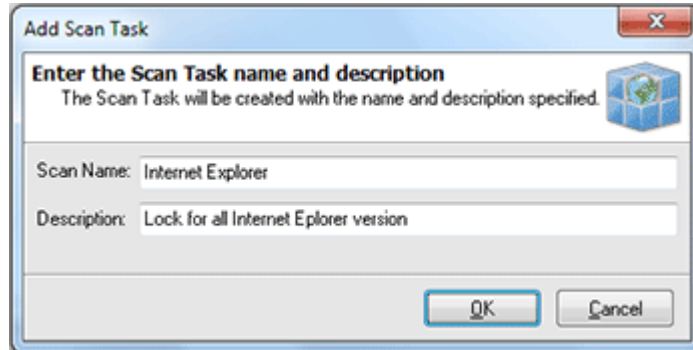
Pic 2. Creating a File System Scan

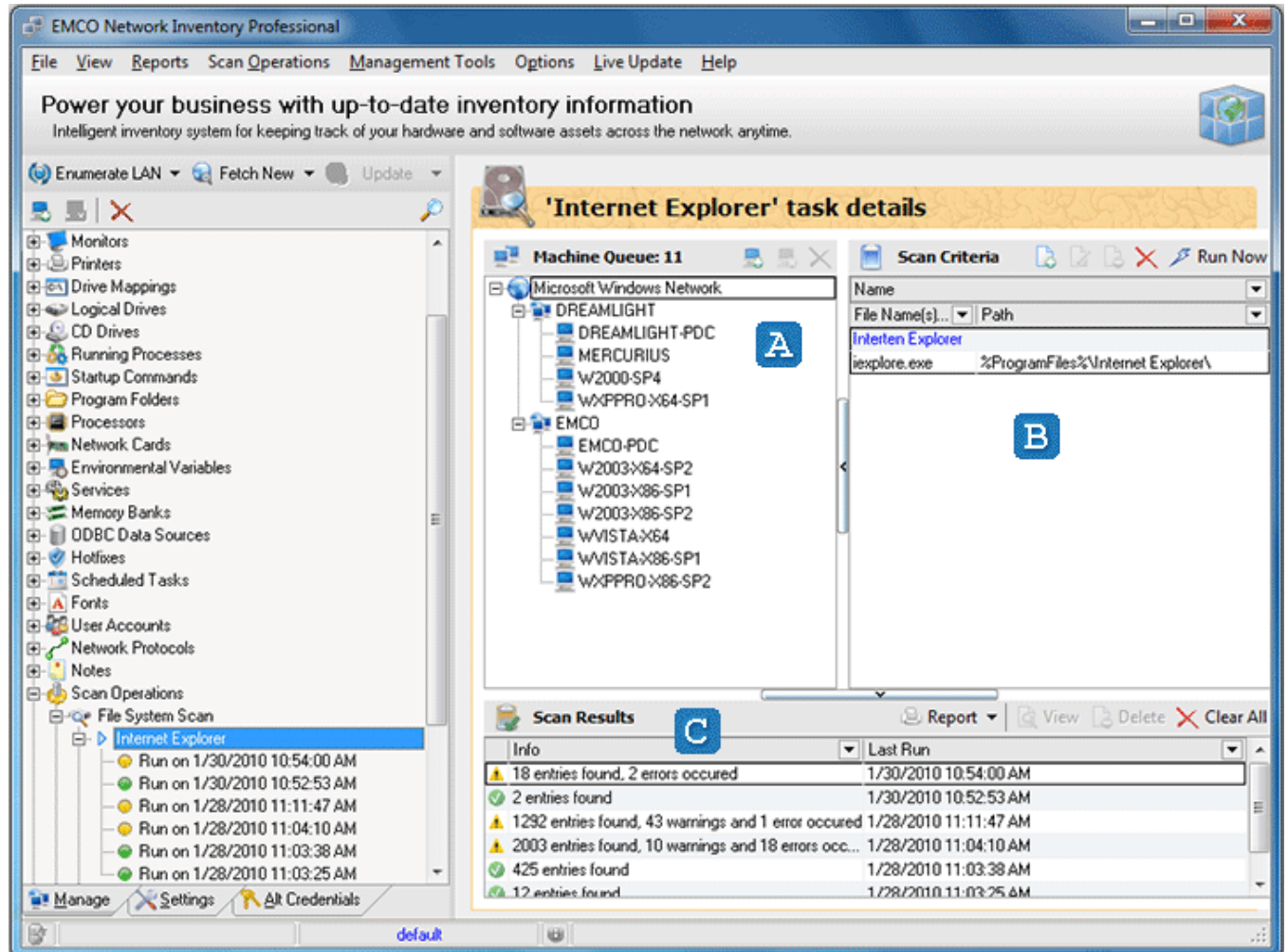In the **Add Scan Task** dialog you are proposed to provide a scan name and description. The scan created will contain the criteria to match and the Machines to scan for the items matching the criteria along with the scan results. You can then execute this scan as many times as you want. When you are ready with filling the data required press **OK** button to proceed. When the task is added the view is automatically switched to the task configuration. **Pic 3** In the **Task Details** area you are to specify a criteria, Machines to take part in scan and review scan results.

Pic 3. The task details area

The **Tasks Details** area consists of three parts. These are the **Machine Queue** A, **Scan Criteria** B and **Scan Results** C panes. The **Machine Queue** pane shows you the Machines to take part in the scan task, the **Scan Criteria** pane manages the list of criteria to be used for scan task and **Scan Results** pane contains the list of task execution results.

Adding Machines to scan

When the scan is created you can define Machines to be scanned. These Machines are displayed within the **Machine Queue** pane. To add the Machine press **Include Machine(s)** button on the tool bar of the **Machine Queue** pane. The **Add Machines to Queue** dialog will appear on the screen. `Pic 4`

Pic 4. Selecting Machines to scan for file system items

Configuring Scan Criteria

After the Machines to take part in scan are defined it is time to specify a scan criteria. All the scan criteria to match are displayed w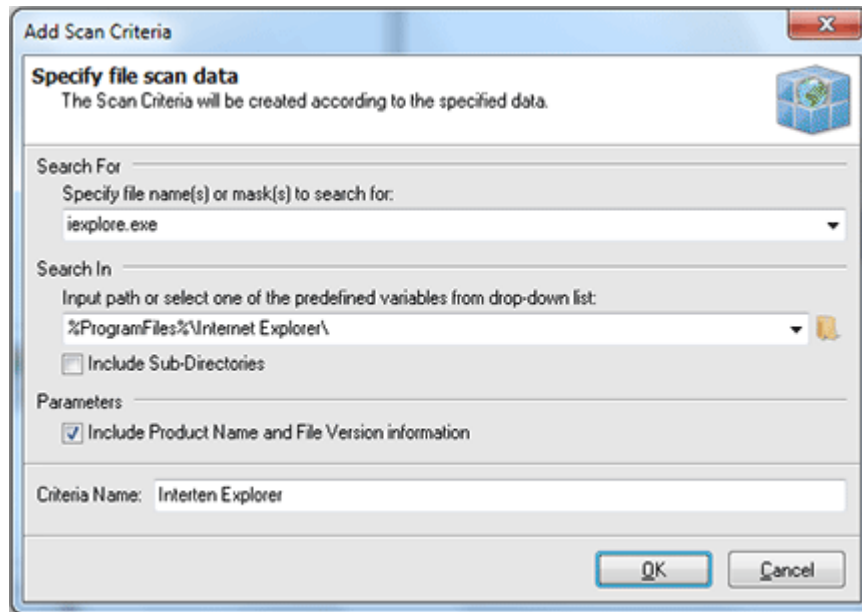ithin the **Scan Criteria** pane. You can add as many criteria as you wish. To add a new criteria press **Add** button on the tool bar of the **Scan Criteria** pane. The **Add Scan Criteria** dialog will appear on the screen to specify the criteria. `Pic 5`

Pic 5. Specifying File System Scan criteria

In the **Add Scan Criteria** dialog you should specify a file system item name or mask to search for, where to search, if the sub directories of search root are included in the search and a name for the criteria being created. You can use the predefined constants available from the drop-down list to specify the search root. When you have defined all the parameters required press **OK** button to proceed.

Executing File System Scan

Now you have the fully configured File System Scan and can execute it. To execute the scan press **Run Now** button on the tool bar of the **Scan Criteria** pane. The scan is now being executed and its progress is shown in the status bar. When the scan completes the result is added to the **Scan Results** pane. Double click the result to see the details. Pic 6
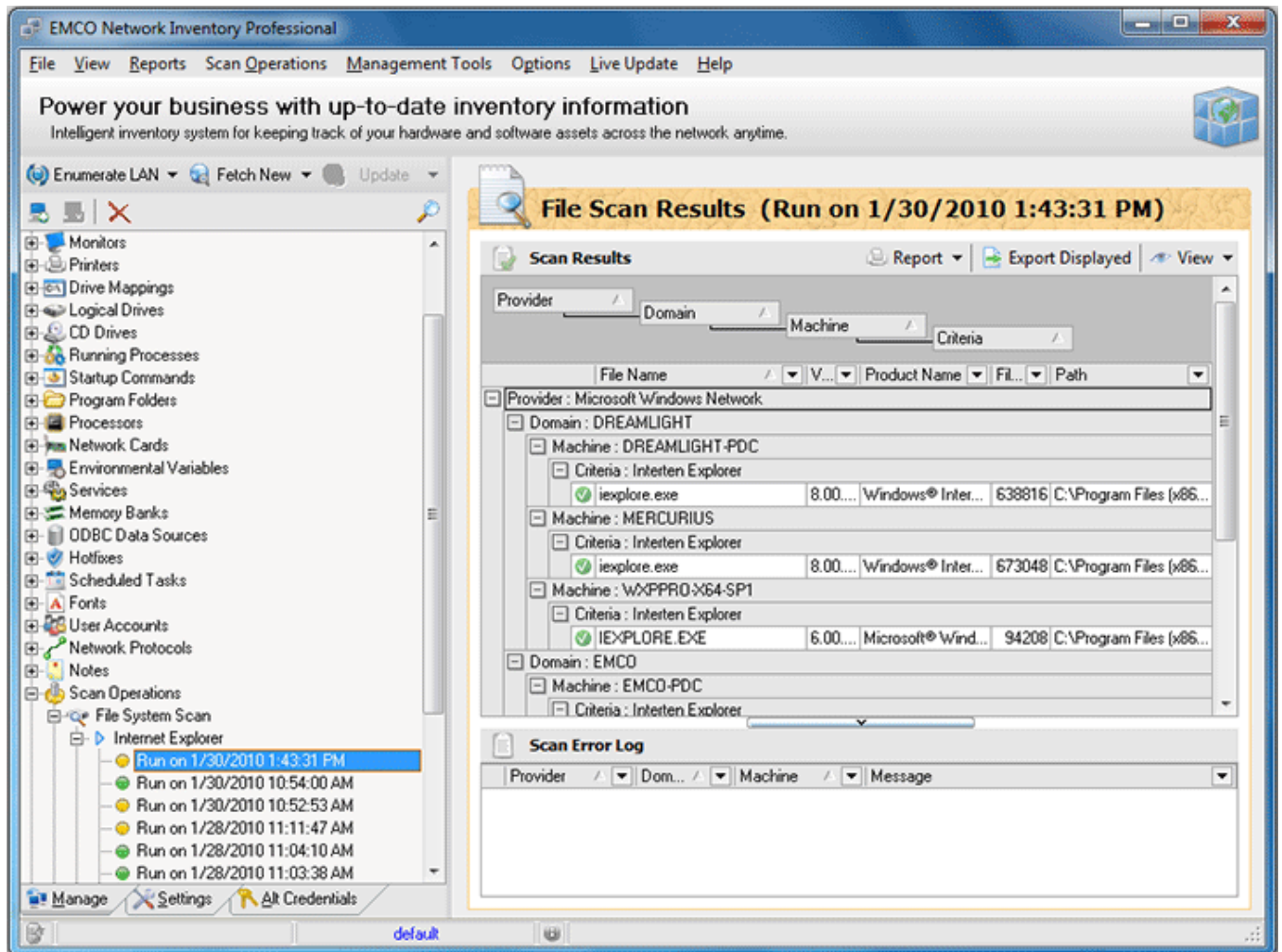
Pic 6. File System Scan results

You have successfully created, configured and executed the File System Scan and ready to use this feature of Network Inventory.

Registry Scan

Registry scan feature of Network Inventory provides you with an ability of searching for the Windows registry items matching a defined criteria any time you want. Registry scan capabilities can be accessed by selecting the **Registry** node under the **Scan Operations** node of the **Machine Tree**. The Registry Scan area will appear on the right of the application screen showing you the list of scan tasks. This part will guide you through creating, configuring and executing custom **Registry Scans**.
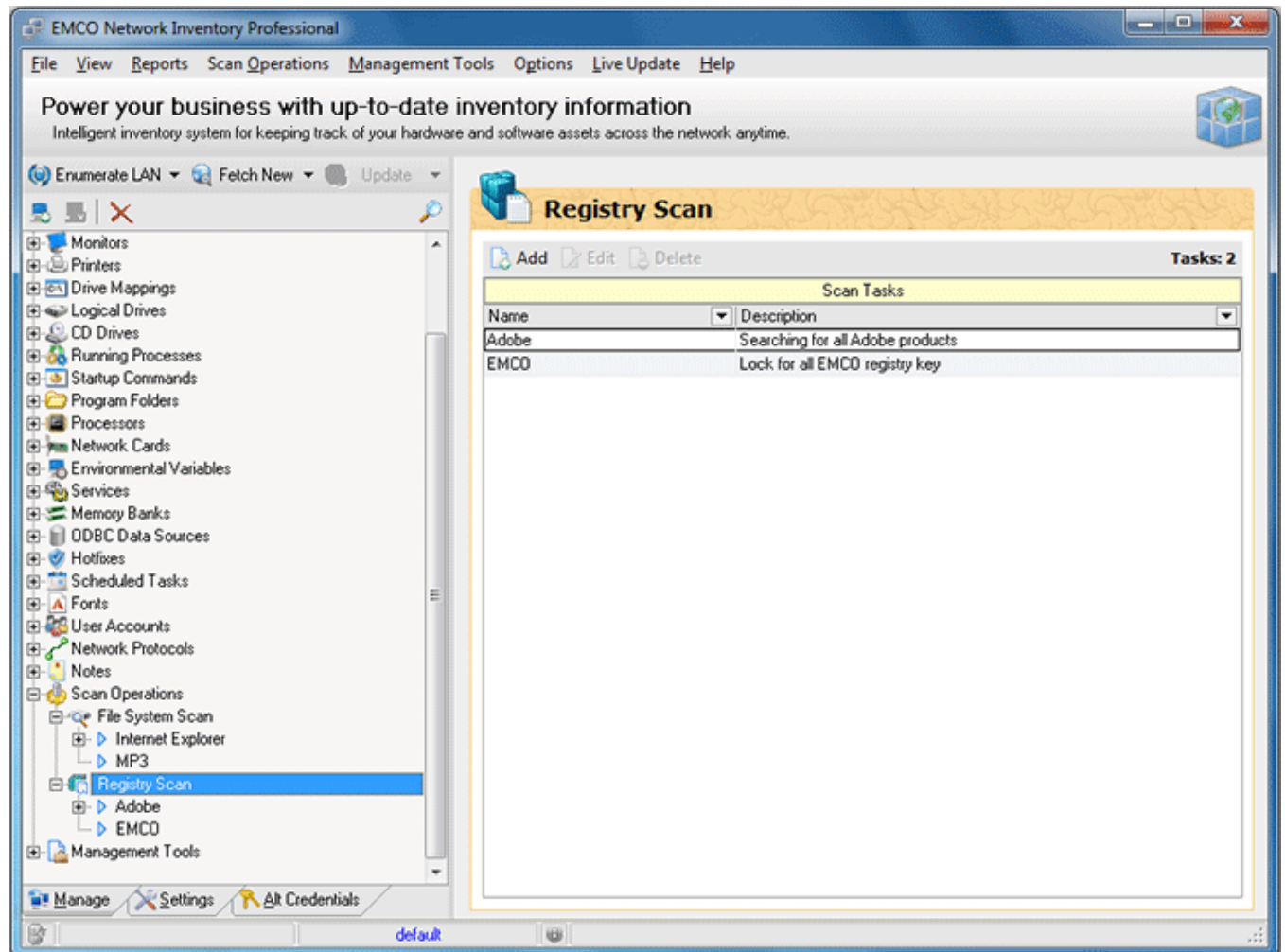
Pic 1. Registry scan tasks list

Creating a Registry Scan

To create a new registry scan select **Registry Scan** node under the **Scan Operations** node of the **Machine Tree** and press **Add** button on the tool bar of the **Registry Scan** area. The **Add Scan Task** dialog will appear on the screen. Pic 2
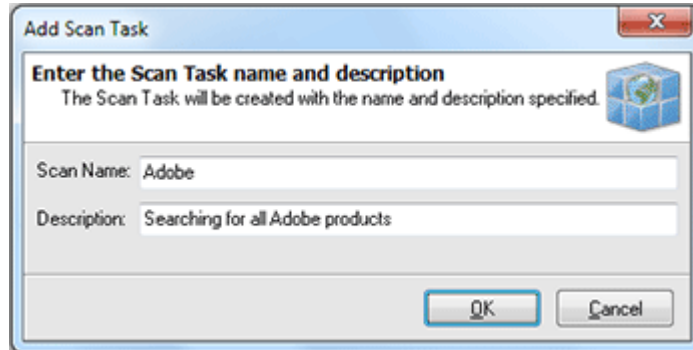
Pic 2. Creating a Registry Scan

In the **Add Scan Task** dialog you are proposed to provide a scan name and description. The scan created will contain the criteria to match and the Machines to scan for the items matching the criteria along with the scan results. You can then execu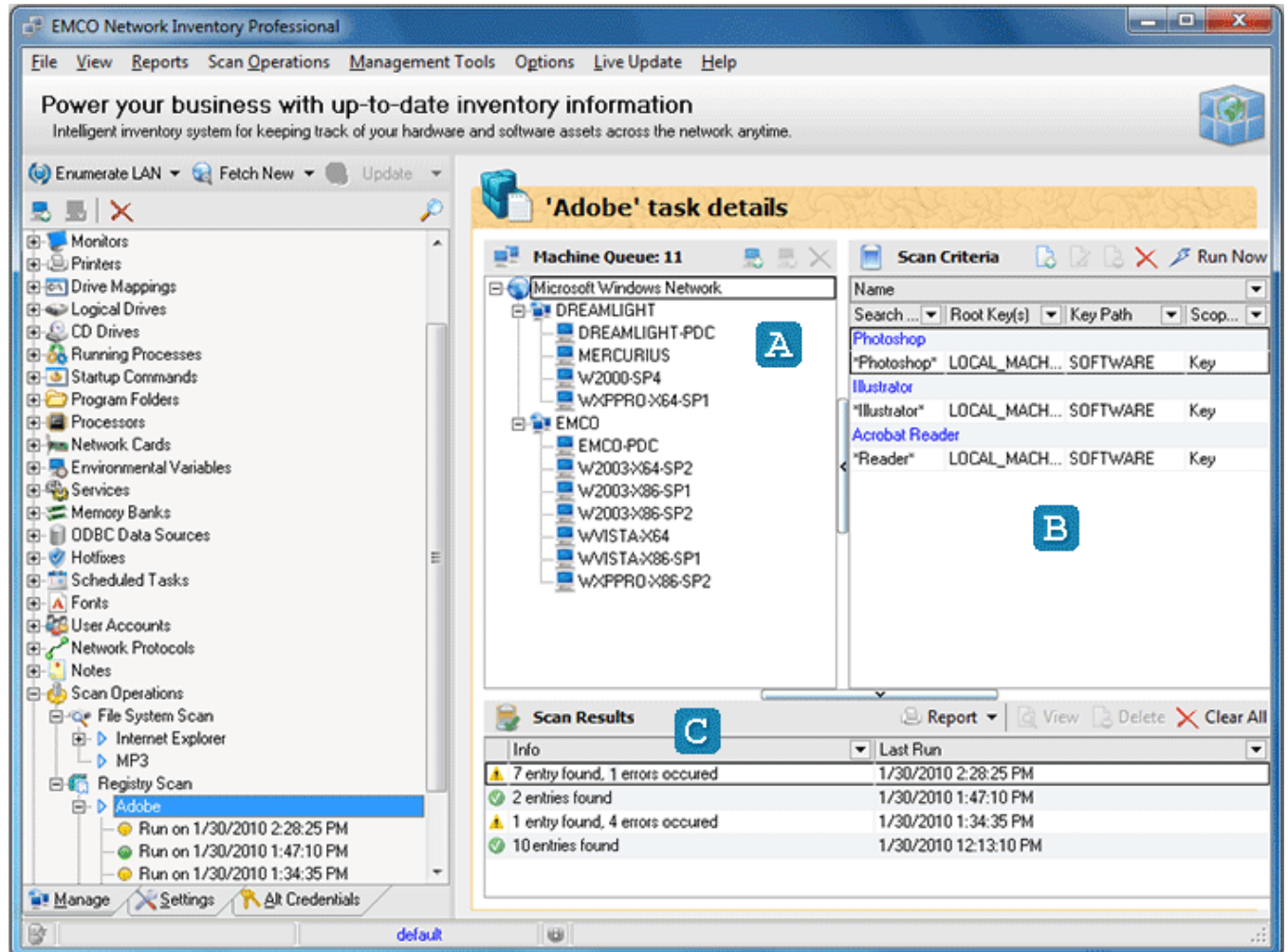te this scan as many times as you want. When you are ready with filling the data required press **OK** button to proceed. When the task is added the view is automatically switched to the task configuration. **Pic 3** In the **Task Details** area you are to specify a criteria, Machines to take part in scan and review scan results.

Pic 3. The task details area

The **Tasks Details** area consists of three parts. These are the **Machine Queue** [A], **Scan Criteria** [B] and **Scan Results** [C] panes. The **Machine Queue** pane shows you the Machines to take part in the scan task, the **Scan Criteria** pane manages the list of criteria to be used for scan task and **Scan Results** pane contains the list of task execution results.

Adding Machines to scan

When the scan is created you can define Machines to be scanned. These Machines are displayed within the **Machine Queue** pane. To add the Machine press **Include Machine(s)** button on the tool bar of the **Machine Queue** pane. The **Add Machines to Queue** dialog will appear on the screen. `Pic 4`

Pic 4. Selecting Machines to scan for registry items

In the **Add Machines to Queue** dialog you are to check the Machines to participate in scan from the available network structure. After checking these press **OK** button to proceed. The Machines you have checked are now added to the **Machine Queue**.

Configuring Scan Criteria

After the Machines to take part in scan are defined it is time to specify a scan criteria. All the scan criteria to match are displayed within the **Scan Criteria** pane. You can add as many criteria as you wish. To add a new criteria press **Add** button on the tool bar of the **Scan Criteria** pane. The **Add Scan Criteria** dialog will appear on the screen to specify the criteria. Pic 5
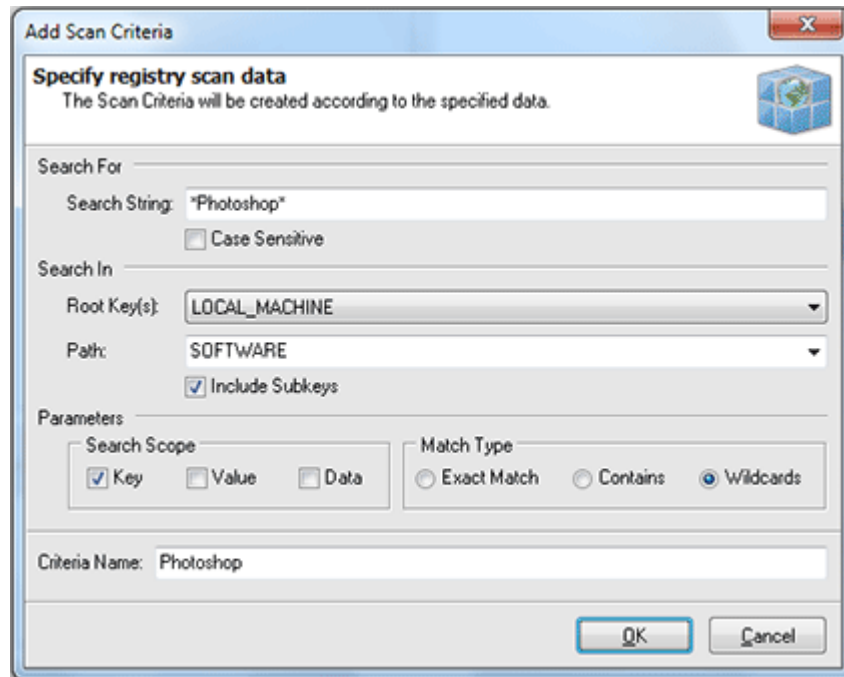
Pic 5. Specifying Registry Scan criteria

In the **Add Scan Criteria** dialog you should specify a string to search for, where to search, if the sub keys of search root are included in the search, search scope, matching rule and a name for the criteria being created. When you have defined all the parameters required press **OK** button to proceed.

Executing Registry Scan

Now you have the fully configured Registry Scan and can execute it. To execute the scan press **Run Now** button on the tool bar of the **Scan Criteria** pane. The scan is now being executed and its progress is shown in the status bar. When the scan completes the result is added to the **Scan Results** pane. Double click the result to see the details. `Pic 6`
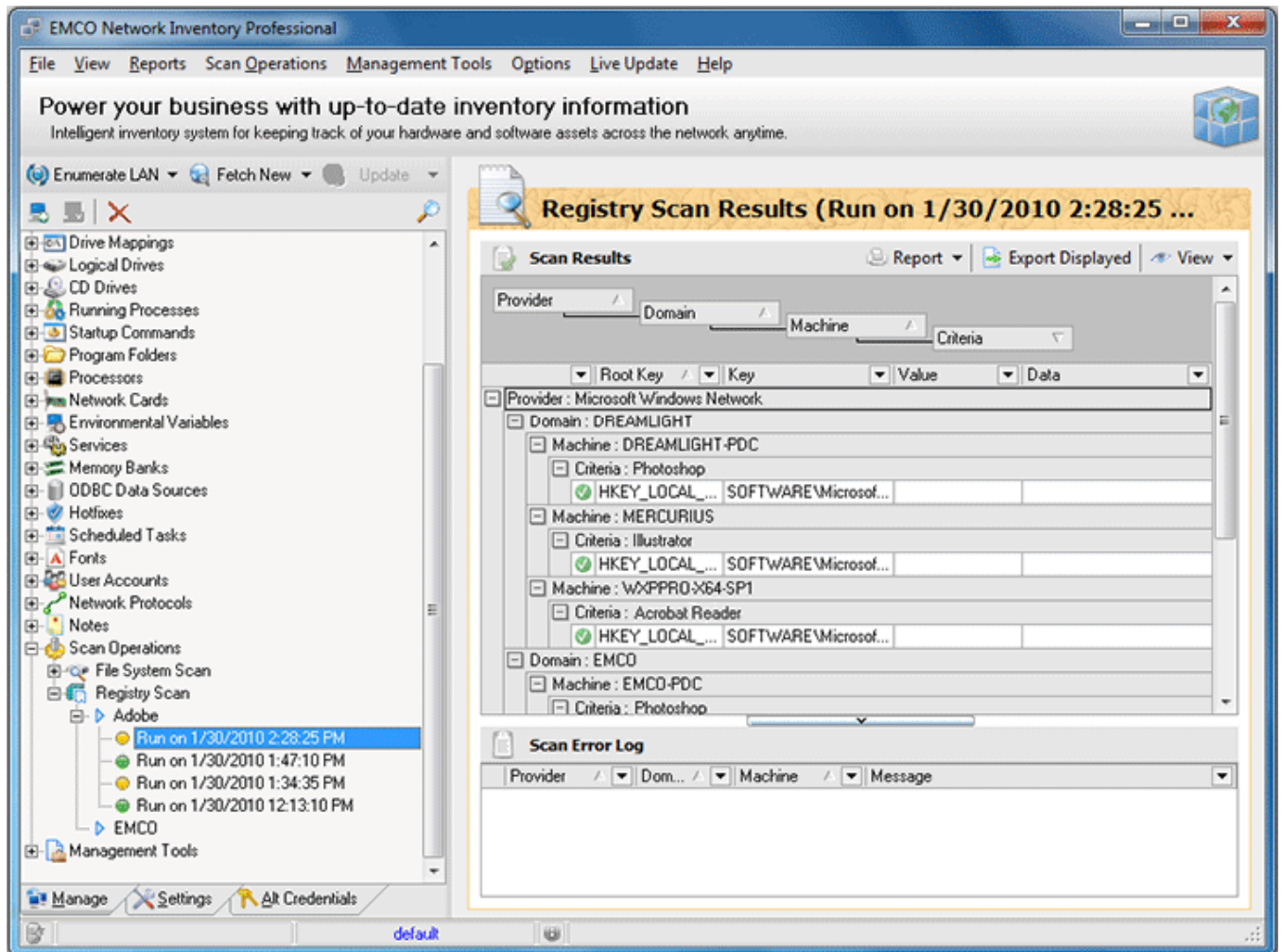
Pic 6. Registry Scan results

You have successfully created, configured and executed the Registry Scan and ready to use this feature of Network Inventory.

Custom Scan Criteria

Along with the simple File Scan and Registry Scan you can provide a custom scan criteria to be used along with other **Detailed Scan** options. This criteria allows you to fetch additional file system, registry and services info that can't be fetched with simple scan. To use custom scan criteria first of all you should enable the **Execute Custom Scan** option on the **Settings** tab under the **Software Information Scan Options**.

The next step is specifying a criteria itself – select **Management Tools > Custom Scan Criteria** menu item from the main application menu or select **Custom Scan Criteria** node under the **Management Tools** one in the **Machine Tree**. The **Custom Scan Criteria** dialog will appear on the screen. `Pic 1`
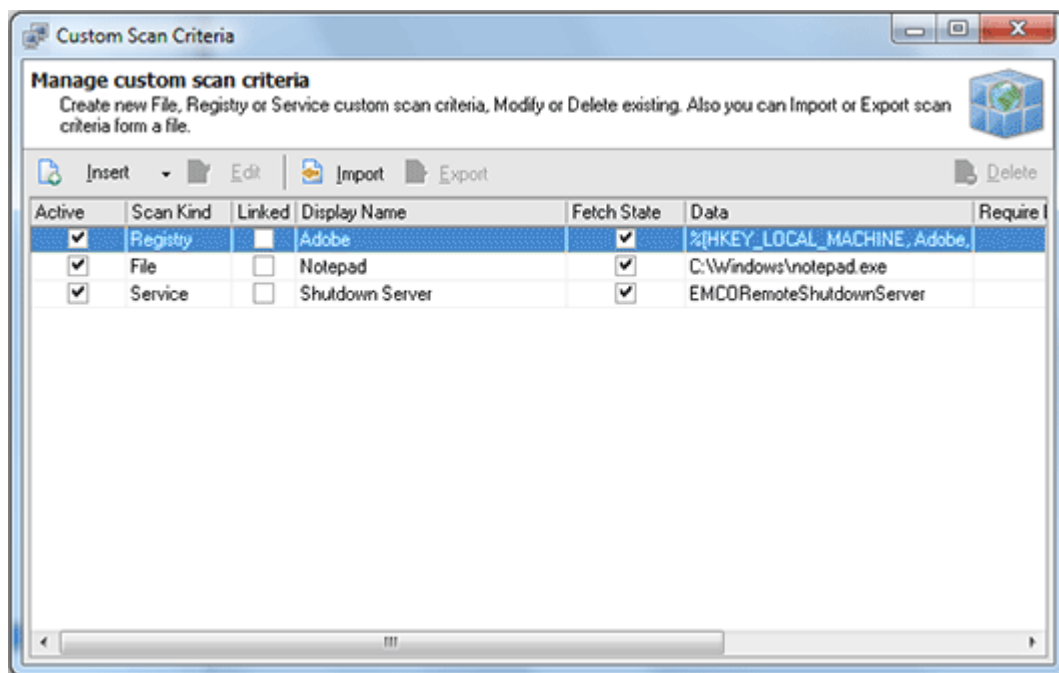
Pic 1. Custom Scan Criteria dialog

The **Custom Scan Criteria** dialog contains the list of all custom scan criteria defined. You can add a criteria, edit one and delete. Also you can export this list to a file for a future use or import existing from file. It is possible to define file, registry or service scan criteria.

File scan criteria

File custom scan criteria allows you to find specific files on the remote Machines and link them to the applications list. To add a file scan criteria choose **File** item from the **Insert** button drop-down on the tool bar over the criteria list. The **Custom File Scan Criteria** dialog will appear on the screen. `Pic 2`
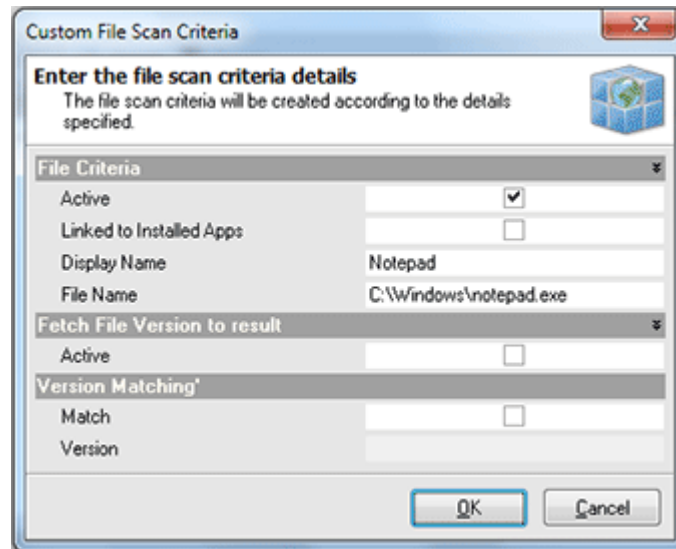

Pic 2. Adding the custom file scan criteria

In the **Custom File Scan Criteria** dialog you are proposed to specify a Display Name of the application this file belongs to by entering a name or choosing from the applications list if the linkage is enabled and the file to search itself. Optionally you can choose if the version should also match. After all the required information is specified press **OK** button to proceed. The custom file scan criteria is now added to the criteria list.

Registry scan criteria

Registry custom scan criteria allows you to find a specific registry data on the remote Machines and link in to the applications list. To add a registry scan criteria choose **Registry** item from the **Insert** button drop-down on the tool bar over the criteria list. The **Custom Registry Scan Criteria** dialog will appear on the screen. `Pic 3`

Pic 3. Adding the custom registry scan criteria

In the **Custom Registry Scan Criteria** dialog you are proposed to specify a Display Name of the application this registry data belongs to by entering a name or choosing from the applications list if the linkage is enabled and registry value-key pare itself. Optionally you can choose if the data of the key should match with the data provided. After all the required information is specified press **OK** button to proceed. The custom registry scan criteria is now added to the criteria list.

Service scan criteria

Service custom scan criteria allows you to find specific services on the remote Machines and link them to the applications list. To add a service scan criteria choose **Service** item from the **Insert** button drop-down on the tool bar over the criteria list. The **Custom Service Scan Criteria** dialog will appear on the screen. **Pic 4**
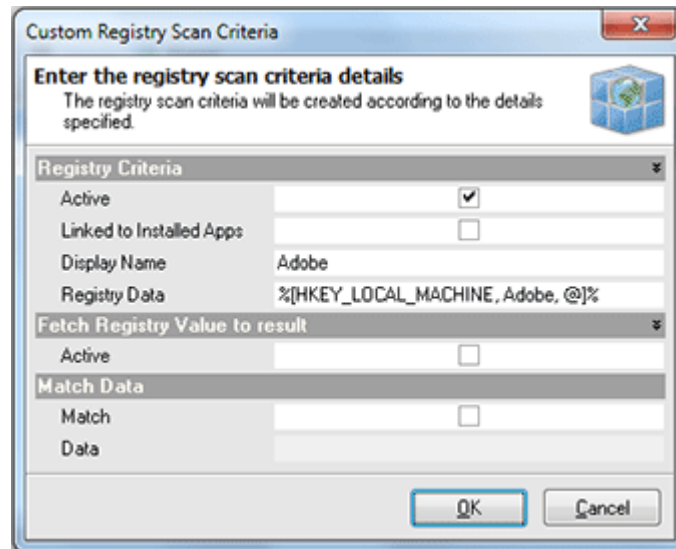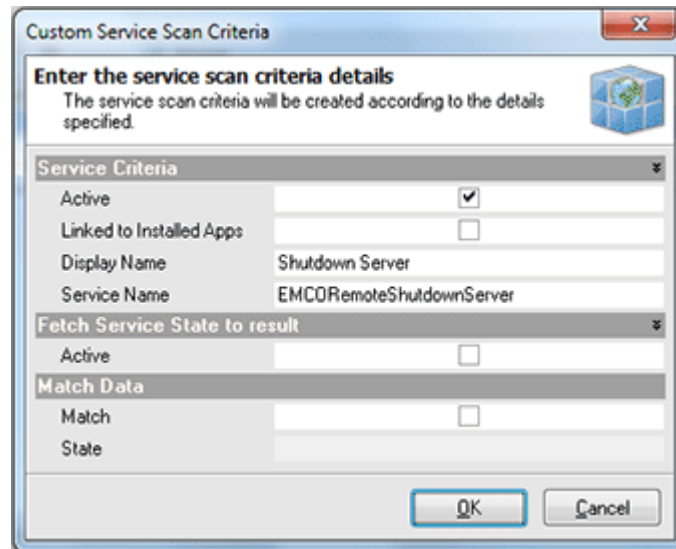

Pic 4. Adding the custom service scan criteria

In the **Custom Service Scan Criteria** dialog you are proposed to specify a Display Name of the application this service belongs to by entering a name or choosing from the applications list if the linkage is enabled and the service name to search itself. Optionally you can choose if the service state should match with the state provided. After all the required information is specified press **OK** button to proceed. The custom service scan criteria is now added to the criteria list.

When all the criteria required are specified select the Machines you want to run custom scan for and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. As soon as the update process completes you are about to see the custom scan results for the Machine by selecting its **Custom Scan Results** child node in the **Machine Tree**. Pic 5
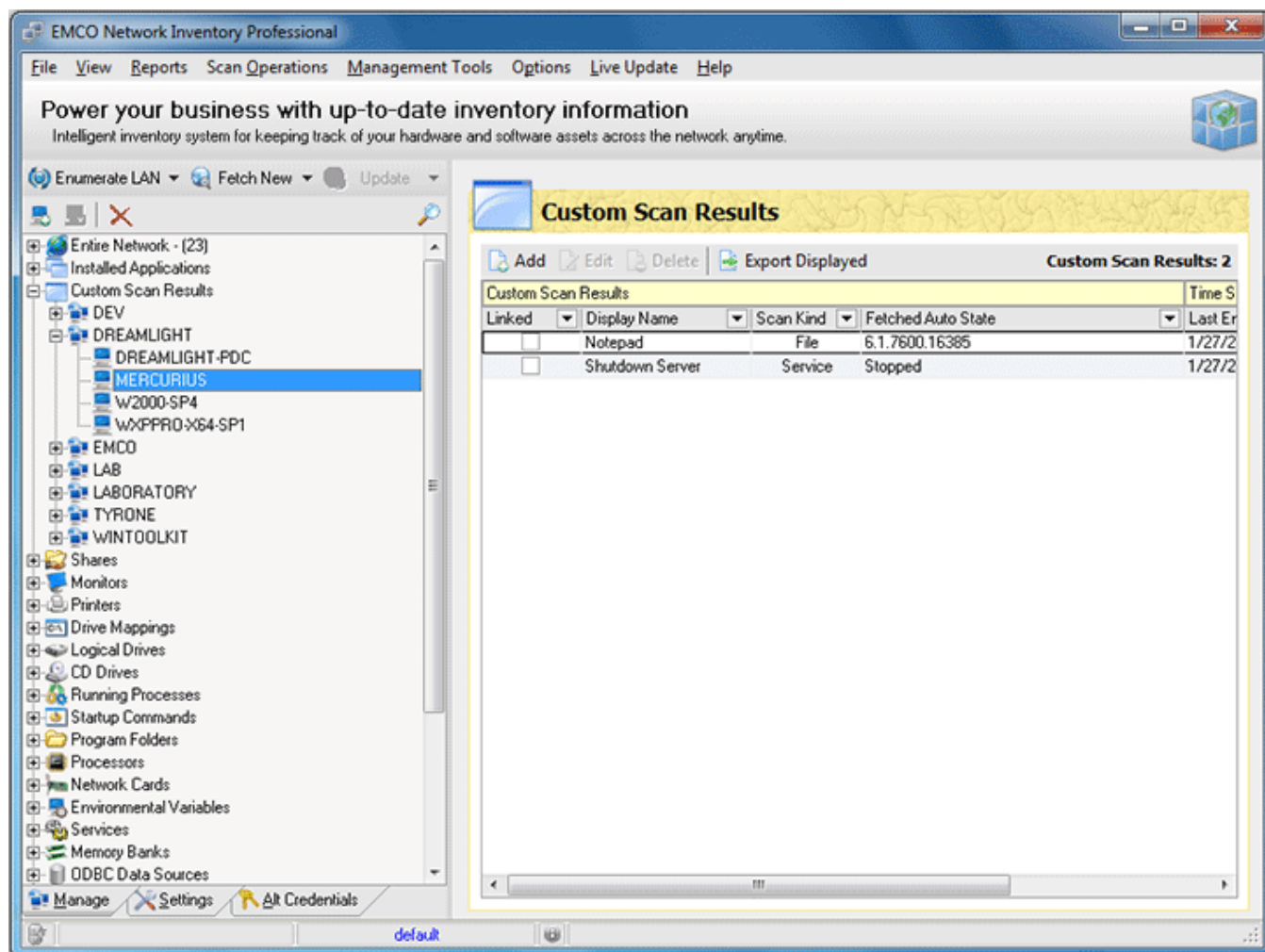
Pic 5. Custom scan results

Now you are familiar with the Custom Scan Criteria functionality and can use this feature of Network Inventory without any difficulties.

Updating Scan Data

After you have once collected inventory information with a help of Network Inventory you can easily build a report on this information. But the other important feature is that you can always keep this information up to date using the update scan functionality. The update can be performed both manually and automatically. This chapter describes how to keep your data up to date.

What's Inside

Automatic Update

Manual Update

Automatic Update

Network Inventory allows you to keep inventory information up to date with no effort. All you need is to enable automatic inventory data update. The automatic update can be enabled both on a single Machine and on a range of Machines. To enable this feature for a single Machine select it in the **Machine Tree** and press **Auto Update** button on the management tool bar of the machine details area. If you want to turn the automatic update on for a scope of Machines select this scope in the **Machine Tree**, right click the selection and choose **Auto Update > Include All** menu item. The automatic update process should execute regarding the auto processing options defined.

Manual Update

Sometimes the automatic update of inventory data is not a convenient way. In such a case you can always perform the update of inventory information manually. There are four possible scenarios of manual update – you can update the data for the selected Machines, the Machines that were offline during the last update though marked with a red cross, the Machines which data was not updated during last 30 days and custom update. All these scenarios are described below.

Update Selected

To update only some particular Machines select these Machines in the **Machine Tree** and choose **Update Selected** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. The update process starts and soon you'll have inventory data updated for the selected Machines.

Update Offline only

The Machines that were offline during the last scan or just added manually are marked with a red cross and may not have inventory information at all. To collect inventory data only for these Machines you should choose **Update Offline only** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. The update process starts and soon you'll have inventory data updated for these Machines.

Update Scan Age > 30 days

Lets consider that you do not have to update the inventory data constantly but would like to have at least some accuracy of the information collected about the remote Machines. In such a case you can always update only those Machines which were not scanned during the last 30 days. To perform such kind of an update choose **Update Scan Age > 30 days** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. The update process starts and soon you'll have inventory data updated for those Machines.

Update Custom

It may be so that 30 days is not a convenient period for update inventory data and you would like to update it more or less frequently. In such a case Network Inventory provides you with the feature of custom update. To perform such kind of an update choose **Update Custom** option from the drop-down of the **Update** button located on the tool bar above the **Machine Tree**. In the dialog opened `Pic 1` specify a date you are supposed to believe as the inventory time stamp and press **OK** button to proceed.
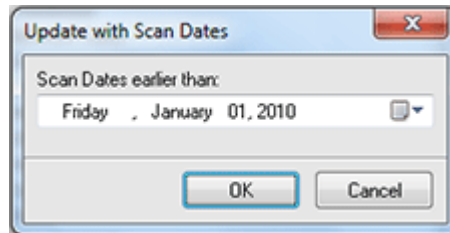
Pic 1. Selecting scan age for custom update

The update process starts and soon you'll have inventory data updated for the Machines matching the specified criteria.

Managing Exclude List

While performing inventory with Network Inventory you obviously do not need to bother about the freeware applications installed on the remote Machines along with the Windows updates, etc. For such a case Network Inventory provides you with an ability of specifying a list of the applications to be excluded from reporting and inventory data. To reach this list choose **Management Tools > Installed Applications > Maintain Exclude List** menu item or select the appropriate node in the **Machine Tree**. The **Installed Applications Exclude List** dialog will appear on the screen. `Pic  1`
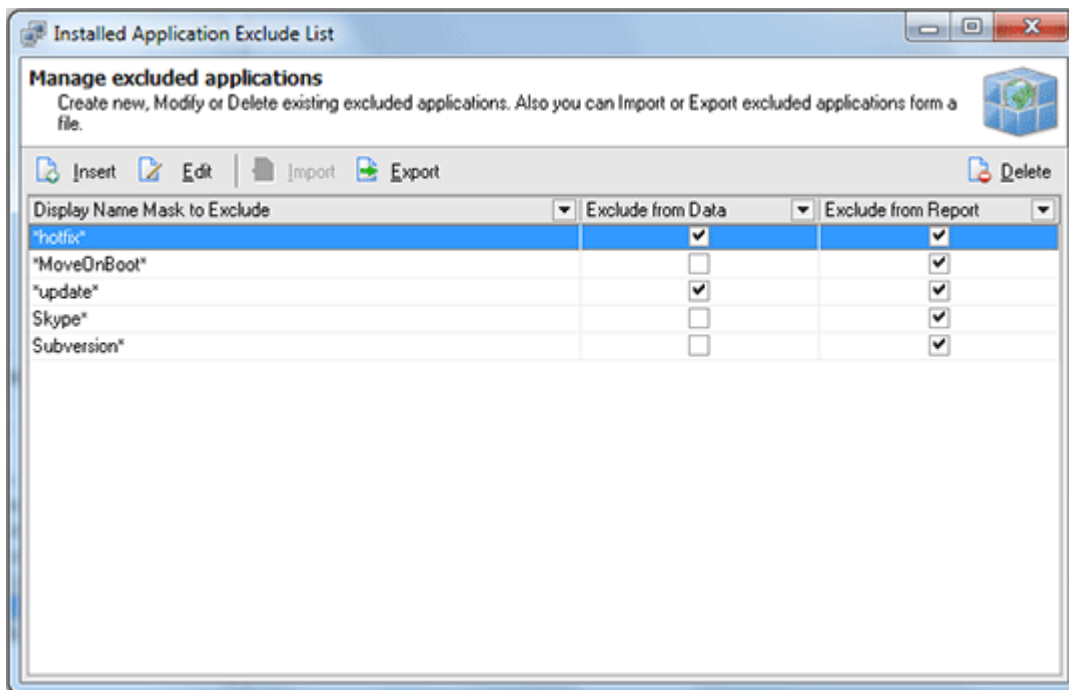
Pic 1. The Installed Applications Exclude List dialog

The **Installed Applications Exclude List** dialog shows you the list of applications that should be excluded from reports or Machine inventory data. You can add applications to this list, edit existing items, remove some, export the list to file for further usage and import it from the other file. To add a new criteria into exclude list press **Insert** button on the tool bar over the list. The **Installed Applications Exclude** dialog will appear on the screen. `Pic  2`
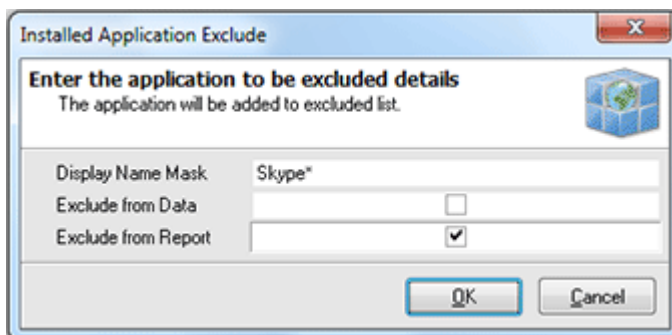
**Pic 2. Adding the criteria to the applications exclude list**

In the **Installed Application Exclude** dialog you are to specify a display name mask used as an excluding criteria and if the items matching the criteria should be excluded from the inventory reports, data or both. After all the required information is provided press **OK** button to proceed. The criteria will be added to the list.

Using Notes for Machines

How many times have you asked yourself a question "How can I remember what should I change on some Machine if there is dozens of them?". With Network Inventory you can simply leave a note on each Machine just like you've written this on a piece of paper. To leave a note you should find the Machine in the **Machine Tree** and select its **Notes** child node. The notes list will be shown on the right. Pic 1
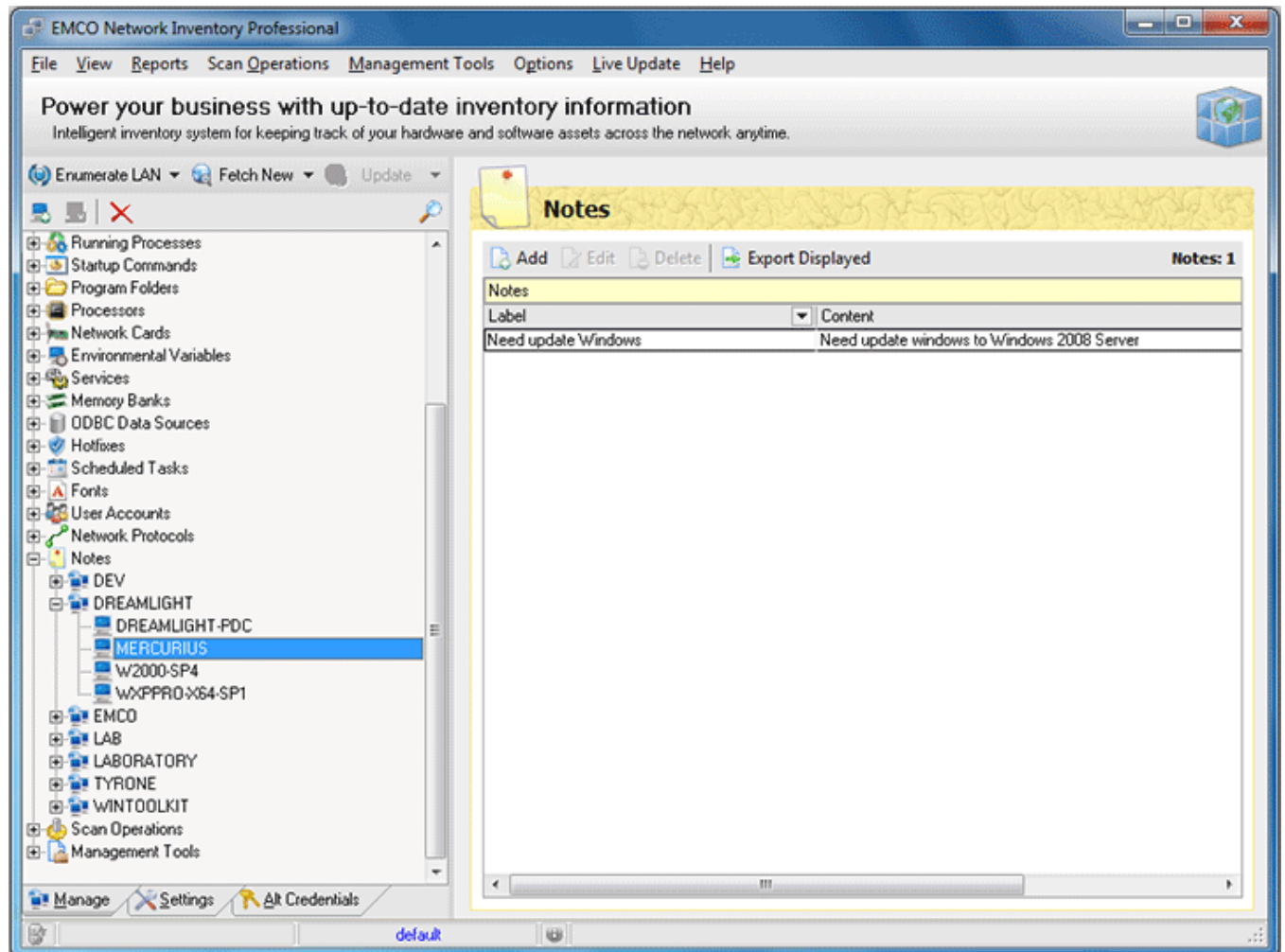
Pic 1. Notes left for the Machine

You can add as many notes as you wish, edit them or delete some. To add a note press **Add** button on the tool bar of the **Notes** area. The **Note Detail** dialog will appear on the screen. Pic 2
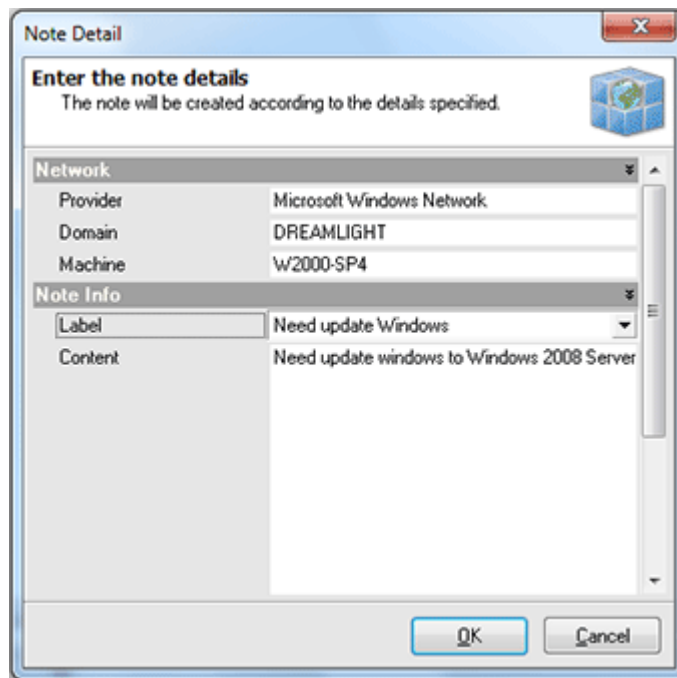
Pic 2. Specifying note details

In the **Note Details** dialog you are proposed to enter a note label for easier note identification along with a note content. After the required data is specified press **OK** button to proceed. The new note will be added to the list of the notes for this Machine.

## How can I get Inventory Information for not connected Machines?

Let us suppose you need to get inventory information for the Machines that are not connected to the corporate network, for example corporate notebooks. Network Inventory provides the solution for this problem – the stubs that come together with the product will help you to reach the target. This chapter will guide you through the process of using the stub files to collect inventory information for such Machines.

Prepare stub settings file

Firstly you should export the scan options to the stub options file. To do this switch to the **Settings** tab and press **Export** button on the tool bar. The **Export Stub Options** dialog will appear on the screen. `Pic 1`
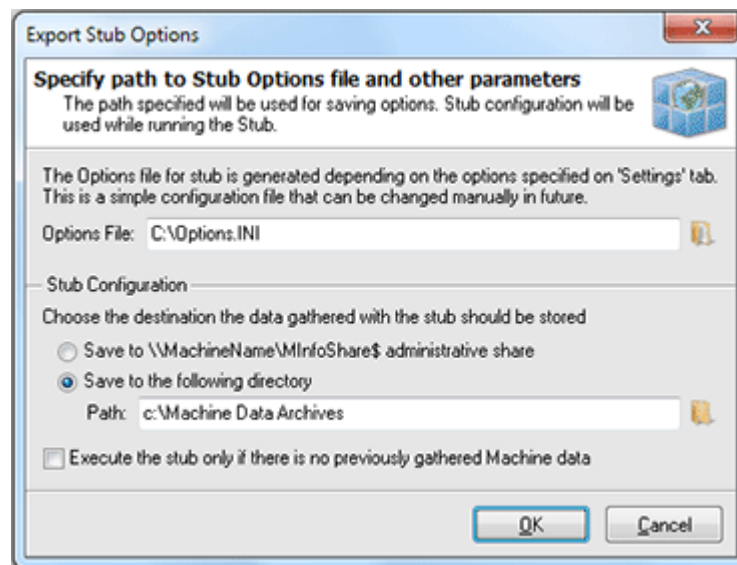
Pic 1. Exporting scan options to the stub settings file

In the **Export Stub Options** dialog you are to specify where to save the stub settings – this information should be provided to the **Options File** field. The other thing to define is the **Stub Configuration** – the configuration to be used while executing the stub. You can specify where to save the stub execution results along with the sign if the stub should execute if there is no scan results already saved on the Machine being scanned with a stub.

Executing scan on the Machine

You have prepared the stub settings file and are ready to execute it to scan the Machine for inventory data. To perform the scan you need to copy the **MinfoNT.exe** from the Stubs directory located in the Network Inventory installation directory along with the options you have exported to the Machine. Then simply execute the **MinfoNT.exe** on the Machine and it will save the scan data to the directory specified in the settings file.

Importing scan results into Network Inventory

After you have performed the scan on the Machine using the stub file you can then import the results to the Network Inventory. To import the results select the Machine you've scanned with the stub file in the **Machine Tree** (if it does not exist there you should add it manually), right click it and select **Load Machine Data > Load From Data File(s)**. The file system browser dialog will be opened to help you choose a file with inventory results. As soon as you proceed with choosing the file the data will be imported to Network Inventory and you can browse it the same way as if it was scanned from the Network Inventory interface.

Chapter 6: Inventory Reports

One of the main features of Network Inventory is automatic generation of inventory reports. You can include in a report any inventory information collected, build reports for all Machines from the Network or for an individual Machine with the effort of one mouse click. This chapter will guide you through the report generation process.

What's Inside

Building Report for an individual Machine

With Network Inventory you can generate and print an inventory report for an individual Machine with least effort. To create a report first of all you should select the interested Machine in the **Machine Tree**. The **Machine Details** area will appear on the right to the **Machine Tree**. Press **Report** button on the tool bar of the **Machine Details** area. The **Field Output Selection** dialog will appear on the screen. `Pic 1`
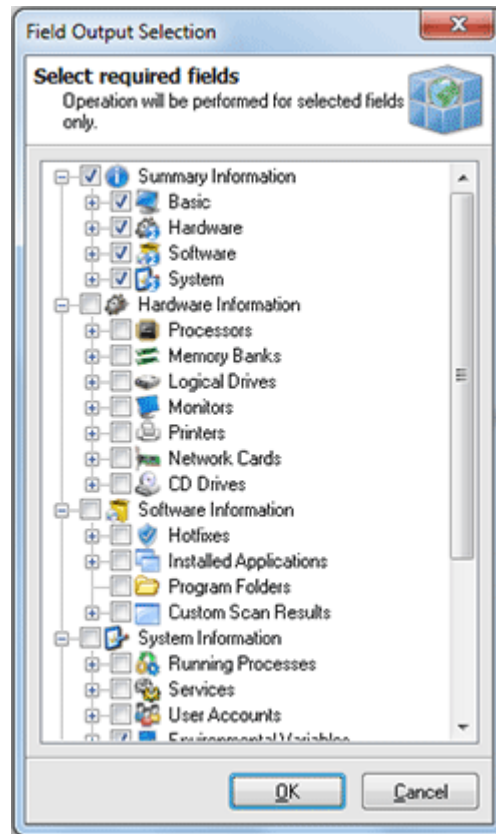
Pic 1. Choosing inventory data to be included into the generated report

In the **Field Output Selection** dialog you are proposed to choose the inventory data to be included into the report being generated. When you are ready with selection press **OK** button to proceed with report generation. After the report is generated the **Print Preview** dialog is displayed. Pic 2
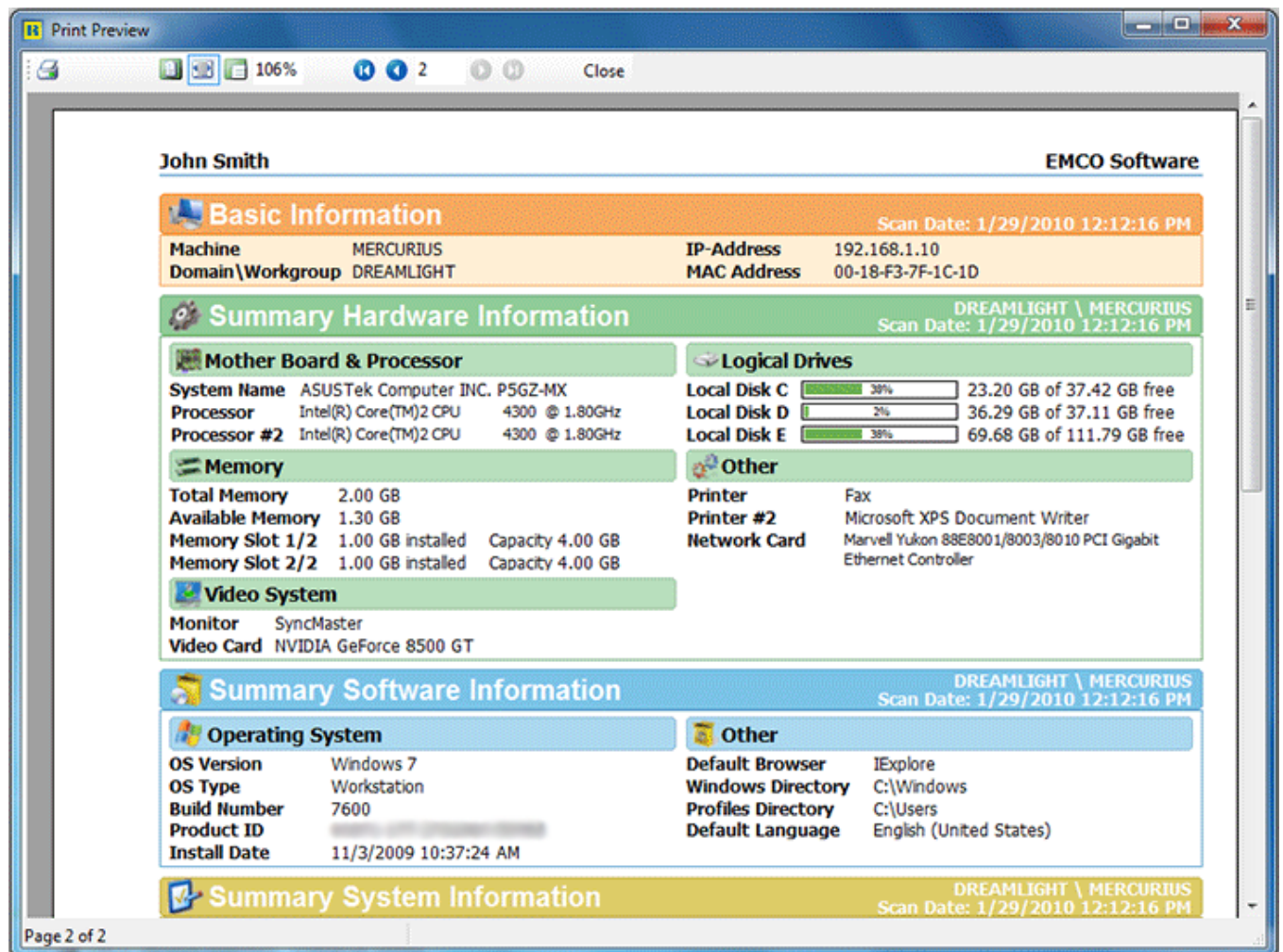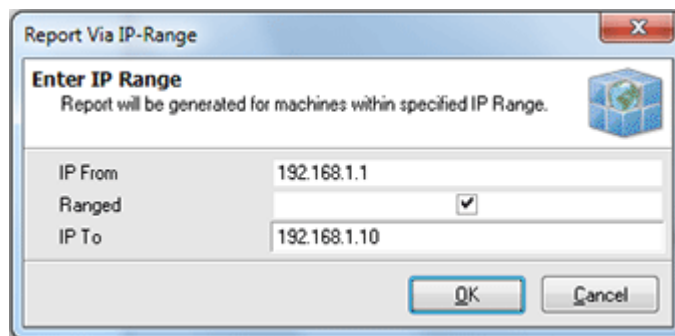

Pic 2. Inventory report print preview

In the **Print Preview** dialog you can review the generated report. If you are satisfied with the generated report press **Print** button on the tool bar to print it.

Report Inventory Information for all Machines

With Network Inventory you can generate and print or export to file an inventory report for all the Machine available from inventory database with least effort. You can preview and print such reports, save the reports to file and create custom reports. All this functionality is available from the Reports menu.

Preview and Print the Report

You can create and print a report for all Machines, using **Reports > Machine Data > Preview > All** item, or for the Machines from a specific IP range, using **Reports > Machine Data > Preview > Via IP Range**. If the IP range option is chosen then you are proposed to provide the range of addresses in the **Report Via IP-Range** dialog. `Pic 1`

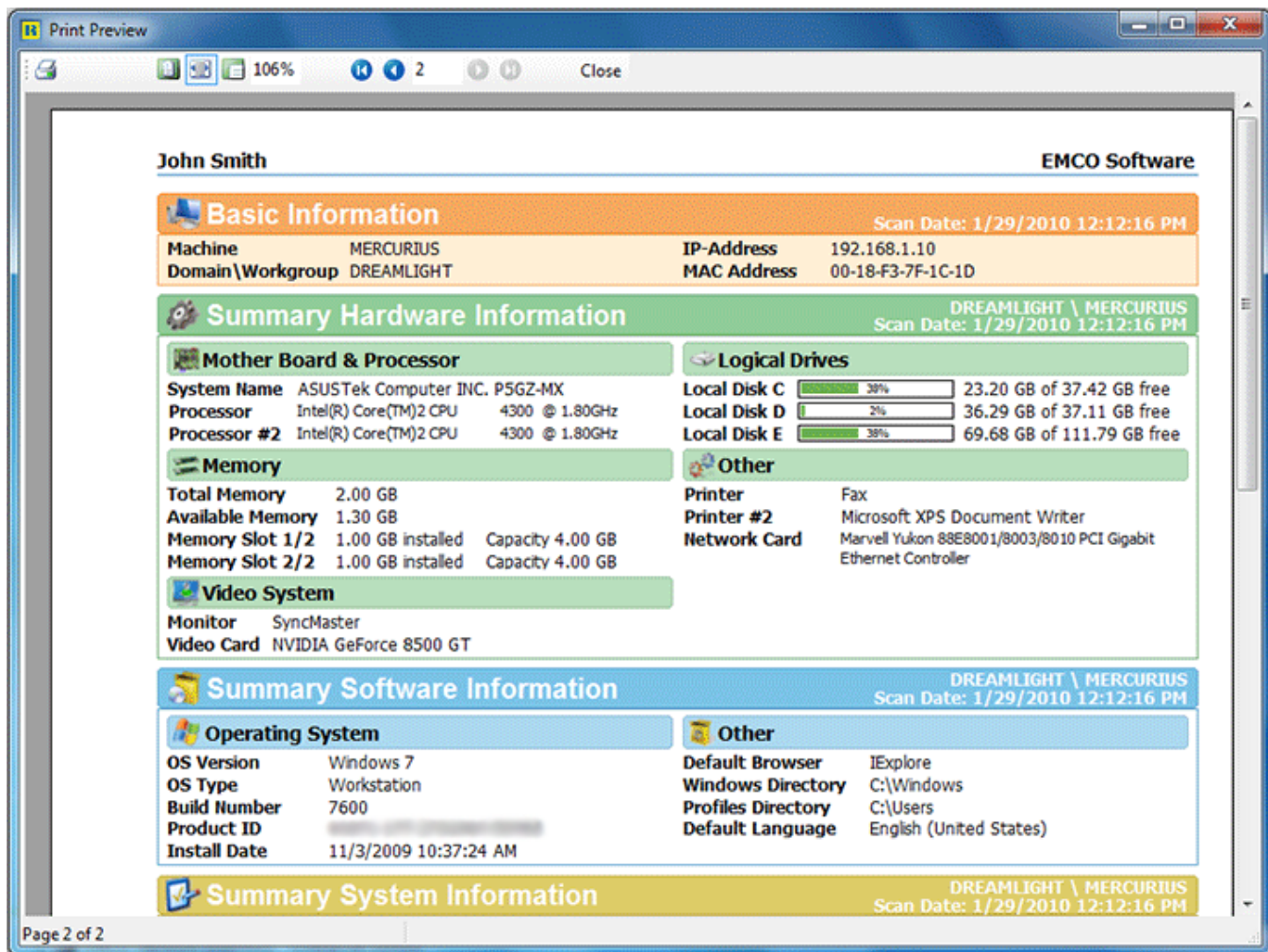

Pic 1. IP Range to create a report for

The next step is to specify the inventory data to be included into the report. **Pic 2**
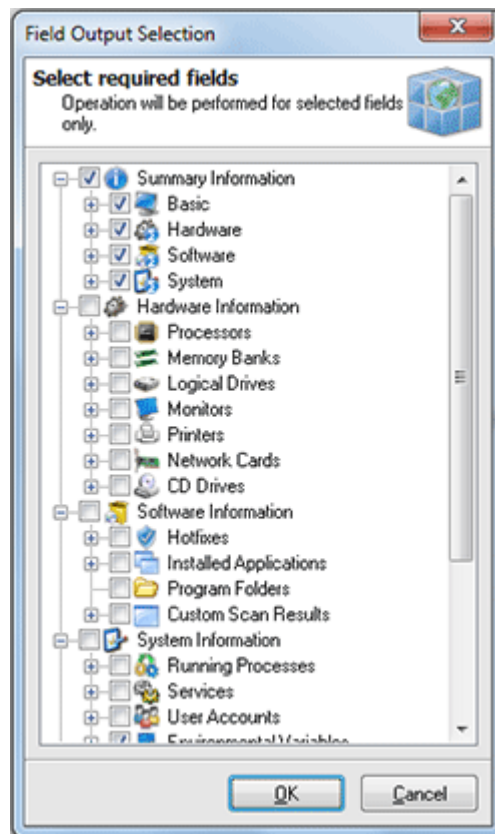
Pic 2. Choosing the inventory data to be included into the generated report

In the **Field Output Selection** dialog you are proposed to choose the inventory data to be included into the report being generated. When you are ready with selection press **OK** button to proceed with report generation. After the report is generated the **Print Preview** dialog is displayed. Pic 3
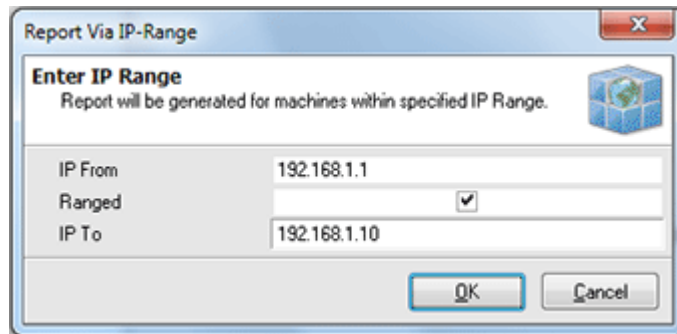

Pic 3. Inventory report print preview

In the **Print Preview** dialog you can review the generated report. If you are satisfied with the generated report press **Print** button on the tool bar to print it.

Save Report to File

You can create and save a report to file for all Machines, using **Reports > Machine Data > Export to File > All** item, or for the Machines from a specific IP range, using **Reports > Machine Data > Export to File > Via IP Range**. If the IP range option is chosen then you are proposed to provide the range of addresses in the **Report Via IP-Range** dialog. `Pic 1`

Pic 1. IP Range to create a report for

The next step is to specify the inventory data to be included into the report. `Pic 2`
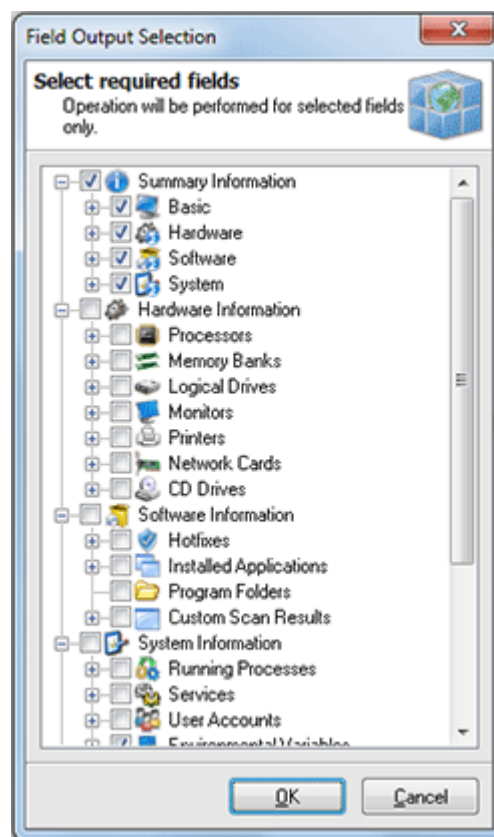
**Pic 2. Choosing the inventory data to be included into the generated report**

In the **Field Output Selection** dialog you are proposed to choose the inventory data to be included into the report being generated. When you are ready with selection press **OK** button to proceed with report generation. In the **Save As** dialog you are proposed to specify the location to save the file and the file format.

Report Machines containing specific inventory data

Network Inventory along with simple inventory reports allows you to create reports with a list of Machines containing specific inventory information. To create such report you should choose **Reports > Machines Containing...** item from the main application menu. The **Report Machines Containing** dialog will appear on the screen. `Pic 1`
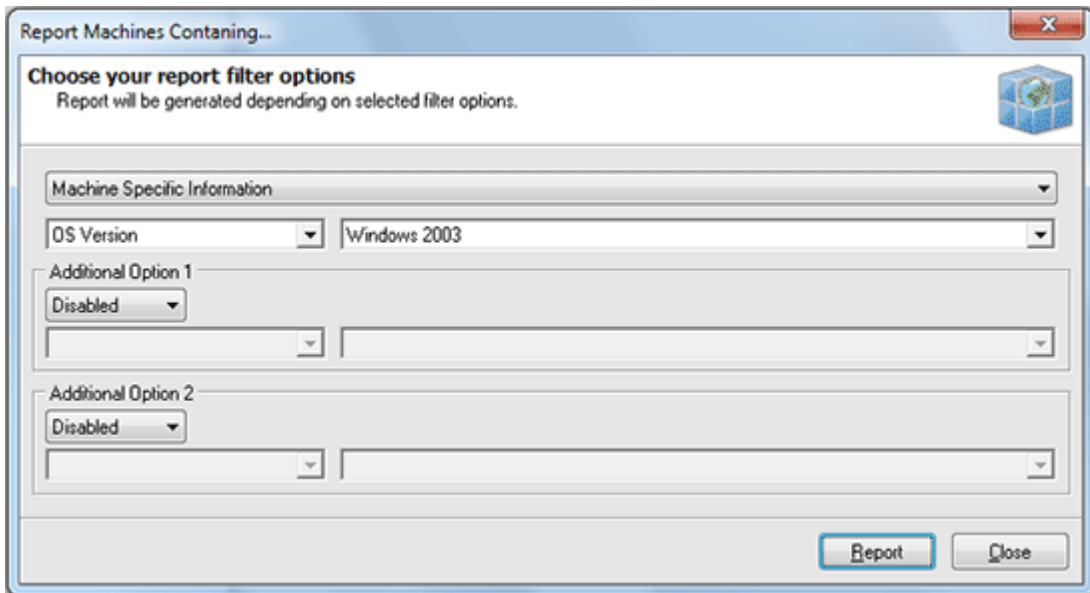
Pic 1. The Report Machines Containing dialog

In the **Report Machines Containing** dialog you are proposed to specify a criteria to filter the Machines for the list to include into the report. When the criteria is specified press **Report** button to proceed. The **Print Preview** dialog is displayed. `Pic 2`
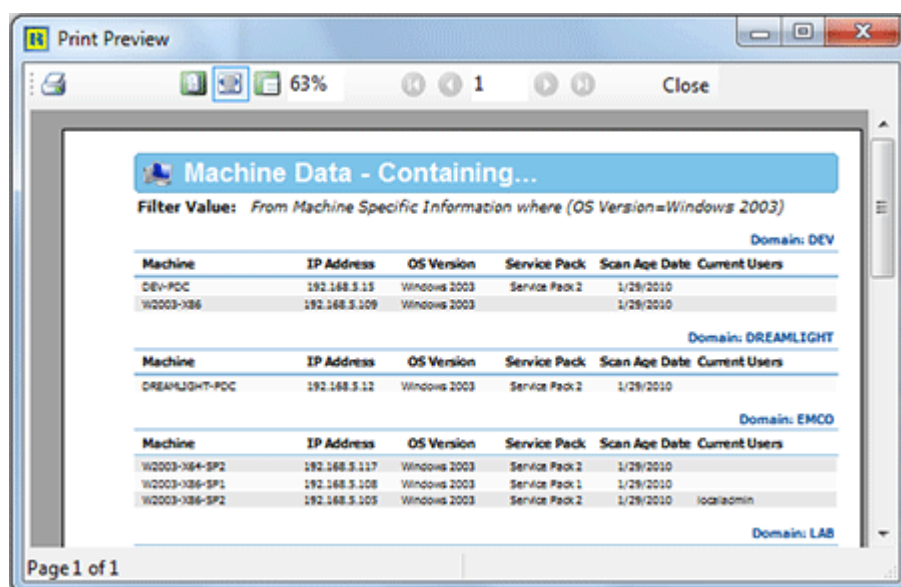
Pic 2. Custom report print preview

In the **Print Preview** dialog you can review the generated report. If you are satisfied with the generated report press **Print** button on the tool bar to print it.

Chapter 7: Alternate Credentials

Alternate credentials is the credentials to use for connecting the remote Machine that are stored between sessions of your work with the application. So you can specify the credentials once for Machine, Group or Network and they are automatically applied when it is required.

> ⚠ Although the alternate credentials are stored in strongly encrypted state, it is still possible for an intruder to decrypt the credentials.

Network credentials are used to set the same credentials for all the Machines in the network.

Individual Group credentials are used when several Domains or Workgroups with different administrative accounts are present in the network.

Individual Machine credentials are mainly used to set the alternative credentials for the separate Machines in the network.

What's Inside

Alternate Credentials Pane

Maintaining Alternate Credentials

How does it work?

How do I access another domain?

Alternate Credentials Pane

The **Alternate Credentials** pane is located on the left of the main application window under the **Alt Credentials** tab. `Pic 1` The representation is quite similar to the **Machine Tree** one, but also contains credentials associated with each network item. This tree can be built both using the auto creation functionality and manually. See **Maintaining Alternate Credentials** section for details.
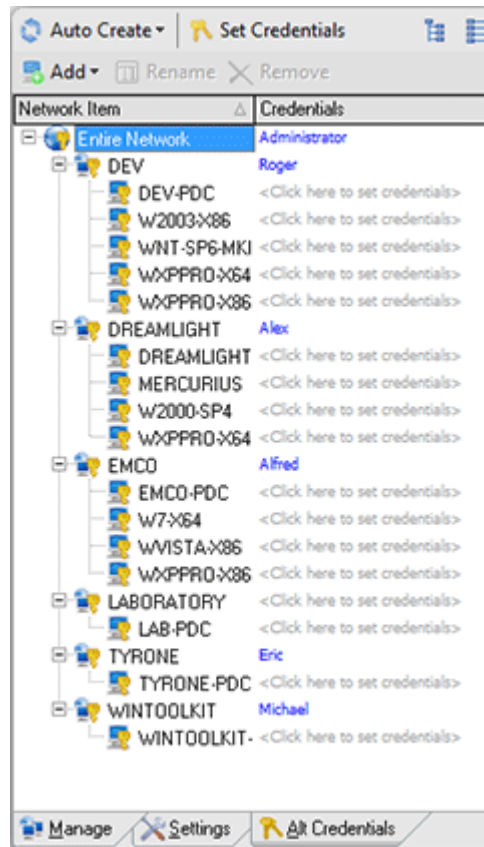
Pic 1. Alternate Credentials tree

Item Icon represents the item type:

🌐 Root of the Alternate Credentials.

🖥️ Machine Group (may be both Domain or Workgroup) credentials.

🖥️ Machine credentials.

Item Name - the name of the item.

Credentials Part - shows the login name to use while connecting to remote Machines or a hint if credentials are not set. In-place edit shows the pop-up window to specify credentials. `Pic 2`

The following actions are available to manage the **Alternate Credentials**:

Set Credentials

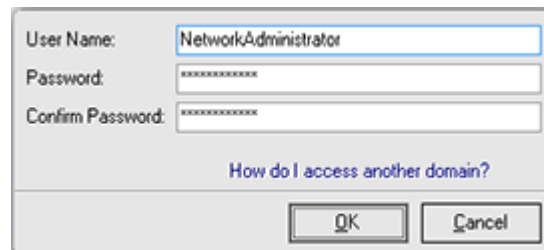Opens the pop-up window to specify the credentials to apply for selected item. `Pic 2` Is available from the tool bar over the **Alternate Credentials** pane and pop-up menu of any item in the **Alternate Credentials** pane. Also the same can be invoked by a click on ⬇ button of credentials part in-place edit.

Pic 2. Specifying Alternate Credentials

> 💡 While setting an alternate credential's user name pay attention to the domain it will be used for. This information is shown in **Log on to: <Name>** field, where <Name> is the domain or computer name the account with the following user name is present. To access another domain see How do I access another domain.

Reset Credentials

Removes the associated credentials from the item. It can be invoked from the pop-up menu of any item in the **Alternate Credentials** pane. It is also available in credentials part in-place edit and is represented with ❌ button.

Maintaining Alternate Credentials

To specify alternate credentials in Network Inventory the **Alternate Credentials** pane should be filled with the information on the network structure to set the credentials for. This can be reached both automatically, on a basis of the network structure in the **Machine Tree** or by manually adding each element to provide credentials for.

Auto Create

Automatic creation is used to build the **Alternate Credentials** tree structure on a basis of the network structure in the **Machine Tree**. You can create the appropriate credentials nodes for the Groups only or for the Groups and Machines, depending on a selected option. Both this options are available in the drop-down of the **Auto Create** button located on the tool bar of the **Alternate Credentials** pane.

Add Group

It is also possible to add a group manually using the **Group** option of the **Add** button located on the tool bar of the **Alternate Credentials** pane. After the group is created it is displayed as a child of the item selected. You can rename it and set the appropriate credentials.

Add Machine

To add a single Machine to the alternate credentials choose **Machine** option of the **Add** button located on the tool bar of the **Alternate Credentials** pane. After the Machine is created it is displayed as a child of the item selected. You can rename it and set the appropriate credentials.

Rename

When you are creating a credentials item manually or the network item name is changed within your network environment you are to rename the credentials node for this item. To rename the item select in the **Alternate Credentials** pane and press **Rename** button on the tool bar of the **Alternate Credentials** pane.

Remove

Sometimes you do not need the specific credentials for the network item any more. Of course you can just reset the credentials for this item, but if you want your credentials structure to be accurate you are to remove such item. To remove the item select it in the **Alternate Credentials** pane and press **Remove** button on the tool bar of the **Alternate Credentials** pane. The confirmation dialog will appear on the screen – press **Yes** button to proceed with removing.

How does it work?

<%PRODUCTNAME%> allows you to specify credentials both for groups of Machines and for individual Machines. Credentials can be provided with or without explicit specification of the domain. The domain may be specified by using the User Principle Name or Down-Level Logon Name.

User Principal Name

The User Principal Name (UPN) format is used to specify an Internet-style name, such as *UserName@Example.Emco.local*. The following table summarizes the UPN components.

Component	Example
User account name. Also known as the logon name.	UserName
Separator. A character literal, the at sign (@).	@
UPN suffix. Also known as the domain name.	Example.Emco.local

A UPN can be defined implicitly or explicitly. An implicit UPN has the following form: *UserName@FQDN*. An implicit UPN is always associated with the user's account, even if an explicit UPN is not defined. An explicit UPN has the form *Name@Suffix*, where both the name and suffix strings are explicitly defined by the administrator.

Down-Level Logon Name

The down-level logon name format is used to specify a domain and a user account in that domain, for example, *DOMAIN\UserName*. The following table summarizes the components of a down-level logon name.

| Component	Example
NetBIOS domain name.	DOMAIN
Separator. A character literal, the backslash (\).	\
User account name. Also known as the logon name.	UserName

Beside an explicit domain specification, you can use an implicit one by providing the Down-Level Logon Name with the '.' character instead of the domain part (*.\UserName*). In such case, the '.' character is replaced by the NetBIOS name of the Machine to connect to.

If the user name is provided without an explicit or implicit domain specification, the application generates one of the user name formats described above using the following rules:

- If credentials are specified on the Machine node, the following Down-Level Logon Name is generated for connection: *MACHINE\UserName*, where '*MACHINE*' is the NetBIOS name of the Machine the application is connecting to and '*UserName*' is the specified user name.

- If credentials are specified on the Network or Group node, than the group the Machine is located in is used to form the user name used for connection. If the group is an Active Directory domain, then the following UPN name is formed: *UserName@FQDN*, where '*UserName*' is the specified user name and '*FQDN*' is a fully qualified name of the domain the Machine is located in. In case the group is not an Active Directory domain, the following Down-Level Logon Name is generated for connection: *DOMAIN\UserName*, where '*DOMAIN*' is the NetBIOS name of the group the Machine is located in and '*UserName*' is the specified user name.

## Examples for Alternate Credentials specification

Specifying Alternate Credentials for complex network environments may not be a trivial task, and this chapter is written to show you some examples that can help you with this task. Let's assume we have the following network structure:
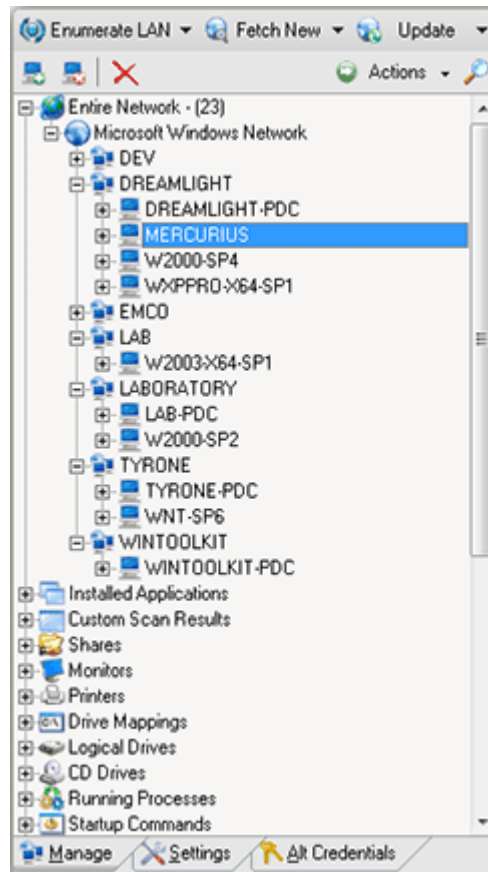
Consider the following methods of setting the alternate credentials:

1. The Alternate Credentials are not set for any item. Retrieving data from the network will take place using the current user credentials.

Example
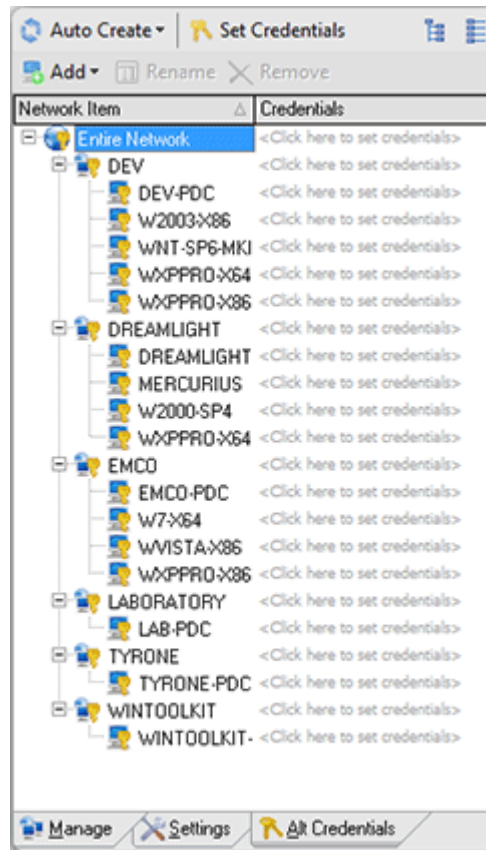
2. The Alternate Credentials are set for the Network item. Retrieving data from the network will take place using the credentials set for the Network.
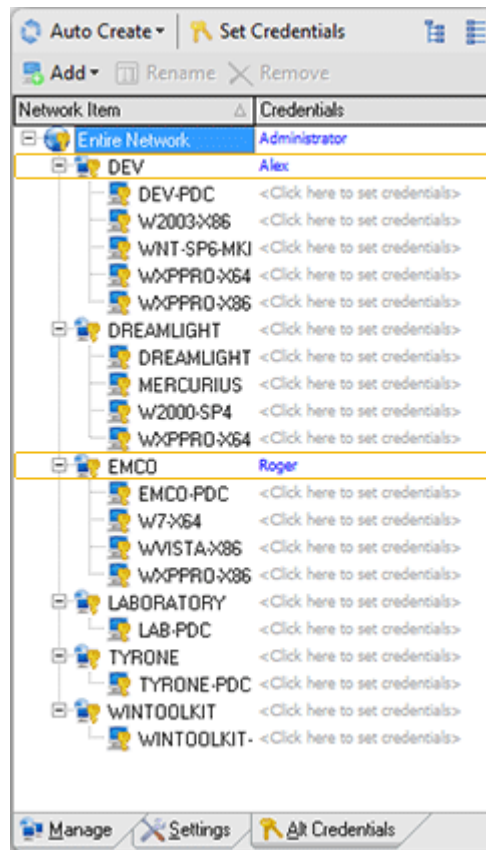
Example
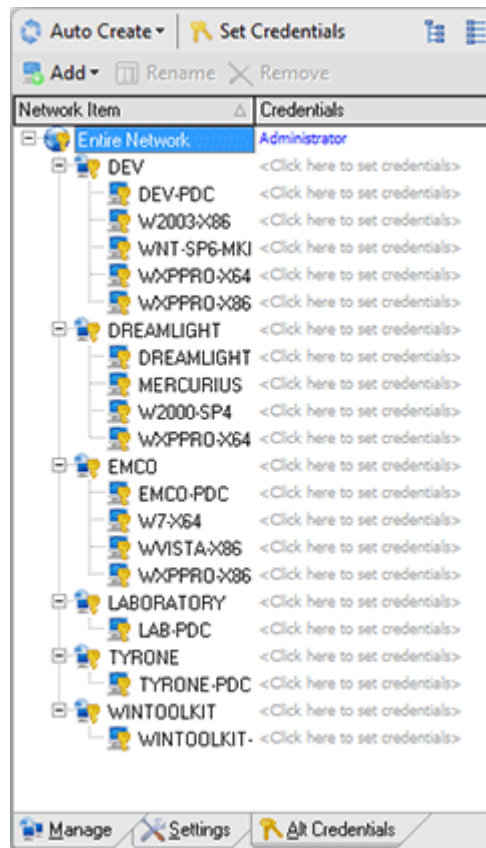
3. Two different Alternate Credentials are set for the *EMCO* and *DEV* groups. Retrieving data from the *DEV* group Machines will take place using the credentials set for the *DEV* group, data from the *EMCO* group Machines will be retrieved using the credentials set for the *EMCO* group.

Example

4. The Alternate Credentials are set for the *Dev-PDC* Machine. The current user credentials will be used for retrieving data for all the Machines in the network except for those from *Dev-PDC*, for which the respective preset credentials will be used.

Example
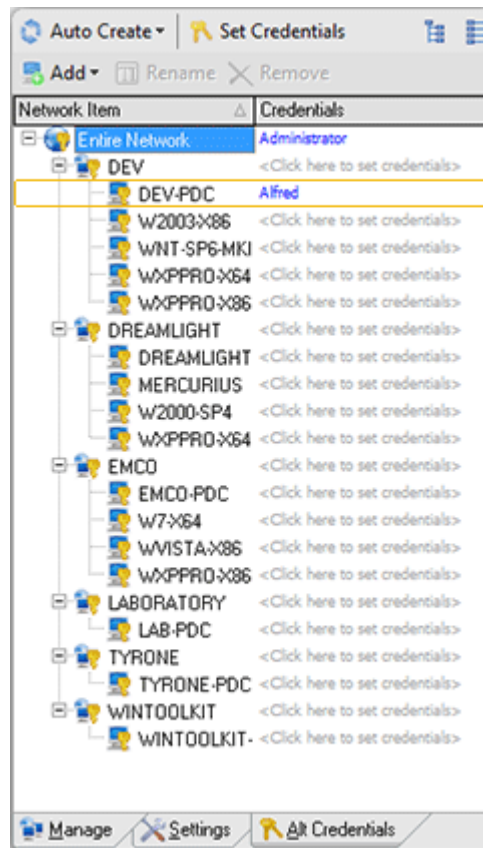
5. Three different Alternate Credentials are set for the *Network*, the *DEV* group and the *Dev-PDC* Machine. Retrieving data from the Emco group computers will take place using the credentials set for the *Network*, the *DEV* group will use the credentials specified for the *DEV* group and for *Dev-PDC* the credentials set for *Dev-PDC* will be used.

Example
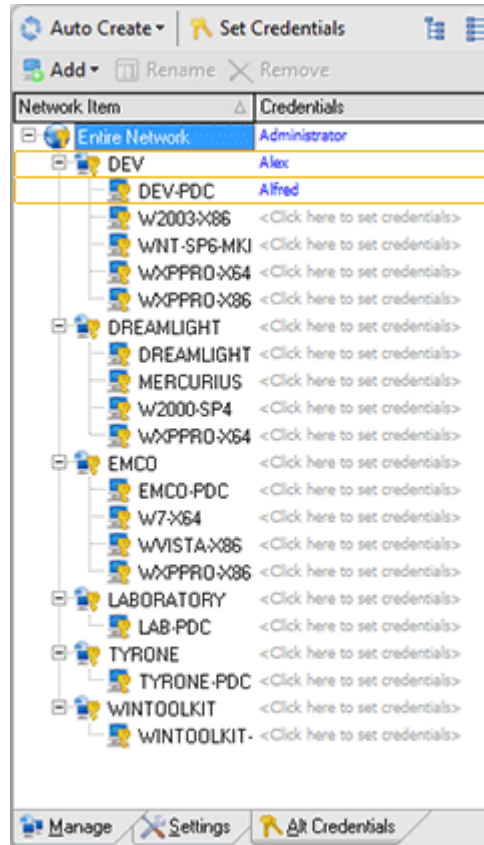
How do I access another domain?

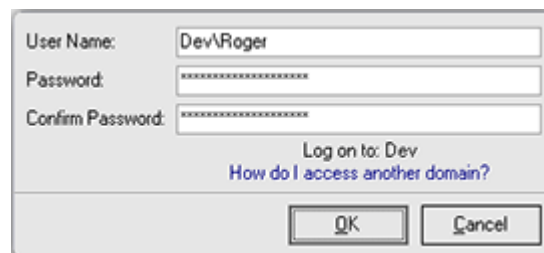By default the credentials used for the Machine are applied as credentials for Domain remote Machine is located in. It is displayed in **Log on to** field of credentials edit. In case you need to use the remote Machine's local account or the account from the Domain that differs from the provided by default you should specify the Machine or Domain, account is located, in name explicitly. **Log on to** field value is then changed to help you understand clearly which Domain credentials are used.

To do the described you should input a value of the following format to the User Name field of alternate credentials pop-up edit.

<**Domain name**>\<**User name**> - for the explicit specification of Domain account

<**Machine name**>\<**User name**> - for the explicit specification of the remote Machine account

Pic 1. Providing specific credentials

> 💡 Domain provided by default, if applicable, is displayed in Log on to field of credentials alternate pop-up edit.

Chapter 8: Additional Capabilities

It is supposed that you have already introduced yourself to the main features of Network Inventory and we would like to introduced to you some special built-in sugar. The capabilities described in this part are added to make your every day inventory work easier and more comfortable. This chapter will show you how to use external tools with Network Inventory, specify a note label to be used while creating **Machine Tree** and exclude the Machines that should not be inventoried from the enumeration.

What's Inside

Using External Tools together with Network Inventory

Excluding specific Machines from Enumeration

Note Labels

# Using External Tools together with Network Inventory

Network Inventory provides you with an ability of using any external tool you want with the product itself without any difficulties. The tool will be added as a sub menu item of the Tools item for the pop-up menu of the **Machine Tree**. When adding a command to launch the external tool you can use *%MACHINE%* placeholder that will be replaced to the name of the selected Machine.

Let us for example add the **Ping** command to be used as an external tool. To review the tools defined select **Options > Configure Tools** item from the main application menu. The **Configure Tools** dialog will appear on the screen. `Pic 1`
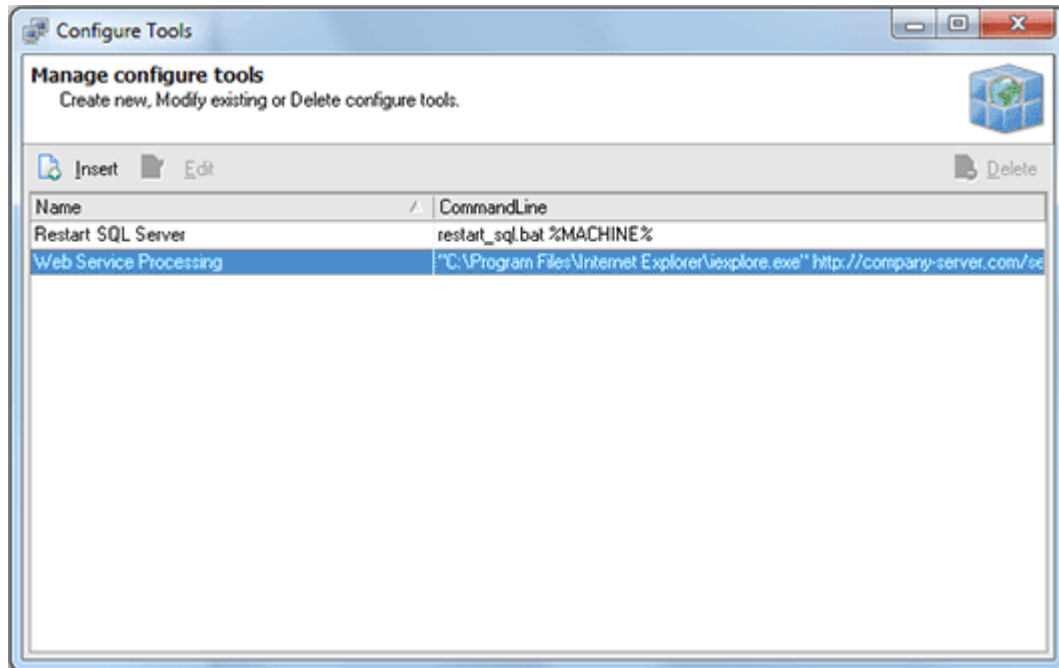
Pic 1. The Configure Tools dialog with a list of defined tools

To add a new tool press **Insert** button on the tool bar over the tools list. The **Tools Item** dialog will appear to specify the tool information. `Pic 2`
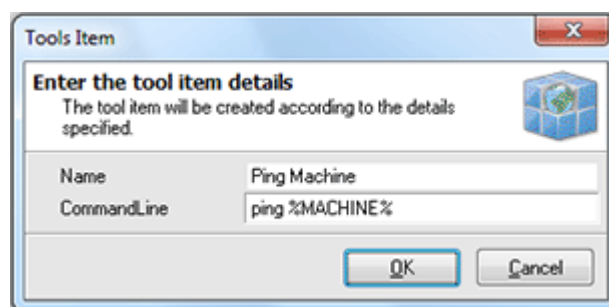
Pic 2. Specifying the tool information

Fill the **Name** and **Command Line** fields with the values required – for ping functionality let us type *Ping Machine* as name and *ping %MACHINE%* as command line. Press **OK** button to add the tool. When you are finished with adding, editing or removing the tools press just close the **Configure Tools** dialog.

All the tools added are available from the **Tools** item of the **Machine Tree** pop-up menu.
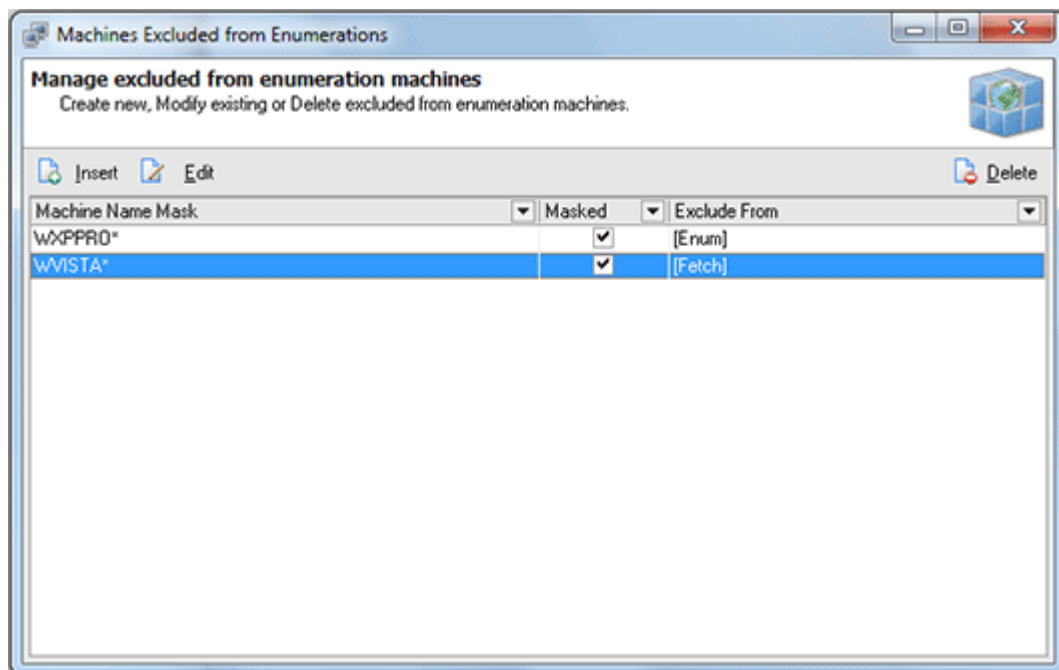

Excluding specific Machines from Enumeration

Network Inventory allows you to skip the Machines defined from enumeration, fetch and update processes. This can be used if the corporate network contains the Machines that should not by inventoried, for example personal notebooks of the workers. You can exclude Machines by name mask or by IP range.

Excluding Machines by Name Mask

To specify the Machines name mask to be excluded from enumeration choose **Options > Exclude from Enumeration > Machines** item from the main application menu. The **Machines Excluded from Enumeration** dialog will appear on the screen. `Pic 1`

Pic 1. The Machines Excluded from Enumeration dialog

The **Machines Excluded from Enumeration** dialog shows the list of defined mask criteria to be used for excluding. To add a new criteria press **Insert** button on the tool bar above the criteria list. The **Excluded Machines** dialog will appear on the screen. `Pic 2`

Pic 2. Specifying the exclusion criteria

In the **Exclude Machines** dialog you should specify a Machine name mask criteria along with the process for the Machines to be excluded from. When all the required data is specified press **OK** button to proceed. You can add as many criteria as you wish, edit criteria or remove some.
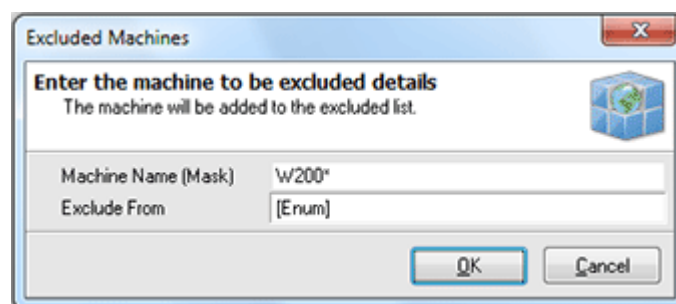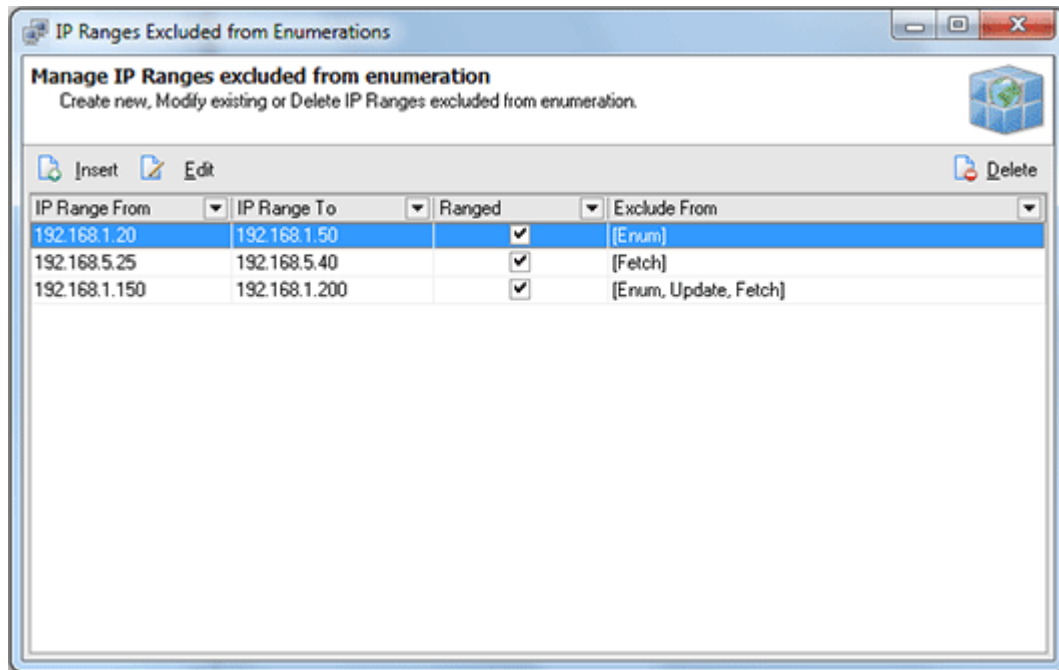
Excluding Machines by IP Range

To specify the Machines IP range to be excluded from enumeration choose **Options > Exclude from Enumeration > IP Range** item from the main application menu. The **IP Ranges Excluded from Enumeration** dialog will appear on the screen. `Pic 3`

Pic 3. The IP Ranges Excluded from Enumeration dialog

The **IP Ranges Excluded from Enumeration** dialog shows the list of defined criteria to be used for excluding. To add a new criteria press **Insert** button on the tool bar above the criteria list. The **Excluded IP Ranges** dialog will appear on the screen. `Pic 4`

Pic 4. Specifying the exclusion criteria

In the **Excluded IP Ranges** dialog you should specify a start IP address, if the addresses are ranged and if so an end IP address along with the process for the Machines to be excluded from. When all the required data is specified press **OK** button to proceed. You can add as many criteria as you wish, edit criteria or remove some.
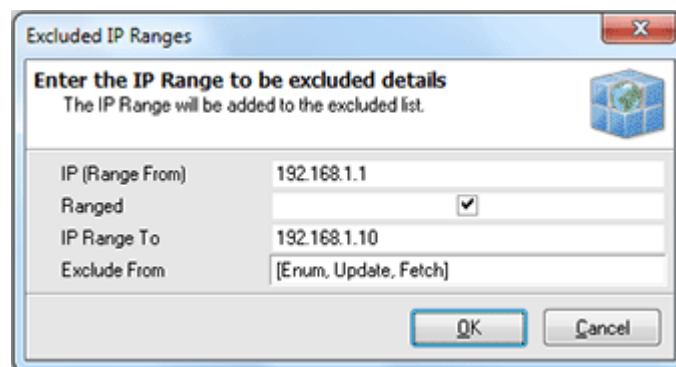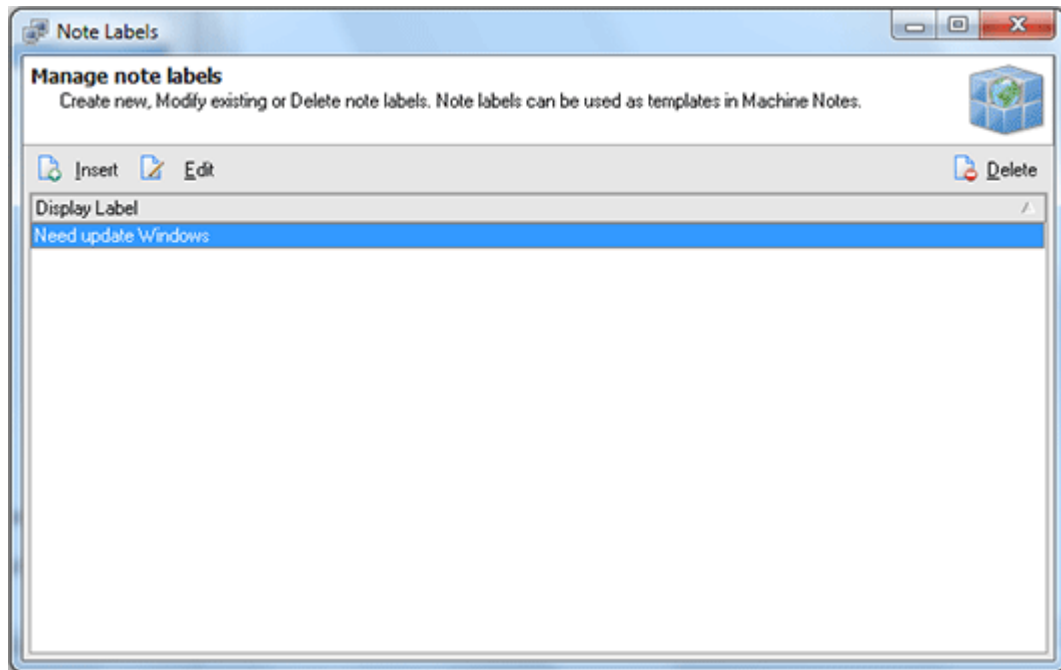
Note Labels

Network Inventory allows you to add notes to Machines specifying a note label and its content. If you face the situation when the labels are similar for different Machines you probably do not want to input the label each time. In such a case you can specify a list of the predefined note labels. Choose **Options > Note Labels** menu item from the main application menu. The **Note Labels** dialog will appear on the screen. Pic 1

Pic 1. The Note Labels dialog

The **Note Labels** dialog shows you the list of note labels defined. To add a new label press **Insert** button on the tool bar above the labels list. The **Note Label** dialog will appear on the screen. Pic 2
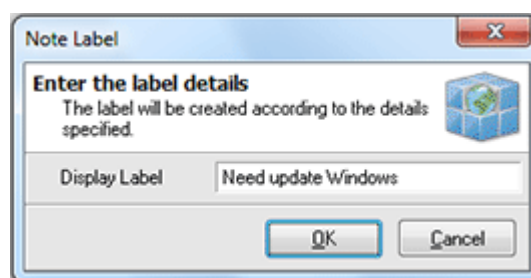
Pic 2. Adding a predefined note label

In the **Note Label** dialog you are to provide a label name. When you are ready press **OK** button to proceed with addition. You can add as many predefined labels as you wish, edit them or delete some.

Chapter 9: Application Preferences

Network Inventory comes with a wide range of preferences available for flexible configuration. It is possible to configure network scan process, automation features and reports view style. To reach the preferences choose the **File > Preferences...** command from the main application menu.

What's Inside

Scanning Settings

Scanning settings are designed to let you configure processing remote Machines in the most optimal way depending network structure, which allows to increase scan performance. **Pic 1** To configure **Scanning** settings choose the **File > Preferences...** command from the main application menu and switch to **Scanning** preference page using the appropriate link in the navigation bar on the left of **Preferences** dialog or switch to the appropriate tab. You are proposed to configure network enumeration type, Machines availability detection, administrative access assurance and hyper-threading technology.
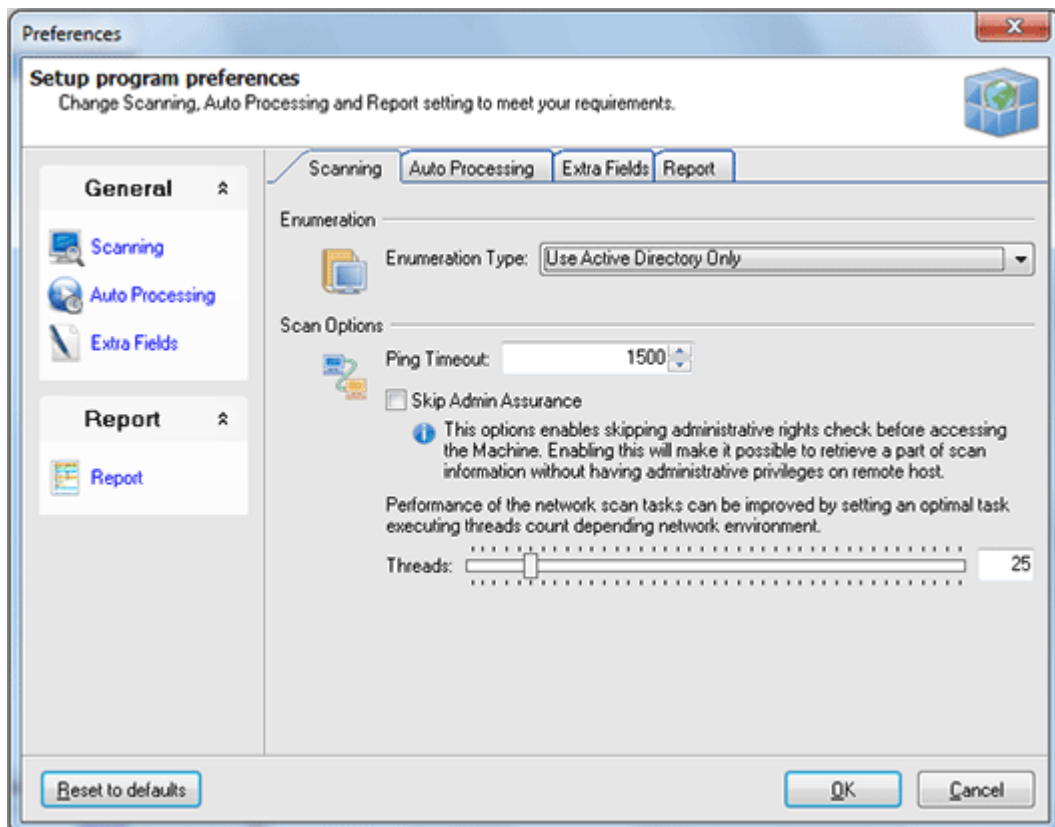
Pic 1. Configuring scanning settings

Enumeration Type specifies the way of performing network scan for Machines.

Active Directory scan allows you to get more information on your network structure and runs significantly faster than Computer Browser one. Also it is not needed for all network computers to be turned on cause the information on the network is gathered directly from the domain controller. But on the other hand this type of enumeration requires access to the domain controller and also won't find Machines that are not registered in Active Directory database.

Searching for computers using the Computer Browser will result in finding all the Machines that are turned on and visible from your one during the Enumeration process.

In the combined mode the application firstly performs Active Directory scan and then adds the computers found using Computer Browser.

Scan Options define the Machine availability detection options along with the hyper-threading configuration.

The Machine availability detection within Network Inventory is performed by pinging the remote Machine. You can specify a timeout to be used for each ping in the **Ping Timeout** field.

Skip Admin Assurance option enables skipping administrative rights check before accessing a Machine. Enabling this options will make it possible to retrieve a part of the scan information without having administrative privileges on the remote Machine.

The ultimate hyper-threading technology provided by EMCO allows you to perform network tasks in parallel to reach the highest available performance. You can set optimal task executing threads count depending network environment in the **Threads** field.

Auto Processing Options

The **Auto Processing** options are designed to control the automation features of Network Inventory. `Pic 1` To configure **Auto Processing** options choose the **File > Preferences…** command from the main application menu and switch to **Auto Processing** preference page using the appropriate link in the navigation bar on the left of Preferences dialog or switch to the appropriate tab. Here you can enable the automatic fetch and update processes and specify if Network Inventory should automatically create file reports.
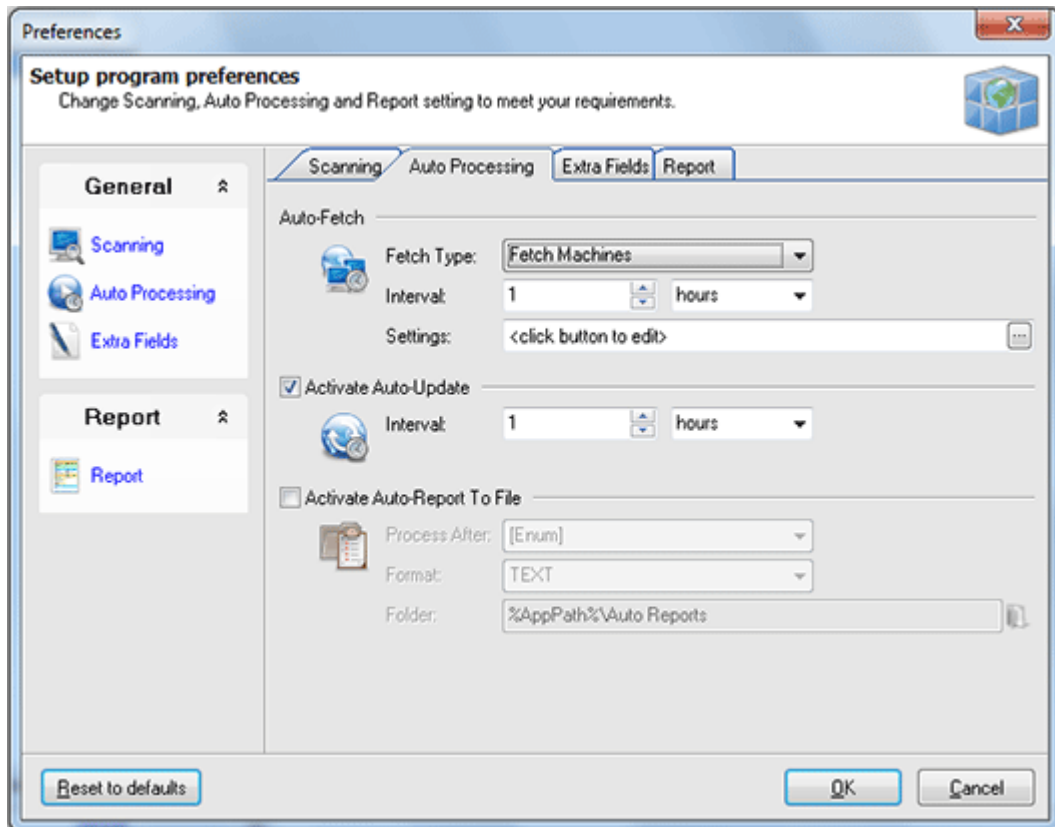
Pic 1. Configuring auto processing options

Auto-Fetch

To activate the auto fetch process you should choose the auto fetch type from the drop-down of the **Fetch Type** field. You can choose between the Machines fetch and fetching via IP range. When the fetch type is chosen you should specify an automatic fetch interval along with fetch settings.

Auto-Update

To enable automatic inventory data update you should check the **Activate Auto-Update** option and specify an automatic update interval in the **Interval** field.

Auto-Report to File

You can also enable the automatic reporting into file on the end of enumerate, fetch and/or update process by checking the **Activate Auto-Report to File** option. In the **Process After** field you are to specify the process after which the report should be created. Optionally you can change a report file format and location to save report to.

Extra Fields

The **Extra Fields** are designed to allow you specify custom fields for Machines to store user data that is not changed between inventory scans. You can bind any information required to this fields. The captions for those fields are defined on **Extra Fields** preference page. **Pic 1** To configure **Extra Fields** choose the **File > Preferences...** command from the main application menu and switch to **Extra Fields** preference page using the appropriate link in the navigation bar on the left of **Preferences** dialog or switch to the appropriate tab.
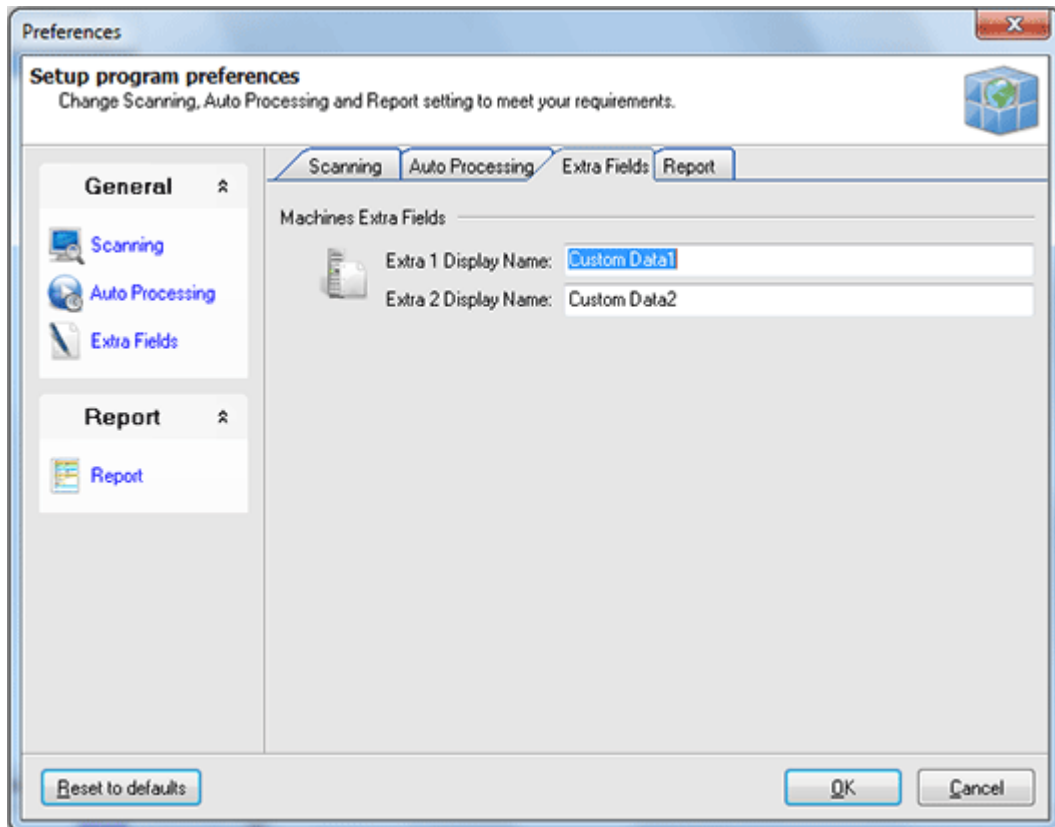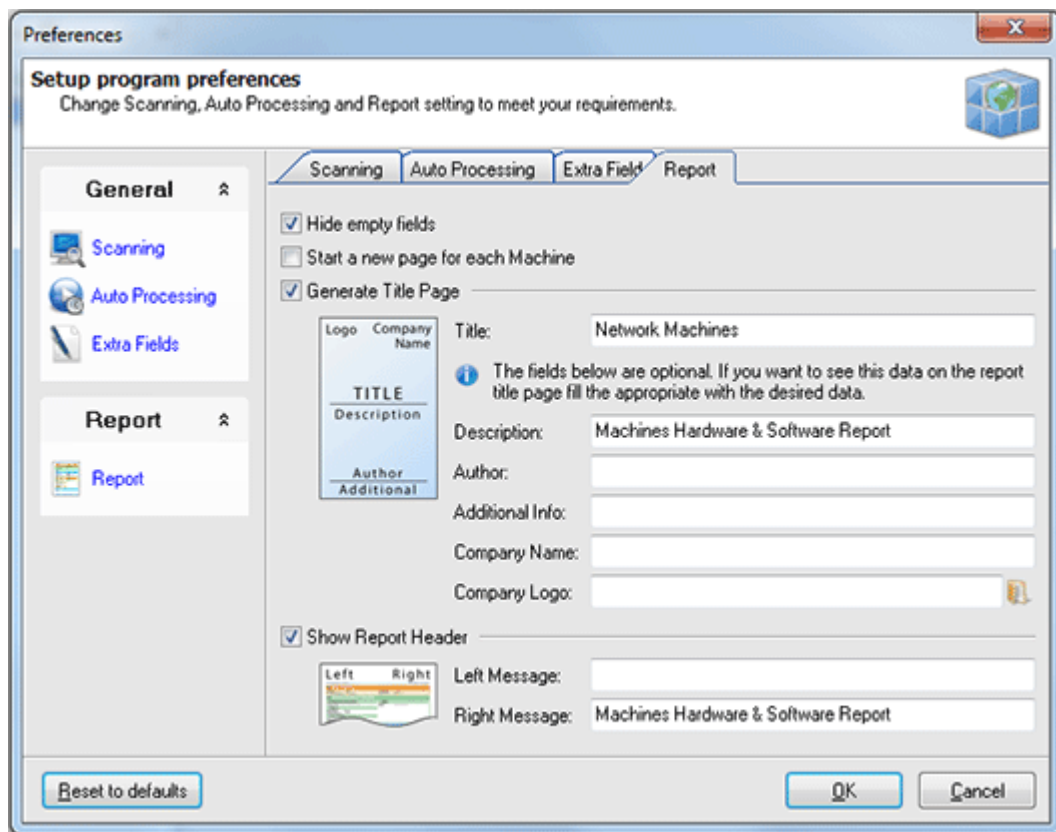

Pic 1. Configuring Extra Fields

The **Machines Extra Fields** group allows you to provide captions for the custom fields bound to each inventoried Machine. Captions should be defined in the **Extra 1 Display Name** and **Extra 2 Display Name** fields.

Report Configuration

The **Report** configuration settings are designed to help you set up the reports representation. **Pic 1** To set up **Report** configuration choose the **File > Preferences...** command from the main application menu and switch to **Report** preference page using the appropriate link in the navigation bar on the left of **Preferences** dialog or switch to the appropriate tab.

Pic 1. Configuring reports representation

On the **Report** page you are proposed to specify if the empty fields are included into a generated report, if the report title page is also generated and if the header is added to each report page.

Title Page Representation

If you have enabled the generation of a title page you can specify data to be displayed on it. The thumbnail on the left to the input fields can be used to understand where the data will be displayed on the title page. You are proposed to specify a **Title**, **Description**, **Additional Info**, **Company Name** and **Company Logo**.

Header Text

The header text if enabled is displayed on the top of each report content page. You can specify texts to be displayed on the left and on the right of a report content pages header.

Chapter 10: Error Log

The Error Log is designed to store the information on the problems taking place during the network inventory along with the other informational messages. This log can help you to understand if the inventory process completed successfully and if not which problems should be resolved to proceed with the inventory. To open the **Error Log** you should select Management **Tools > View Error Log-File** item of the main application menu or select **View Error Log-File** node under the **Management Tools** one in the **Machine Tree**.
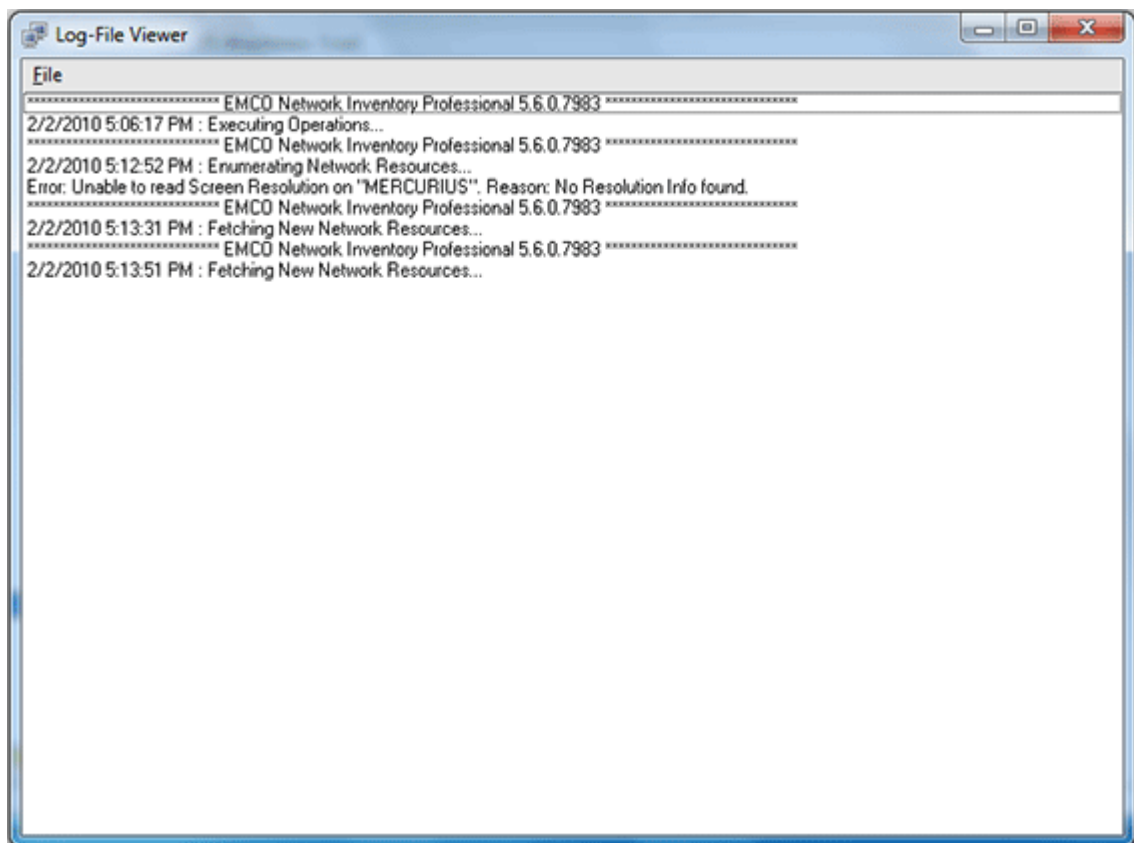

Pic 1. Log-File Viewer

The **Log-File Viewer** shows you the error log in a form of a plain text. You can save this information to any file or print it.

Chapter 11: Live Update

Network Inventory can be easily updated with just one mouse click. The update process is performed through the Internet connection using proxy settings configured.

To check for updates, click **Check for Updates** command from the **Live Update** application menu. Network Inventory will check if the updates are available and if so the **Live Update Wizard** `Pic 1` will appear on the screen.
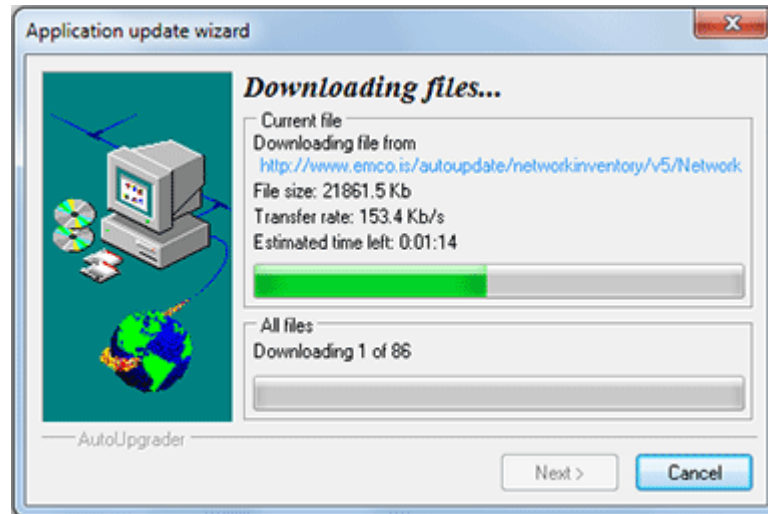

Pic 1. Live Update Wizard

The **Live Update Wizard** will introduce you to the changes made in a newer version and guide you through all update process, showing detailed download progress. When the download is finished the application will be restarted to perform actual update.

Configuring Live Update settings

Network Inventory can automatically check for updates when the Internet connection is active, but it is possible to turn this feature off using the Live Update configuration. Also the Internet connection is required to provide the **Live Update** functionality, so if you are using proxy to connect to the internet you should configure the connection settings. Both this settings are available from the **Connection Settings...** command of the **Live Update** application menu. When you choose this command the settings dialog appears on the screen. Pic 2
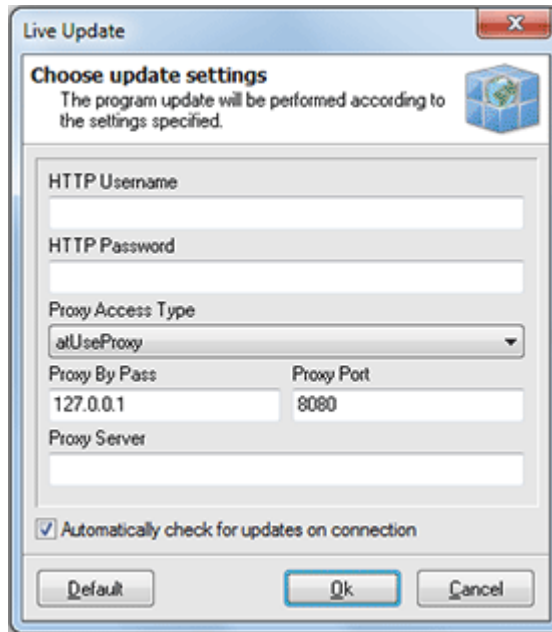
Pic 2. Configuring Live Update settings

In the configuration dialog you can specify if the automatic updates check should proceed and provide the proxy settings to be used to connect to the Internet.

Chapter 12: Requirements

Please carefully read and follow all requirements, listed here, or you may not be able to successfully use the product. You can contact our support if you experience a problem during the product use.

System Requirements

Computer running Network Inventory must meet the following requirements:

Minimum Hardware Requirements

- Intel Core 2 Duo Processor or equivalent

- 2 GB of RAM

- 250 MB of free disk space

Recommended Hardware Requirements

- 6th Gen Intel Core Processor or equivalent

- 4 GB of RAM

- 500 MB of free disk space

Supported Platforms

Windows XP (with SP3 or later), Windows XP x64 (with SP2 or later), Windows 2003 (with SP2 or later), Windows 2003 x64 (with SP2 or later), Windows 2003 R2, Windows 2003 R2 x64, Windows Vista, Windows Vista x64, Windows 2008, Windows 2008 x64, Windows 2008 R2, Windows 7, Windows 7 x64, Windows 8, Windows 8 x64, Windows 2012, Windows 8.1, Windows 8.1 x64, Windows 2012 R2, Windows 10, Windows 10 x64, Windows 2016

Requirements

- Administrative rights on the local computer

- Ability to access ADMIN$ share on remote computers

Chapter 13: About EMCO Software

EMCO Software is a leading innovator on the remote administration and management solutions market. Headquartered in Reykjavik, Iceland, we are an international company with offices and operations around the globe. Since the company's founding in 2001, we have been dedicated to providing network administrators with feature-rich, easy-to-use and affordable software and improving productivity of IT departments. Focused on the real-world needs of network professionals, our products are simple to try, simple to use, and simple to maintain while providing the power, scalability and flexibility needed by companies and organizations of all sizes.

Our solutions portfolio includes award-winning products targeted at remote network inventory, remote software deployment, remote desktop access and administration, network protection from viruses and malware, network security and health analyzing, remote power management, and remote automation.

Our Innovations

For a long time, products for remote desktops management, administration and inventorying were positioned on the market as enterprise-level solutions with a prohibitive total cost of ownership. A high price and a significant complexity kept many companies and organizations away from those solutions despite their high demand for tools that can improve productivity of their IT departments. We came onto the market looking to change this situation focusing on real-world needs of network professionals by providing simple but effective products and making them affordable for companies and organizations of all sizes.

Our first releases in 2001 proved that our products - which can be up and running within minutes, with no learning and complex configuration required, to immediately provide remote desktop control over the network - were exactly the solution that network engineers need most. An intuitive interface, valuable highly demanded features and an affordable price were the key factors to our quick market acquiring. After the first big success, our solutions portfolio quickly grew to 35 products that cover various fields of network administration and help automate hundreds of administration tasks. Along with this, there is still a lot of space for improvement, and we plan to further extend our product range to provide best-of-breed solutions.

EMCO Worldwide

More than 20,000 customers in 85 countries around the world rely on our products every day to take the complex routine out of their network management tasks. Our solutions help them to remotely manage as many as 2,3 million desktops and 103,000 servers and save millions of hours of work and multi-million dollar costs in total every year. Our worldwide customer base includes dozens of Fortune 100 and hundreds of Fortune 500 companies, as well as numerous large and small businesses representing all industries, educational and healthcare organizations, charity and non-profit organizations, and government institutions.

As a global company, we have partners all around the world who contribute to our products development, international sales and technical support. We are proud to cooperate with leading distributors and more than 50 resellers from 20 countries who represent our products on local markets.

Company Facts

- Year founded: 2001

- Headquarters: Reykjavik, Iceland

- Status: International corporation

- Expertise: Software network solutions

- Number of products: 35+

- Technology awards: 100+

- Number of customers: 20,000+

- Customers in: 85 countries worldwide

- Fortune 100 customers: 37%

- Fortune 500 customers: 49%

- Operations in: 20 countries worldwide

- Number of sales partners: 50+

Chapter 14: Contact Information

We would be glad to help you with any questions and problems you might have. Here you can find all the information you will need to contact us. To get quick answers regarding support issues or any other services, use corresponding contact information.

Company Requisites

- Name: EMCO ehf.

- Address: 12, Bildshofda St.

- City: Reykjavik

- Country: Iceland

- Postal code: 110

- E-mail: emco@emcosoftware.com

- Site: emcosoftware.com

Sales Questions

For any pre-sales or sales questions, contact us at sales@emcosoftware.com or call us:

🇺🇸 +1 646 233-1163	Business days 9.00-18.00 GMT (8.00-13.00 EST; 8.00-12.00 CST; 8.00-10.00 PDT).	
🇬🇧 +44 20 3287-7651	Business days 9.00-18.00 GMT.	
	Other hours: please leave your phone number and message - we will recall you within one business day.	

Technical Support

In case of any problems with our products or any technical question related to our products, please visit our Support area to receive FREE technical support.