YourSafetynet® pro+

by Media Security Networks

User Guide

EN - Revision 3.7   YourSafetynet pro+

CONTENTS

1 Introduction

Unlike most software products, YourSafetynet boasts a highly unique and simple user manual. YourSafetynet utilizes an integrated interactive 'support' in the software. This interactive support was mostly proactively contributed by many companies and schools during the development of YourSafetynet.

As a result installation takes just a few minutes. The information listed below is in actual fact all you need to know for successful installation and maintaining YourSafetynet user security.

2 Installation

YourSafetynet consists of three software components:

1. **The server software.**
   Responsible for distributing new or modified settings to clients and retrieving log records. Should be installed on a central server, but may also be installed on a workstation acting as a server. Clients will continue to function when the server is (temporarily) unavailable.
2. **The client software.**
   Responsible for the actual filtering. Installs itself as a local proxy on the client machine. Also suited for Terminal Servers. Please read the provided README for more detailed installation instructions.
3. **The server manager.**
   For managing the settings and viewing log records. May be installed on the server, but can also be installed on the workstation of the sysadmin or manager.

In the provided zip file you will find the needed installer files. You can always download the latest installer files from www.yoursafetynet.com/download.

Please bear the following prerequisites in mind before you start.

2.1 System requirements

The minimum system requirements for YourSafetynet are as follows:

- **Operating system:**
  - Windows XP® SP3 (only 32 bit)
  - Windows Vista® SP2
  - Windows 7®
  - Windows 8®
  - Windows Server 2003® SP2

  - Windows Server 2008® SP2
  - Windows Server 2008® R2
  - Windows Server 2012®
- **RAM:** 96 MB (minimum); 256 MB RAM (recommended)
- **Hard drive:** up to 500 MB available disk space may be required (depending on the Components already installed)
- **Processor**: 400 MHz Pentium processor or comparable (minimum); 1GHz Pentium processor or comparable (recommended)
- **DVD or CD-ROM drive:** only required for CD installation
- **Browser:** Microsoft® Internet Explorer 6 or higher, Firefox 1.6 or higher, Opera 6 or higher. Or a comparable web browser.
- **Internet connection**: DSL, ADSL, ISDN, modem, cable modem, LAN (or any internet/IP connection)
- **Monitor**: 800 x 600, 256 colors (minimum); 1024 x 768 with High colors, 32 bits (recommended)

2.2 Software requirements

YourSafetynet uses the Microsoft® .NET Framework® 3.5 SP1.

The Microsoft .NET Framework can be automatically installed during the installation of the Server and Server Manager if needed.

To reduce the client installer package's file size, the .NET Framework is not included in that installer package. You can download the .NET installer from www.yoursafetynet.com/getdotnet (will redirect to the Microsoft download pages).

NOTES:

- Newer Windows versions already include the Microsoft .NET 3.5 SP1 as part of the system. Installation of the framework is not needed on these systems:
  - Windows Vista SP2
  - Windows 7
  - Windows Server 2008 SP2
  - Windows Server 2008 R2
- Take special care with Windows 8 and Server 2012: You have to enable the .NET 3.5.1 feature in Windows before installing the client software.

2.3 Network requirements

YourSafetynet communicates between the client and server software within the local network at port 35350. The machine which has YourSafetynet Server installed on it must be available at this port.

YourSafetynet software also communicate with the Media Security Networks servers for license and update checks. If these checks keep failing for a longer period of time, the software may stop functioning.

2.3.1 Firewall settings

Please see below for an overview of potential firewall settings:

YourSafetynetServer.exe

→	ACCEPT/IN	TCP	PORT 35350	LAN	*YSN Client connections*
→	OUT	TCP	PORT 443	INTERNET	*https://*.yoursafetynet.com*

YourSafetynetCore.exe (Client)

→	OUT	TCP	PORT 35350	LAN	*YSN Server connection*
→	OUT	TCP	PORT 443	INTERNET	*https://*.yoursafetynet.com*

YourSafetynetServerManager.exe

→	OUT	TCP	PORT 35350	LAN	*YSN Server connection*

2.3.2 Proxy settings

The YourSafetynet client software installs itself as a local proxy on the client machine. This will overwrite any other (previously set) proxy settings.

If the use of a proxy is mandatory within your organization, please make sure you have this proxy also set as a forward proxy in YourSafetynet. This can be done in the Server Manager under *Filters* → *Network*.

When a forward proxy is set, the client software will forward incoming requests to this proxy. If proxy authentication is required, the client will forward this transparently from the user’s web browser to the set forward proxy.

Clients and Server software will also use this set proxy in their connection with the Media Security Networks servers for license/update checks (over HTTPS). If proxy authentication is required, please make sure you set special credentials for YourSafetynet to use in connections for these system requests (license/update checks).

3 YourSafetynet Server Manager

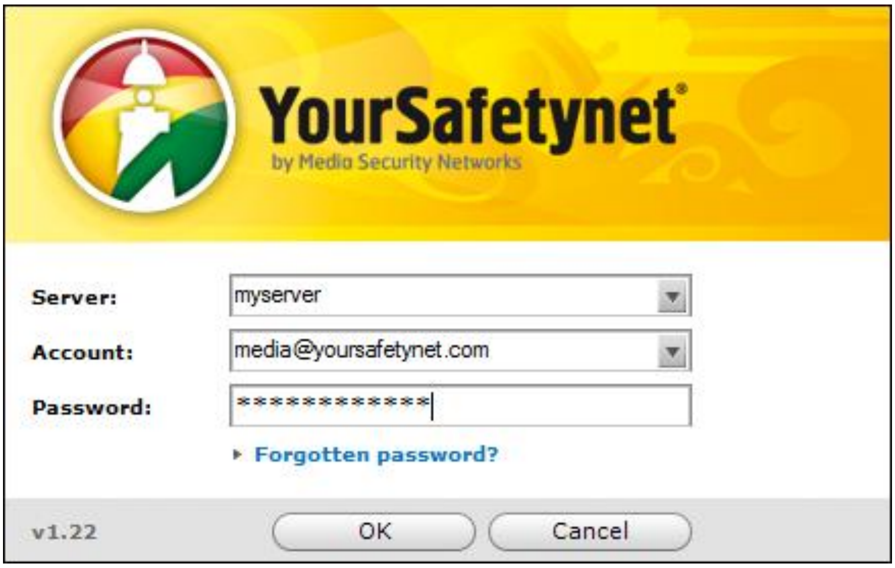
3.1 Settings

Having installed the YourSafetynet Server Manager, a shortcut is placed on the desktop (Figure 1). Click this to log in to the YourSafetynet server and to make your settings for the YourSafetynet client(s).

Figure 1: YourSafetynet Server Manager shortcut

3.2 Management

Only a manager who is acquainted with the YourSafetynet account and password may change the existing settings. Fill in the server name of the YourSafetynet Server and your account details in the login screen (Figure 2) that pops up when using the YourSafetynet Server Manager. Your account details are the same as those used during the installation and activation of YourSafetynet.



Server: myserver

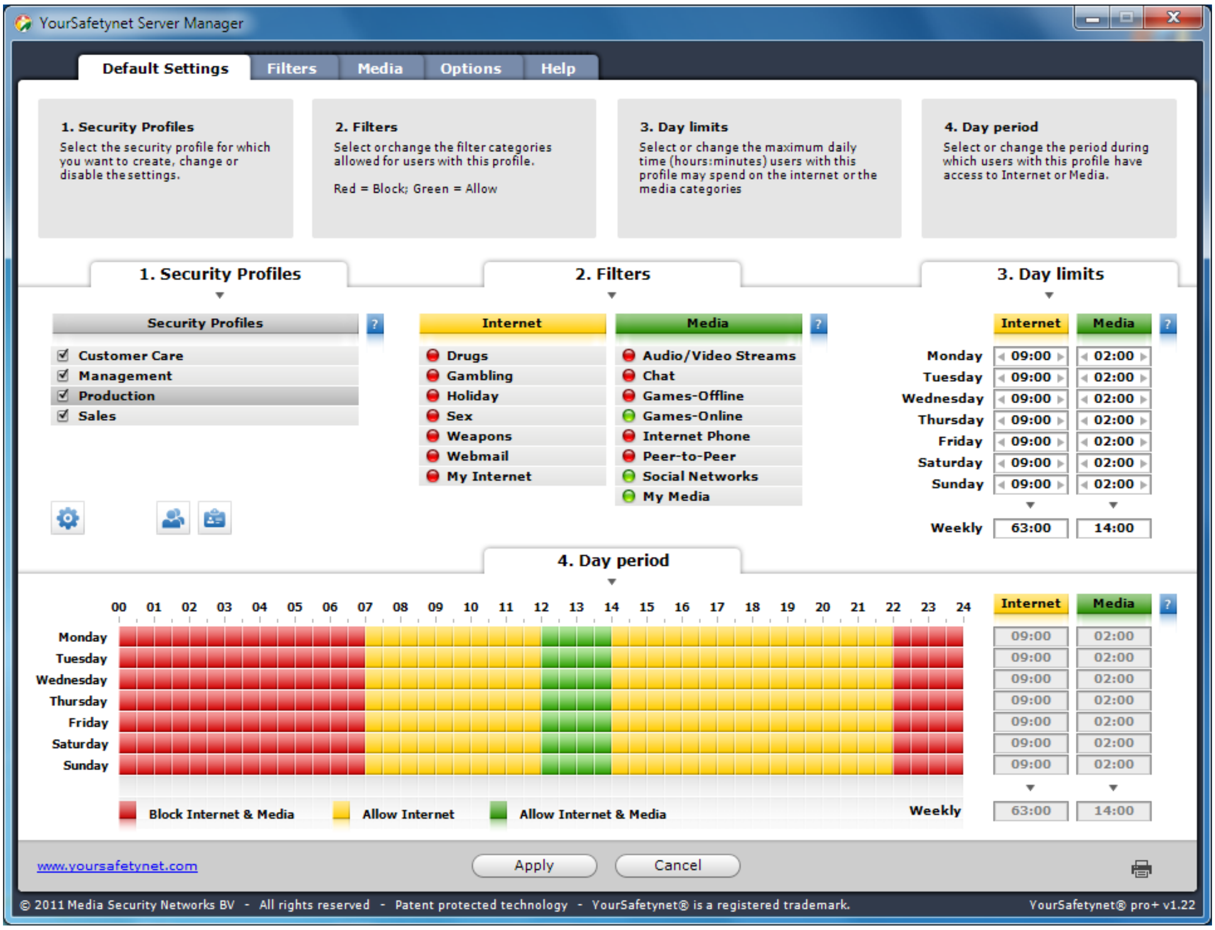
Account: media@yoursafetynet.com

Password: ************

Figure 2: Login screen

3.3 Settings

The interactive help function is under each tab of the settings screen (Figure 3), which explains all settings and functions step by step.



YourSafetynet Server Manager

1. Security Profiles
Select the security profile for which you want to create, change or disable the settings.

2. Filters
Select or change the filter categories allowed for users with this profile.

Red = Block; Green = Allow

3. Day limits
Select or change the maximum daily time (hours:minutes) users with this profile may spend on the internet or the media categories

4. Day period
Select or change the period during which users with this profile have access to Internet or Media.

1. Security Profiles

Security Profiles
☑ Customer Care
☑ Management
☑ Production
☑ Sales

2. Filters

Internet	Media
🔴 Drugs	🔴 Audio/Video Streams
🔴 Gambling	🔴 Chat
🔴 Holiday	🔴 Games-Offline
🔴 Sex	🟢 Games-Online
🔴 Weapons	🔴 Internet Phone
🔴 Webmail	🔴 Peer-to-Peer
🔴 My Internet	🟢 Social Networks
	🟢 My Media

3. Day limits

	Internet	Media
Monday	09:00	02:00
Tuesday	09:00	02:00
Wednesday	09:00	02:00
Thursday	09:00	02:00
Friday	09:00	02:00
Saturday	09:00	02:00
Sunday	09:00	02:00
Weekly	63:00	14:00

4. Day period

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Internet	Media
Monday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Tuesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Wednesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Thursday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Friday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Saturday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Sunday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Weekly																									63:00	14:00

🟥 Block Internet & Media 🟨 Allow Internet 🟩 Allow Internet & Media

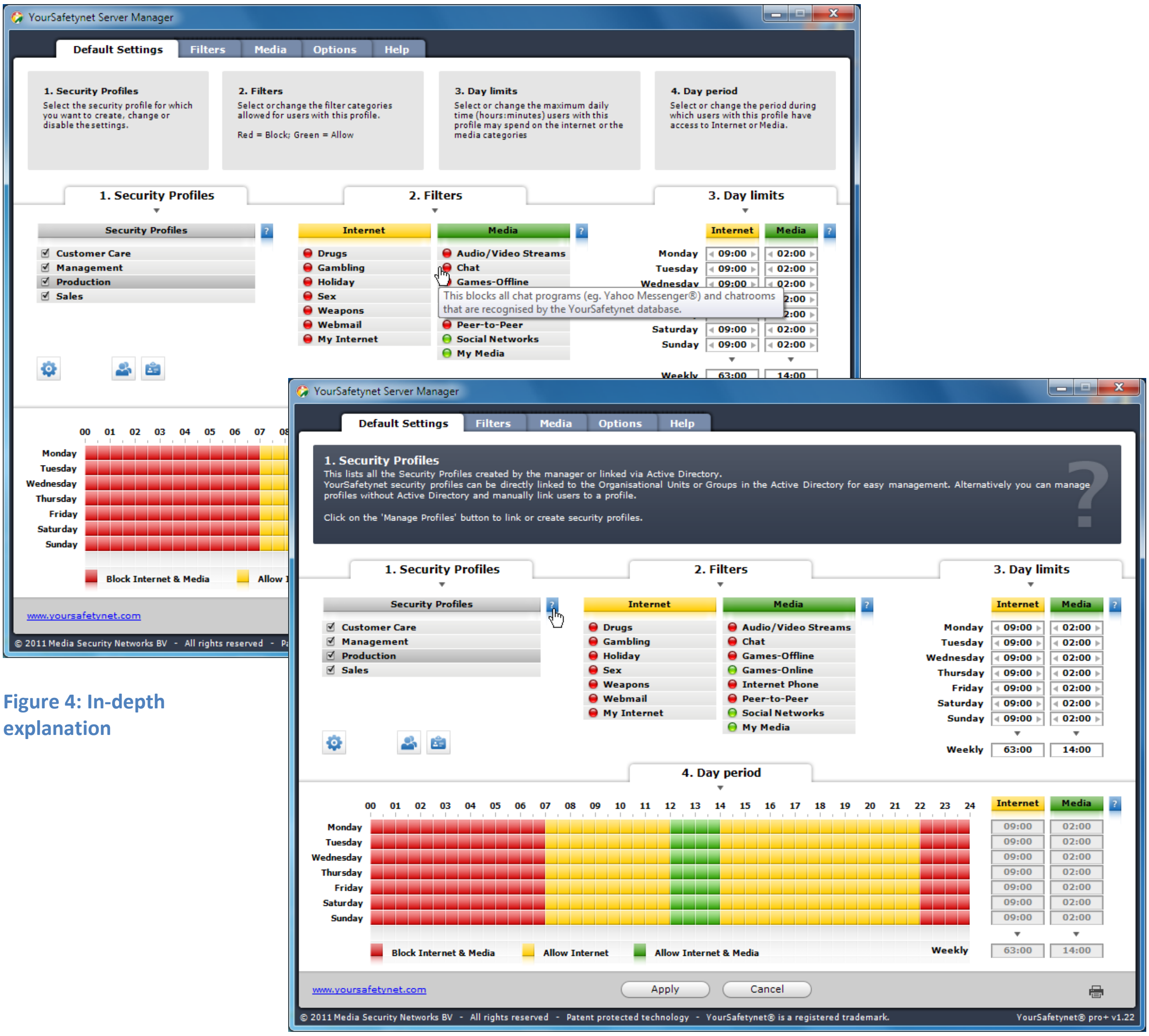
www.yoursafetynet.com

© 2011 Media Security Networks BV - All rights reserved - Patent protected technology - YourSafetynet® is a registered trademark. YourSafetynet® pro+ v1.22

Figure 3: Default Settings

3.4 In-depth Explanation

An in-depth explanation on the various settings and functions is listed under each tab (Figure 4). Place the cursor on the filter category or on a ?, where an explanation or extra background information will appear.



YourSafetynet Server Manager

Default Settings | Filters | Media | Options | Help

1. Security Profiles
Select the security profile for which you want to create, change or disable the settings.

2. Filters
Select or change the filter categories allowed for users with this profile.

Red = Block; Green = Allow

3. Day limits
Select or change the maximum daily time (hours:minutes) users with this profile may spend on the internet or the media categories

4. Day period
Select or change the period during which users with this profile have access to Internet or Media.

This blocks all chat programs (eg. Yahoo Messenger®) and chatrooms that are recognised by the YourSafetynet database.

YourSafetynet Server Manager

Default Settings | Filters | Media | Options | Help

1. Security Profiles
This lists all the Security Profiles created by the manager or linked via Active Directory.
YourSafetynet security profiles can be directly linked to the Organisational Units or Groups in the Active Directory for easy management. Alternatively you can manage profiles without Active Directory and manually link users to a profile.

Click on the 'Manage Profiles' button to link or create security profiles.

1. Security Profiles

Security Profiles
☑ Customer Care
☑ Management
☑ Production
☑ Sales

2. Filters

Internet	Media
🔴 Drugs	🔴 Audio/Video Streams
🔴 Gambling	🔴 Chat
🔴 Holiday	🔴 Games-Offline
🔴 Sex	🟢 Games-Online
🔴 Weapons	🔴 Internet Phone
🔴 Webmail	🔴 Peer-to-Peer
🔴 My Internet	🟢 Social Networks
	🟢 My Media

3. Day limits

	Internet	Media
Monday	09:00	02:00
Tuesday	09:00	02:00
Wednesday	09:00	02:00
Thursday	09:00	02:00
Friday	09:00	02:00
Saturday	09:00	02:00
Sunday	09:00	02:00
Weekly	63:00	14:00

4. Day period

	00–07	07–12	12–14	14–22	22–24	Internet	Media
Monday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Tuesday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Wednesday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Thursday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Friday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Saturday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Sunday	🟥	🟨	🟩	🟨	🟥	09:00	02:00
Weekly						63:00	14:00

🟥 Block Internet & Media 🟨 Allow Internet 🟩 Allow Internet & Media

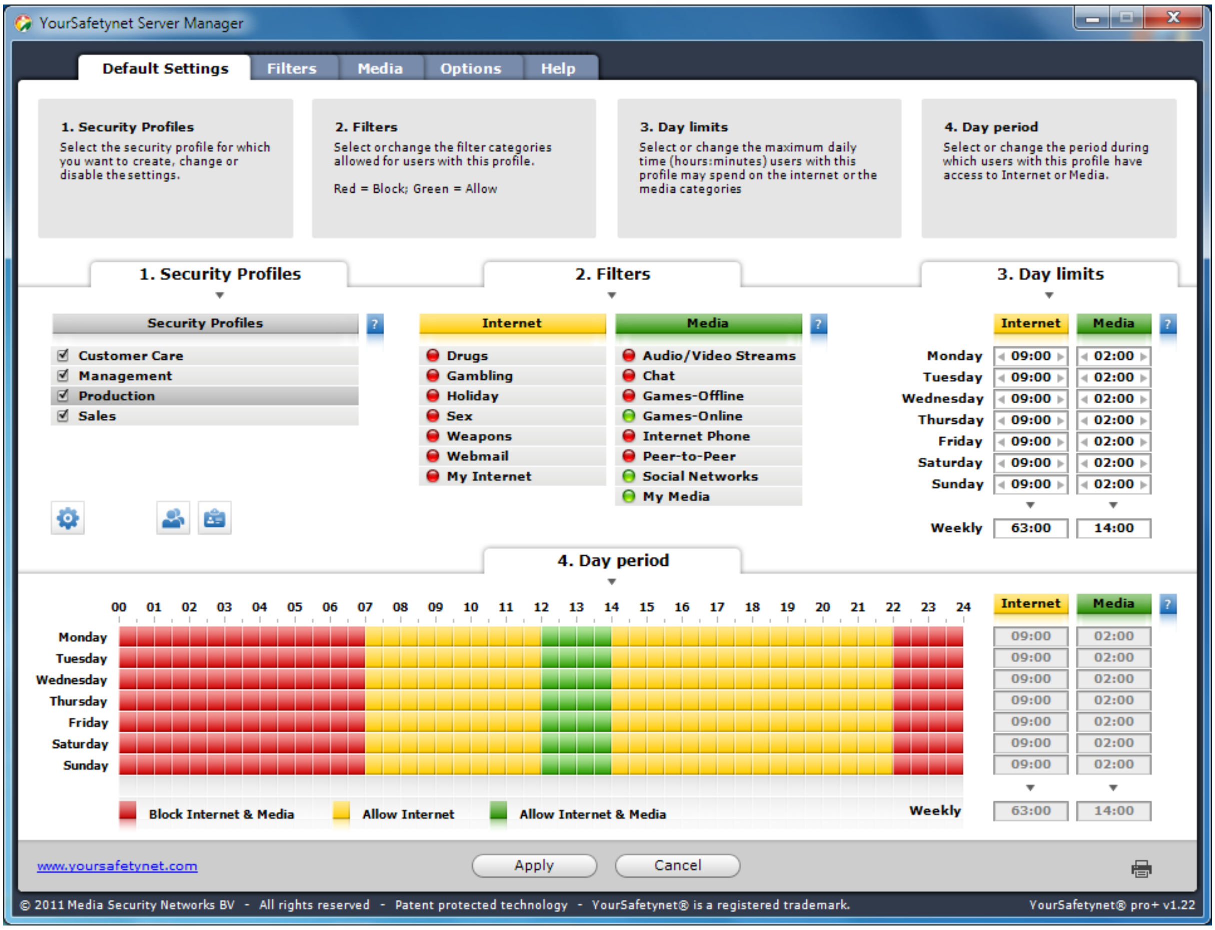
www.yoursafetynet.com Apply Cancel

© 2011 Media Security Networks BV - All rights reserved - Patent protected technology - YourSafetynet® is a registered trademark. YourSafetynet® pro+ v1.22

Figure 4: In-depth explanation

3.5 Overview of the User Interfaces

3.5.1 Default Settings



YourSafetynet Server Manager

1. Security Profiles
Select the security profile for which you want to create, change or disable the settings.

2. Filters
Select or change the filter categories allowed for users with this profile.

Red = Block; Green = Allow

3. Day limits
Select or change the maximum daily time (hours:minutes) users with this profile may spend on the internet or the media categories

4. Day period
Select or change the period during which users with this profile have access to Internet or Media.

1. Security Profiles

Security Profiles
☑ Customer Care
☑ Management
☑ Production
☑ Sales

2. Filters

Internet	Media
🟥 Drugs	🟥 Audio/Video Streams
🟥 Gambling	🟥 Chat
🟥 Holiday	🟥 Games-Offline
🟥 Sex	🟩 Games-Online
🟥 Weapons	🟥 Internet Phone
🟥 Webmail	🟥 Peer-to-Peer
🟥 My Internet	🟩 Social Networks
	🟩 My Media

3. Day limits

	Internet	Media
Monday	09:00	02:00
Tuesday	09:00	02:00
Wednesday	09:00	02:00
Thursday	09:00	02:00
Friday	09:00	02:00
Saturday	09:00	02:00
Sunday	09:00	02:00
Weekly	63:00	14:00

4. Day period

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Internet	Media
Monday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Tuesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Wednesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Thursday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Friday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Saturday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Sunday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟥	09:00	02:00
Weekly																									63:00	14:00

🟥 Block Internet & Media 🟨 Allow Internet 🟩 Allow Internet & Media

© 2011 Media Security Networks BV - All rights reserved - Patent protected technology - YourSafetynet® is a registered trademark. YourSafetynet® pro+ v1.22

Figure 5: Default Settings

1. **Security Profiles**
   This lists all the Security Profiles created by the manager or linked via Active Directory. YourSafetynet security profiles can be directly linked to the Organizational Units or Groups in the Active Directory for easy management. Alternatively you can manage profiles without Active Directory and manually link users to a profile.

2. **Filters**
   The unique YourSafetynet filter provides in blocking or allowing specific categories, including websites, games and software. With this pre-selection it is very easy for the manager to set up a specific set of rules for each security profile. The filter categories are updated on a regular basis to ensure new websites are included automatically.

3. **Day limit**
   With this setting, you can set the time that each user with this profile may spend each day on the Internet or Media. This prevents unlimited user access to the Internet or media activities.

4. **Day period**
   In the day period matrix you can control when users with this profile are allowed access to the Internet or media categories. A yellow field allows access to the Internet, but no access to the media categories. A green field allows access to the Internet and permitted media categories.

3.5.2 User management

Access the 'User management' screen (Figure 7) by clicking the button under the list of security profiles (Figure 6). This screen provides an overview of all YourSafetynet users. Here the manager can manually link users to a security profile, delete users, view and change acceptance of the user agreement. In addition, individual user activity can be seen. Exporting the list of users into a csv file is also supported.

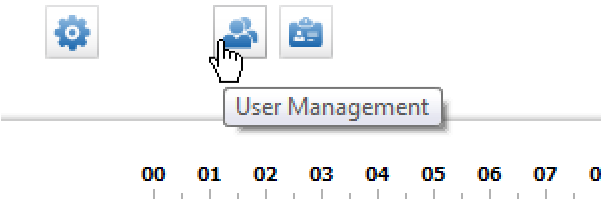
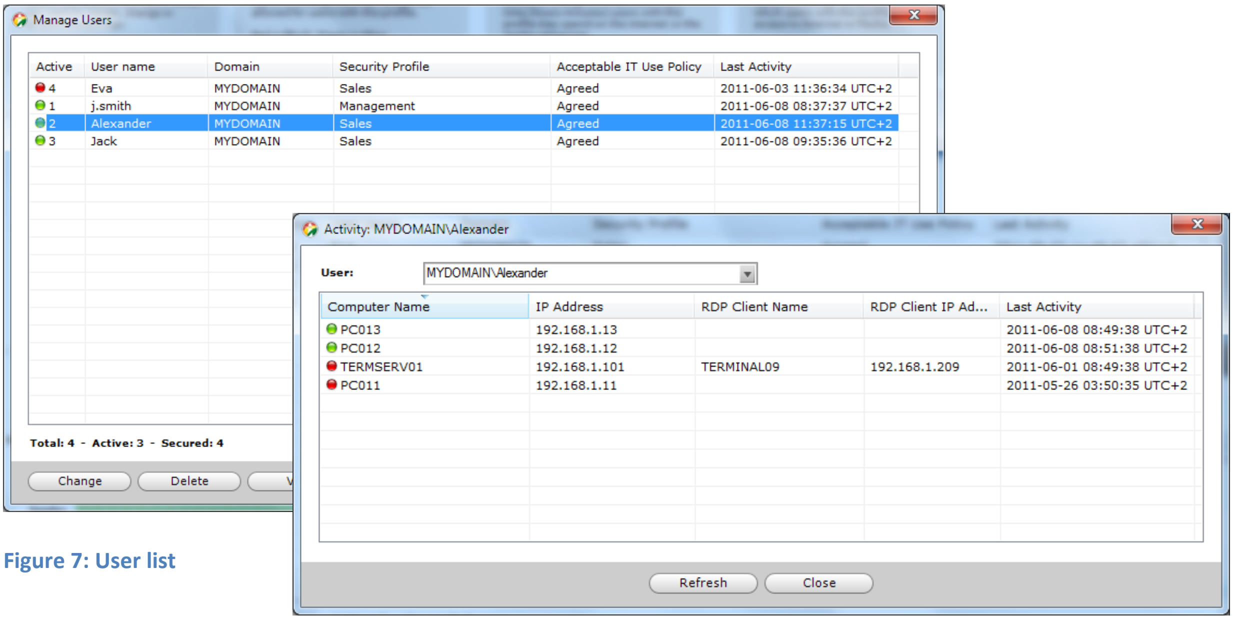


Figure 6: Button user management



Active	User name	Domain	Security Profile	Acceptable IT Use Policy	Last Activity
● 4	Eva	MYDOMAIN	Sales	Agreed	2011-06-03 11:36:34 UTC+2
● 1	j.smith	MYDOMAIN	Management	Agreed	2011-06-08 08:37:37 UTC+2
● 2	Alexander	MYDOMAIN	Sales	Agreed	2011-06-08 11:37:15 UTC+2
● 3	Jack	MYDOMAIN	Sales	Agreed	2011-06-08 09:35:36 UTC+2

Total: 4 - Active: 3 - Secured: 4

User: MYDOMAIN\Alexander

Computer Name	IP Address	RDP Client Name	RDP Client IP Ad...	Last Activity
● PC013	192.168.1.13			2011-06-08 08:49:38 UTC+2
● PC012	192.168.1.12			2011-06-08 08:51:38 UTC+2
● TERMSERV01	192.168.1.101	TERMINAL09	192.168.1.209	2011-06-01 08:49:38 UTC+2
● PC011	192.168.1.11			2011-05-26 03:50:35 UTC+2

Figure 7: User list

3.5.3 Profile management

Access the ‘Profile Management’ (Figure 9) by clicking the button under the list of security profiles (Figure 8).

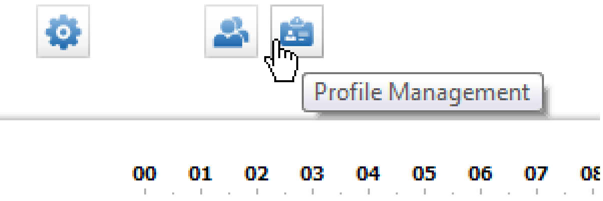
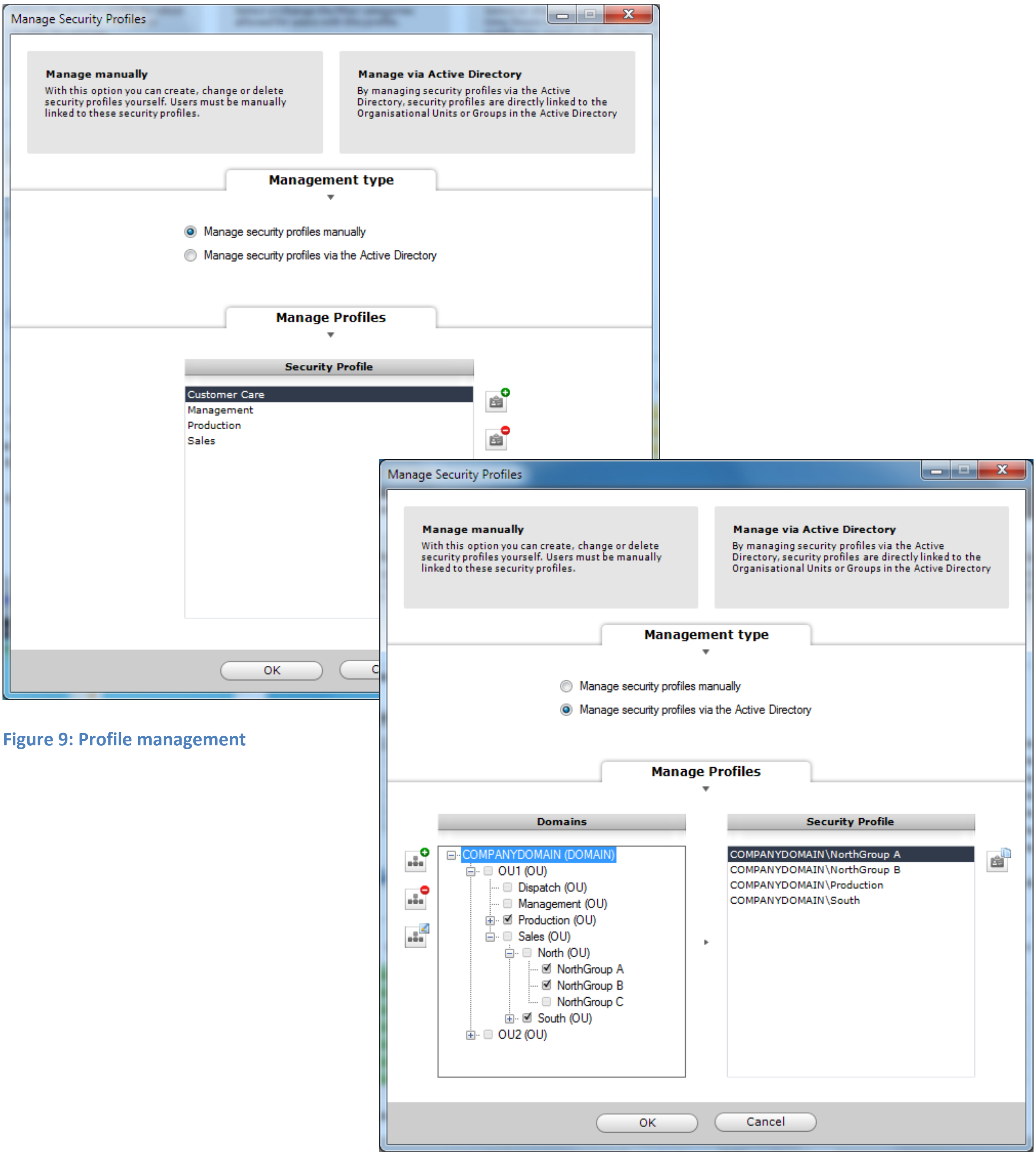


Figure 8: Button profile management



Manage manually
With this option you can create, change or delete security profiles yourself. Users must be manually linked to these security profiles.

Manage via Active Directory
By managing security profiles via the Active Directory, security profiles are directly linked to the Organisational Units or Groups in the Active Directory

Management type

● Manage security profiles manually
○ Manage security profiles via the Active Directory

Manage Profiles

Security Profile
Customer Care
Management
Production
Sales

Manage manually
With this option you can create, change or delete security profiles yourself. Users must be manually linked to these security profiles.

Manage via Active Directory
By managing security profiles via the Active Directory, security profiles are directly linked to the Organisational Units or Groups in the Active Directory

Management type

○ Manage security profiles manually
● Manage security profiles via the Active Directory

Manage Profiles

Domains

```
⊟ COMPANYDOMAIN (DOMAIN)
   ⊟ □ OU1 (OU)
        □ Dispatch (OU)
        □ Management (OU)
      ⊞ ☑ Production (OU)
      ⊟ □ Sales (OU)
         ⊟ □ North (OU)
              ☑ NorthGroup A
              ☑ NorthGroup B
              □ NorthGroup C
         ⊞ ☑ South (OU)
   ⊞ □ OU2 (OU)
```

Security Profile
COMPANYDOMAIN\NorthGroup A
COMPANYDOMAIN\NorthGroup B
COMPANYDOMAIN\Production
COMPANYDOMAIN\South

Figure 9: Profile management

- Manual management; with this option you can personally create, change or delete security profiles. Users must be manually linked to these profiles.

- Manage via Active Directory; by managing security profiles via Active Directory the security profiles are directly linked to the Organizational Units or Groups in the Active Directory.

3.5.4 Extra Manager Settings

Access the 'Extra Manager Settings' (Figure 11) via the button under the list of security profiles (Figure 10). Here you can:

- Set, activate or manage the Acceptable IT Use Policy (AUP) that applies to the organization.

- Set ICT contact information to give users the ability to contact the network administrator.

- Activate a Network Scan. With this tool the activity of YourSafetynet on all computers within the network can be detected. After the scan you can see on which computers the YourSafetynet client still needs to be installed.

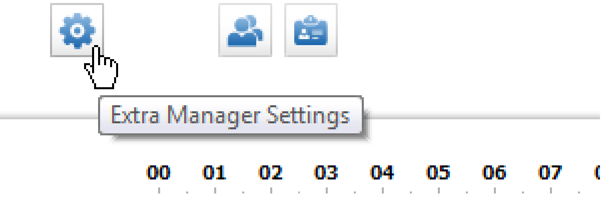
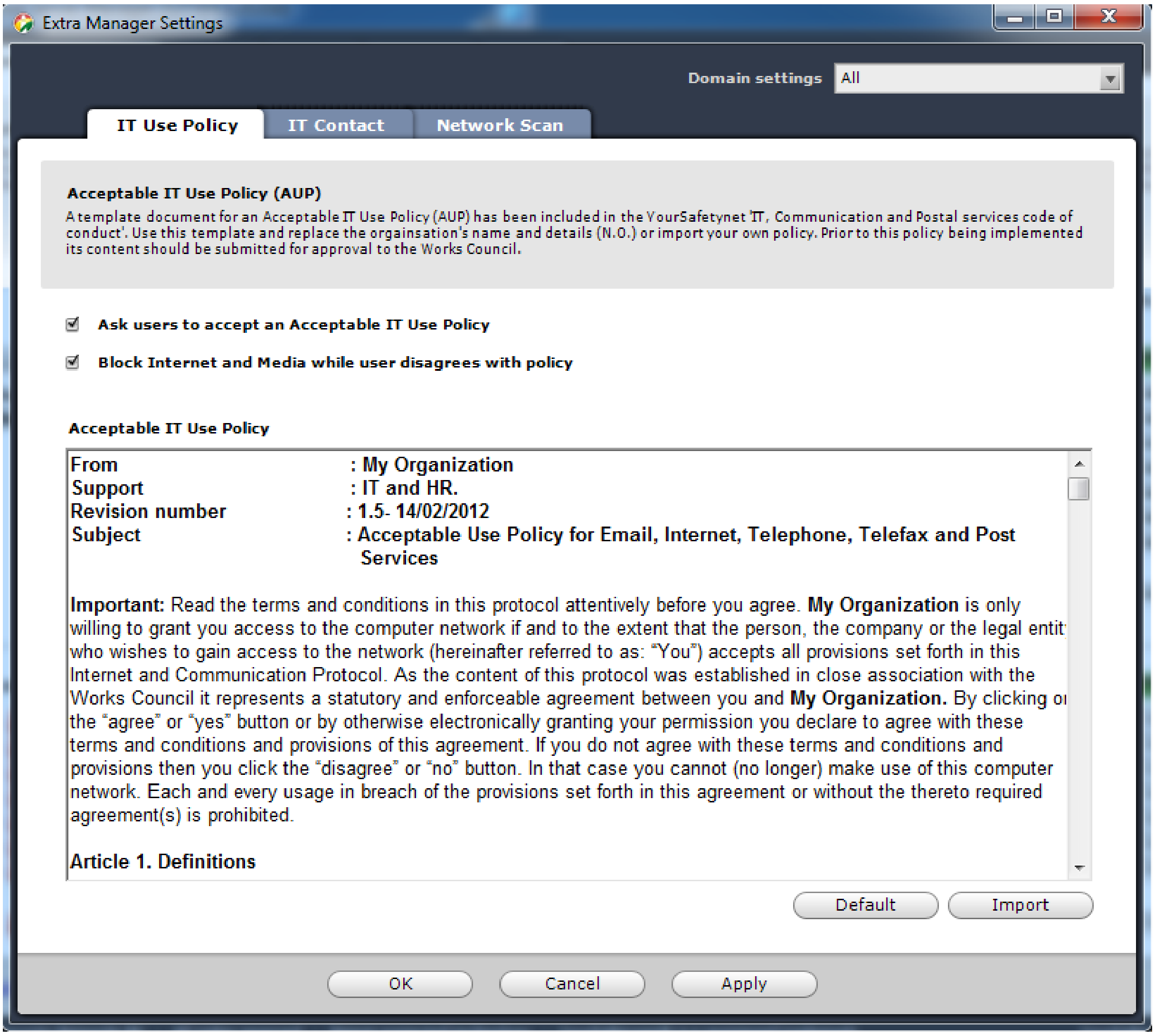


Figure 10: Button Extra Manager Settings



Acceptable IT Use Policy (AUP)

A template document for an Acceptable IT Use Policy (AUP) has been included in the YourSafetynet 'IT, Communication and Postal services code of conduct'. Use this template and replace the orgainsation's name and details (N.O.) or import your own policy. Prior to this policy being implemented its content should be submitted for approval to the Works Council.

☑ Ask users to accept an Acceptable IT Use Policy

☑ Block Internet and Media while user disagrees with policy

Acceptable IT Use Policy

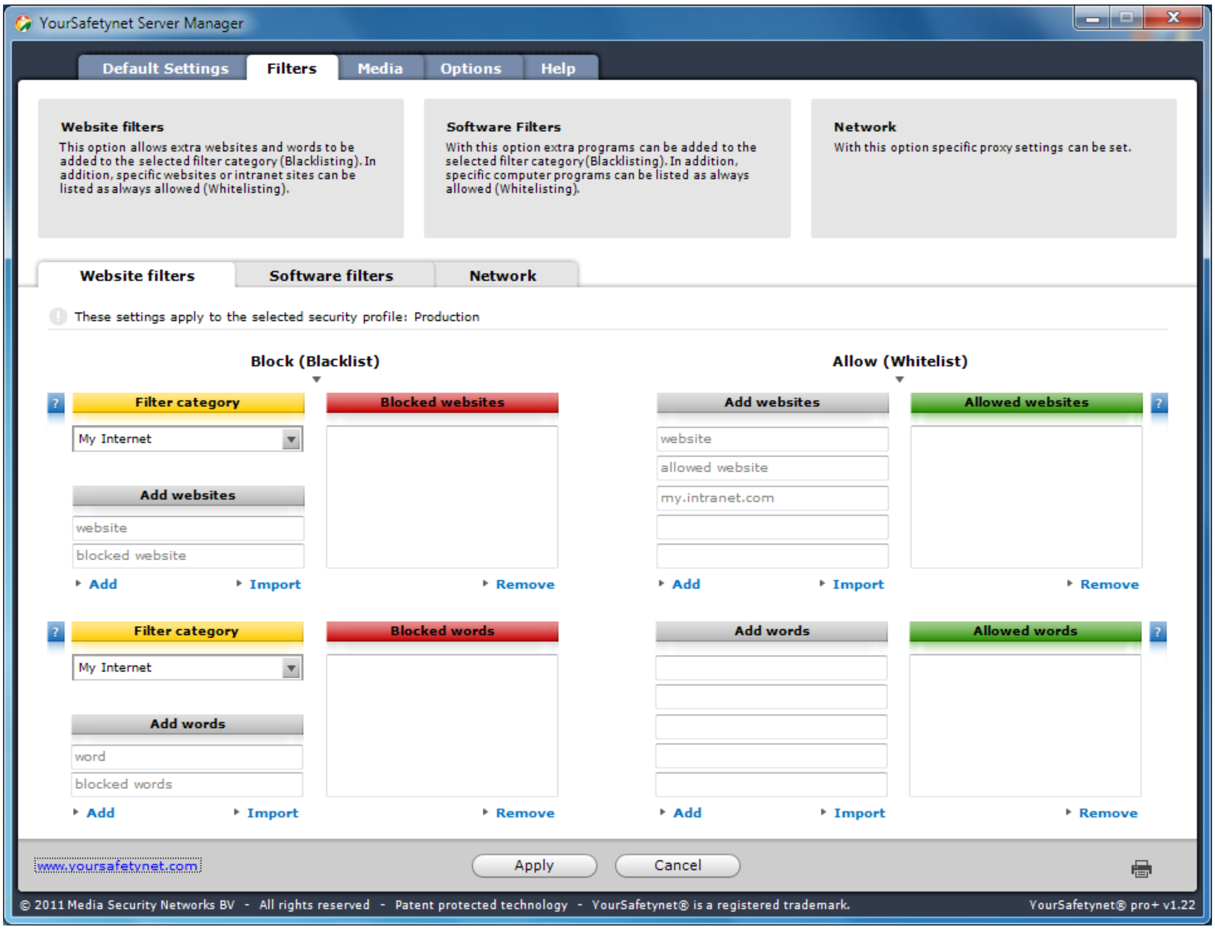
From	: My Organization
Support	: IT and HR.
Revision number	: 1.5- 14/02/2012
Subject	: Acceptable Use Policy for Email, Internet, Telephone, Telefax and Post Services

Important: Read the terms and conditions in this protocol attentively before you agree. **My Organization** is only willing to grant you access to the computer network if and to the extent that the person, the company or the legal entit who wishes to gain access to the network (hereinafter referred to as: "You") accepts all provisions set forth in this Internet and Communication Protocol. As the content of this protocol was established in close association with the Works Council it represents a statutory and enforceable agreement between you and **My Organization.** By clicking o the "agree" or "yes" button or by otherwise electronically granting your permission you declare to agree with these terms and conditions and provisions of this agreement. If you do not agree with these terms and conditions and provisions then you click the "disagree" or "no" button. In that case you cannot (no longer) make use of this computer network. Each and every usage in breach of the provisions set forth in this agreement or without the thereto required agreement(s) is prohibited.

Article 1. Definitions

Figure 11: Extra Manager Settings

3.5.5 Filters



Website filters
This option allows extra websites and words to be added to the selected filter category (Blacklisting). In addition, specific websites or intranet sites can be listed as always allowed (Whitelisting).

Software Filters
With this option extra programs can be added to the selected filter category (Blacklisting). In addition, specific computer programs can be listed as always allowed (Whitelisting).

Network
With this option specific proxy settings can be set.

These settings apply to the selected security profile: Production

© 2011 Media Security Networks BV - All rights reserved - Patent protected technology - YourSafetynet® is a registered trademark. YourSafetynet® pro+ v1.22

Figure 12: Filters

Website and Word filters

- **Blocking websites (Blacklisting)**
  If you want to block specific websites yourself then add these to the 'blocked website' list. You can add a website to a specific filter category. As such always first select the right filter category before adding a website.
  Beware: YourSafetynet only blocks a website if the selected filter category is set to block (red) for this security profile in the 'Default Settings' tab.

- **Blocking words (Blacklisting)**
  YourSafetynet checks websites for word and language use. If you want to block websites that contain certain words, you can add these words to your 'blocked words' list. If a website contains one or more words from this list then YourSafetynet will block access to this website. You can add a 'prohibited word' to a specific filter category. As such always first select the right filter category before adding a word.
  Beware: YourSafetynet only blocks a website if the selected filter category is set to block

(red) for this security profile in the 'Default Settings' tab.

- **Allowing websites (Whitelisting)**
  If you want to always permit specific websites yourself (for example a company or organization's intranet site) then add these to the list of 'allowed websites'. Websites on this list are always permitted by YourSafetynet. Under no circumstances are they prohibited, not even if the user time has expired or if the user time falls outside of the set day period. The setting applies to all users with this security profile.

- **Allowing words (Whitelisting)**
  YourSafetynet checks websites for word and language use. If you want to always permit websites that contain certain words, then add these words to the 'allowed words' list. If a website contains one or more words from this list then this website is always permitted by YourSafetynet. Even if the user time has expired or if the time falls outside of the set day period. The setting applies to all users with this security profile.

Software filters

- **Blocking software (Blacklisting)**
  YourSafetynet can also prohibit or regulate the use of specific programs. This can be done by adding a program to a filter category. As such you can even block software for this security profile that isn't covered by the standard filters. First select the right filter category before adding a program to the list!
  Beware: YourSafetynet only blocks a program if the selected filter category is set to block (red) for this security profile in the 'Default Settings' tab.

- **Allowing software (Whitelisting)**
  If you want to always permit specific programs yourself (for example internal chat software) then add these to the list of 'allowed software'. Programs on this list are always permitted by YourSafetynet. Under no circumstances are they prohibited, not even if the user time has expired or if the user time falls outside of the set day period. The setting applies to all users with this security profile.

Network

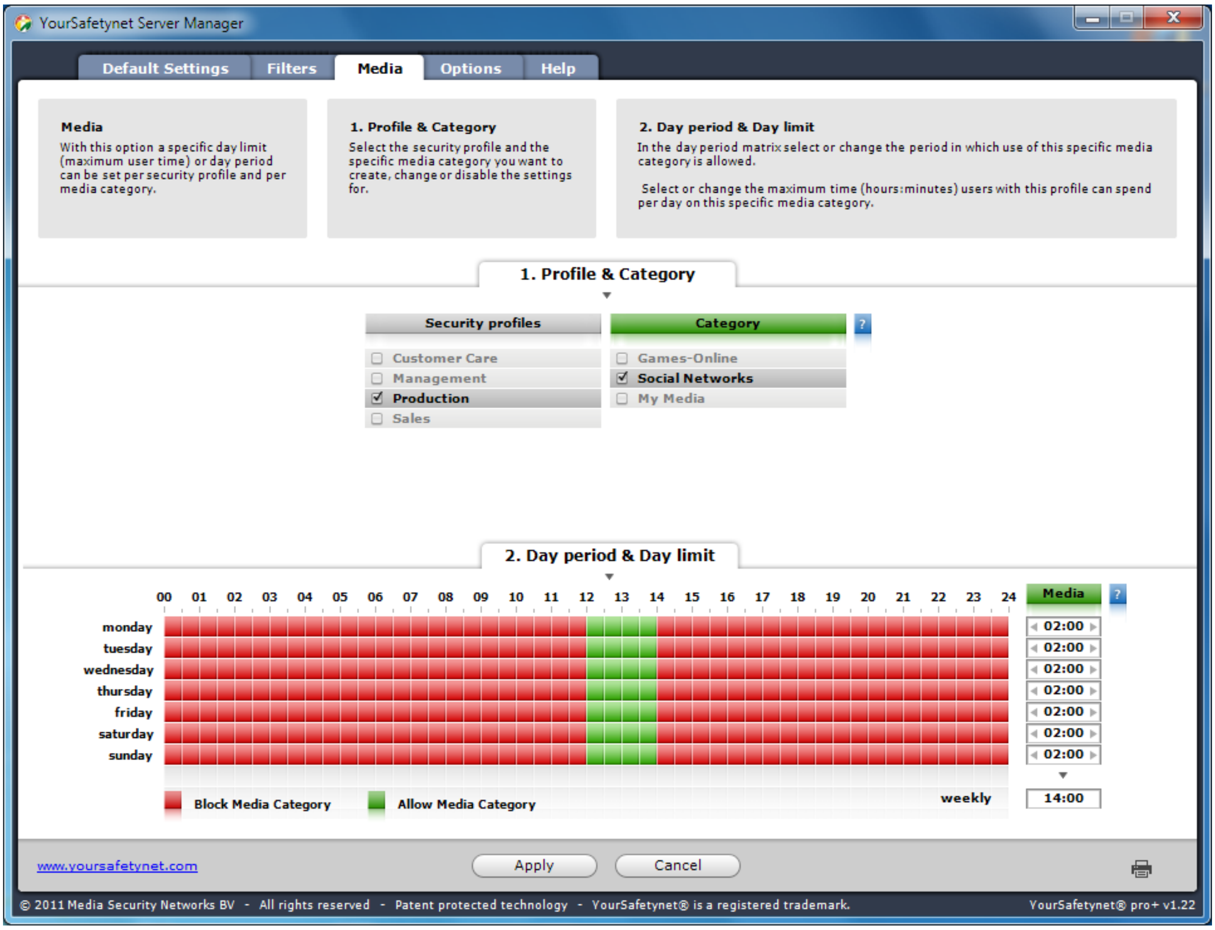
- **YourSafetynet Proxy**
  For the internet filter YourSafetynet uses a local proxy. If you want to exclude certain websites from being filtered (for example an intranet website), you can set it here. All requests for websites set here will completely bypass the YourSafetynet proxy and will not

be filtered.

- **Forward Proxy**
  For the internet filter YourSafetynet uses a local proxy. If a proxy is also required within your organization, it can be set with this option. Beware! Check the settings properly. Incorrect settings will prevent YourSafetynet connecting with the internet.

3.5.6 Media

With this option a specific day limit (maximum user time) and day period can be set up per security profile and per media category.



Media
With this option a specific day limit (maximum user time) or day period can be set up per security profile and per media category.

1. Profile & Category
Select the security profile and the specific media category you want to create, change or disable the settings for.

2. Day period & Day limit
In the day period matrix select or change the period in which use of this specific media category is allowed.

Select or change the maximum time (hours:minutes) users with this profile can spend per day on this specific media category.

1. Profile & Category

Security profiles	Category
□ Customer Care	□ Games-Online
□ Management	☑ Social Networks
☑ Production	□ My Media
□ Sales	

2. Day period & Day limit

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Media
monday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
tuesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
wednesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
thursday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
friday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
saturday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
sunday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	02:00
weekly																									14:00

🟥 Block Media Category 🟩 Allow Media Category

© 2011 Media Security Networks BV - All rights reserved - Patent protected technology - YourSafetynet® is a registered trademark. YourSafetynet® pro+ v1.22

Figure 13: Media

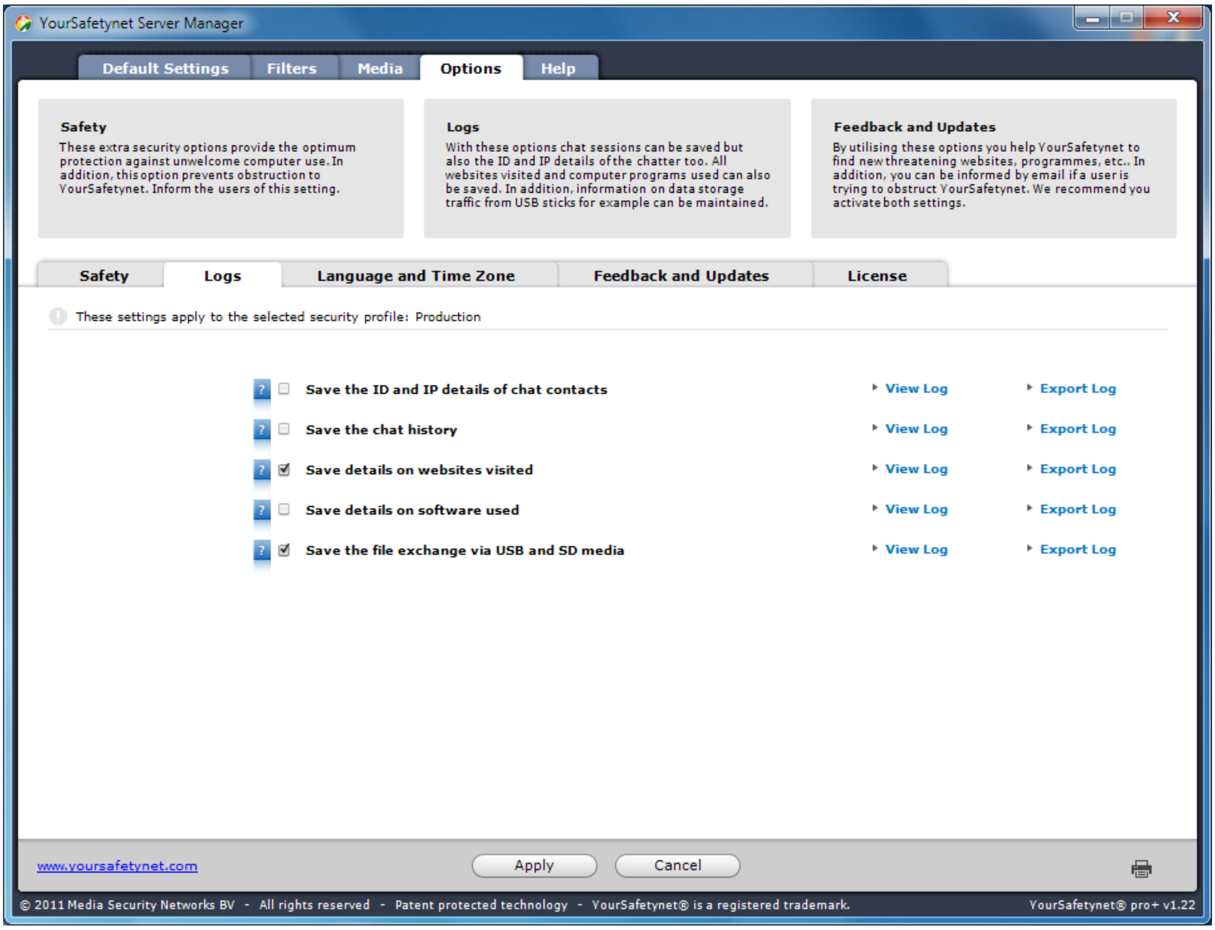
1. **Profile & Category**
   The maximum user times (day limit) and the period in which media categories are permitted (day period) are all set up the same way under the 'Default Settings' tab. It may be that you want the day limit & day period to be different for a specific category. For this, a specific day limit and day period can be set up per security profile for each category.

2. **Day period & Day limit**
   With this option a different day limit (user time) or day period (start time and period) can be set during which time the users with this security profile have access to the specific media category.

The color selected within the day period matrix determines the access status. A green field gives users with this Security Profile access to the specifically selected media category.

3.5.7 Options

In this screen extra options can be managed such as specific safety or logging options.



Safety
These extra security options provide the optimum protection against unwelcome computer use. In addition, this option prevents obstruction to YourSafetynet. Inform the users of this setting.

Logs
With these options chat sessions can be saved but also the ID and IP details of the chatter too. All websites visited and computer programs used can also be saved. In addition, information on data storage traffic from USB sticks for example can be maintained.

Feedback and Updates
By utilising these options you help YourSafetynet to find new threatening websites, programmes, etc.. In addition, you can be informed by email if a user is trying to obstruct YourSafetynet. We recommend you activate both settings.

These settings apply to the selected security profile: Production

- □ Save the ID and IP details of chat contacts — View Log — Export Log
- □ Save the chat history — View Log — Export Log
- ☑ Save details on websites visited — View Log — Export Log
- □ Save details on software used — View Log — Export Log
- ☑ Save the file exchange via USB and SD media — View Log — Export Log

© 2011 Media Security Networks BV - All rights reserved - Patent protected technology - YourSafetynet® is a registered trademark. YourSafetynet® pro+ v1.22

Figure 14: Options

Safety

- **Send a security warning to chat contacts**
  As soon as a conversation starts, a security message will be sent to the recipient:
  “This user is YourSafetynet protected; your account information and IP address may be stored for tracking purposes”.
  Dubious chatters will be scared off by this message and will usually end their chat session immediately. Supported chat software: Windows Live Messenger®, Yahoo Messenger®.

- **Block the webcam**
  By activating this option webcam use on this computer is fully blocked. Beware! Changes to these settings are only activated once the computer has been rebooted.

- **Block data transfers to USB and SD-card storage**
  With this option file exchange via USB sticks and SD-cards, MP3 players and cameras is blocked on the computer. Blocking USB and SD-card storage helps protect your organization against damage, loss or theft of confidential organizational data.

- **Block DVD burning via Windows®**
  This option blocks DVD burning on the computer. This function only applies to the enclosed Windows® burning program.

- **Shut down the computer immediately if YourSafetynet is obstructed**
  If a user successfully obstructs YourSafetynet, the computer will be immediately switched off without warning via the Windows® shutdown procedure.

- **Disable YourSafetynet if the computer is outside the network**
  With this option YourSafetynet is automatically switched off if the computer is no longer within the organization’s network range (for example at home).

Logs

- **Save ID and IP details of chat contacts**
  By activating this option, all ID and IP details of chat contacts are saved in a log file. This relates to all contacts for whom an ID and IP address could be retrieved. Supported chat software: Windows Live Messenger®, Yahoo Messenger®.

- **Save message history of chat software**
  By activating this option, the chat message history is saved in a log file. Supported chat software: Windows Live Messenger®, Yahoo Messenger®.

- **Save details on websites visited**
  By activating this option, information about websites visited is saved in a log file.

- **Save details on software used**
  By activating this option, information about software used is saved in a log file.

- **Save details on file transfers to USB and SD-card storage**
  The history of all outgoing USB and SD-card storage traffic is saved in this log file.

Language and Time zone

- **Language**
  Use this option to select the language you wish to use for YourSafetynet. This setting applies to all users.

- **Time zone**
  YourSafetynet synchronizes its internal clock automatically with an online time server. To attain the right conversion to the current local time it is important that the time zone is correctly set up. The internal YourSafetynet clock adjusts automatically to summer and winter time.

Feedback en Updates

- **Help improve YourSafetynet by sharing anonymous data**
  Enable this option to share anonymous data on internet use and potential threats with YourSafetynet. YourSafetynet only uses this information to track new defective websites and software.

- **Inform me when a user attempts to obstruct YourSafetynet**
  Enable this option to get notified about potential obstructions. Our servers will detect when a user is obstructing YourSafetynet. The server will generate an email message which reports this obstruction. This message will be sent to the email address of the YourSafetynet account.

- **YourSafetynet updates**
  We work continuously on improving YourSafetynet. Therefore we release updates on a regular basis. These updates may be technical or may extend the filter databases (content update). We recommend you enable this option to have YourSafetynet search daily for new updates and install them.

4 YourSafetynet Agent (Client)

Once YourSafetynet client has been installed a number of services and an Agent application are put into place. The YourSafetynet Agent is started for every logged in user and is visible in the system tray (bottom right – Figure 16). Click the YourSafetynet icon to see the menu.

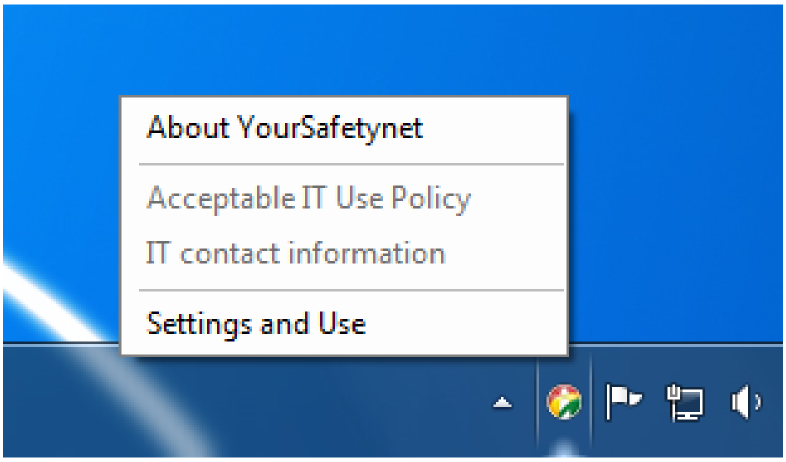
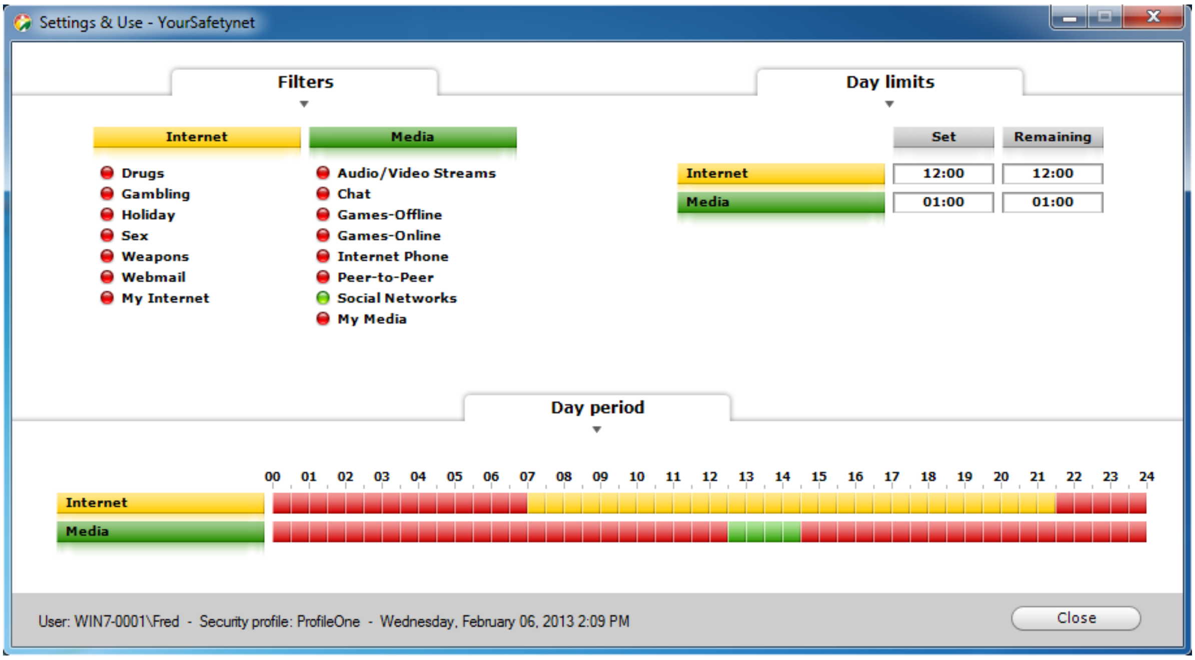


Figure 15: YourSafetynet Agent

4.1 Settings and Use

During computer use, the user can see information on settings and use history. The user can access this information by clicking the YourSafetynet icon in system tray (bottom right) and selecting ‘Settings and Use’.



Settings & Use - YourSafetynet

Filters

Internet	Media
🔴 Drugs	🔴 Audio/Video Streams
🔴 Gambling	🔴 Chat
🔴 Holiday	🔴 Games-Offline
🔴 Sex	🔴 Games-Online
🔴 Weapons	🔴 Internet Phone
🔴 Webmail	🔴 Peer-to-Peer
🔴 My Internet	🟢 Social Networks
	🔴 My Media

Day limits

	Set	Remaining
Internet	12:00	12:00
Media	01:00	01:00

Day period

User: WIN7-0001\Fred - Security profile: ProfileOne - Wednesday, February 06, 2013 2:09 PM

Close

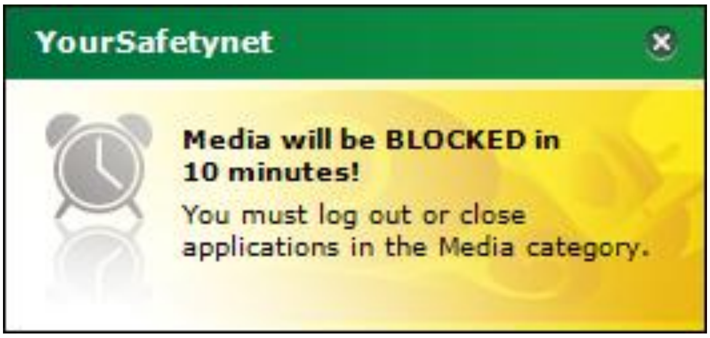
Figure 16: Settings and Use

On this screen the user sees the following information:

- Overview of set times
- Overview of remaining times
- List of blocked periods
- List of permitted periods

4.2 End of Periods of Use

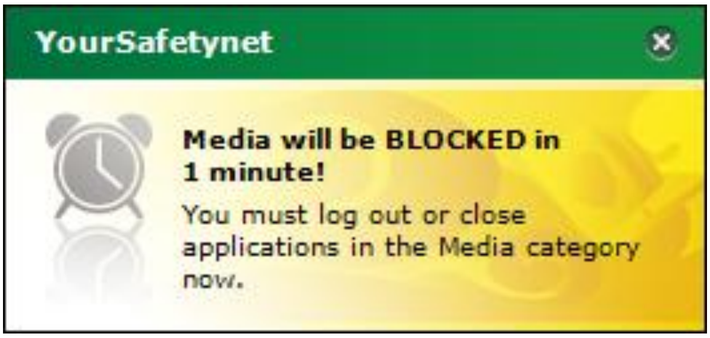
Approximately 10 minutes before the end of the permitted user time the user receives a pop-up notification. This pop-up also states which application type this notification applies to. In the example this is a media application.



Media will be BLOCKED in 10 minutes!
You must log out or close applications in the Media category.

Figure 17: 10 minutes notification

Approximately 1 minute before the end of the permitted time the user sees a final pop-up, in which they are advised to close down applications immediately.



Media will be BLOCKED in 1 minute!
You must log out or close applications in the Media category now.

Figure 18: 1 minute notification

5 Contact

For further information please visit:

www.yoursafetynet.com/pro

Or enquire at your local **YourSafetynet pro+** dealer.