iBoss Enterprise

Web Filter
and Enterprise Reporter

User Manual

Phantom™ Technologies
www.iBossWebFilters.com

Note: Please refer to the User Manual online for the latest updates at www.ibosswebfilters.com.

Phantom Technologies Inc makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defects. Further, this company reserves the right to revise this publication and make changes from time to time in the contents hereof without obligation to notify any person of such revision of changes.

www.iBossWebFilters.com

Open Source Code

This product may include software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other open-source software licenses. Copies of the GPL and LGPL licenses are available upon request. You may also visit www.gnu.org to view more information regarding open-source licensing.

The GPL, LGPL and other open-source code used in Phantom Technologies Inc products are distributed without any warranty and are subject to the copyrights of their authors. Upon request, open-source software source code is available from Phantom Technologies Inc via electronic download or shipment on a physical storage medium at cost. For further details and information please visit www.iphantom.com/opensource.

Table of Contents

Table of Figures

1 iBoss Enterprise Web Filter

1.1 Overview

The iBoss Enterprise is a line of web filters for medium to large networks. Powerful patent-pending filtering technology puts you in control of Internet usage on your network. Flexible Internet controls allow you to easily restrict access to specific categories of Internet destinations and manage time spent using online programs (online chat and messenger programs, file sharing, gaming and more). It utilizes an industry first advanced real-time graphical user interface, robust Internet traffic controls, total network traffic analyzer, up to the second network activity feed MRTG, and a live real-time URL database feed ensuring the most accurate filtering possible.

1.2 Key Features

- **Comprehensive Web Filtering**
- **IM/Application Policies and Blocking**
- **Policy Scheduling**
- **Robust Reports**
- **Real-Time MRTG**
- **Remote Management**
- **Individual User Login with LDAP/Active Directory Integration**
- **Policies Users/Groups**
- **Real-Time URL Updates**
- **Simple & User-Friendly Interface**
- **Plug & Play with No Software to Install**
- **Compatible with any Operating System**

1.3 Manual Structure

This manual includes detailed information and instructions for installing and configuring the iBoss. The "**Getting Started**" section of this manual will guide you through the initial hardware installation and setup process. The "**Configuration**" section of the manual contains detailed instructions for configuring specific settings and customizing preferences.

Note: For quick installation instructions, you may also reference the iBoss Quick Installation Guide included with the product.

1.4 System Requirements

- Broadband (Cable, DSL, T1, FiOS, etc.) Internet service
- Network Adapter for each computer
- Existing Firewall and Switch
- Any Major Operating System running a TCP/IP network (i.e. Mac, Windows, Linux, etc.)
- Standard Web Browser
- Active iBoss Subscription

2 Specifications

2.1 iBoss Enterprise Model Specifications

The iBoss Enterprise has the following specifications:

Model	Recommended Concurrent Users	Identifiable Computers	Identifiable Users	Filtering Groups	Reports Database Size	Generated Reports	Report Schedules
1550	50-100	120	120	25	10 GB	50	5
1750	101-200	240	240	50	20 GB	75	10
2150	201-300	360	360	60	20 GB	75	10
2550	301-400	480	480	75	25 GB	100	15
3550	401-600	720	720	100	35 GB	100	20
4550	601-1000	1200	1200	125	45 GB	125	25
5550	1001-1500	1800	1800	200	55 GB	250	30
6550	1501-2000	2400	2400	300	65 GB	300	35
7550	2001-3000	3600	3600	100	75 GB	300	35

2.2 Front Panel & Back Panels

2.2.1 Ethernet Ports

The back panel contains two Fast Ethernet 10/100 Mbps ports. The following provides a description for each port:

LAN - The port labeled “LAN” should be connected to your local area network. Typically, this port is connected to the switch on your LAN that is connected to all of the filtered computers on the network.

WAN – The port labeled “WAN” should be connected to an Internet accessible connection. Typically, this port is connected to your firewall/router.
Bypass (Fail-Safe) Ports (not in all versions) – These ports are fail-safe ports which will be used instead of using the default ports. It is used for fail-safe features.

2.2.2 Console Port

The Console port provides a serial RS-232 interface to the iBoss. This port provides such functions such as configuring the network settings for the iBoss, displaying the IP Address settings for the iBoss, and restoring factory defaults. When using directly to a computer you must use a NULL MODEM DB9 serial cable.

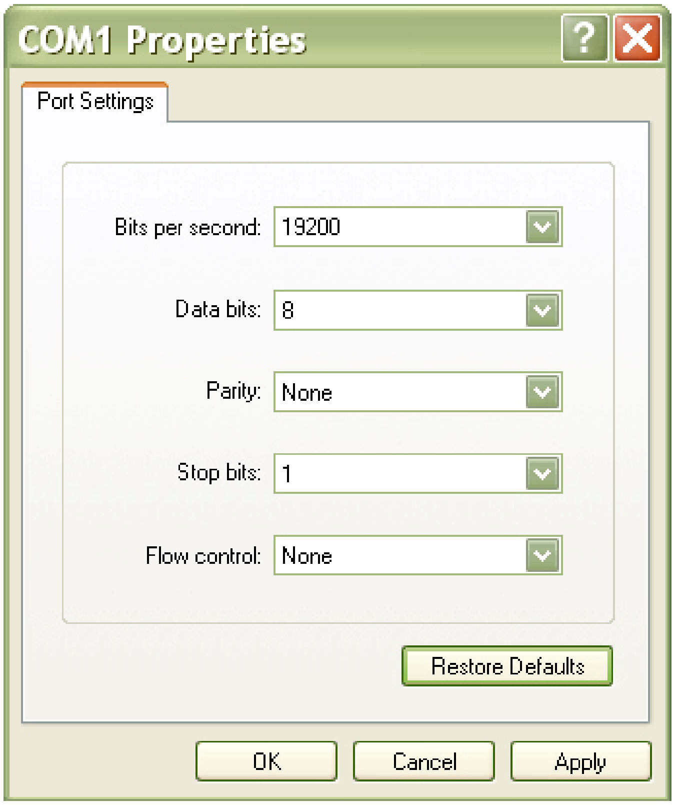
This port can be accessed via any console (COM) program. On windows, you can use the built-in program HyperTerminal. Other console programs that are available include PuTTY.

2.2.2.1 Console Port Settings

The settings for the console port are as follows:

Table 1 - Serial Console Port Settings

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None



COM1 Properties

Port Settings

Bits per second: 19200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 1 - COM Properties

3 Getting Started

This section describes initial setup and configuration of the iBoss appliance. This section contains information that will help you install the iBoss onto your network.

3.1 Operation Mode Overview

The iBoss provides its filtering functionality in a completely transparent fashion on the network. It does not segment a network, nor does it provide firewall or NAT capability. The iBoss filters traffic passing between the LAN and WAN port. The iBoss will actively scan traffic applying filtering rules and intercepting traffic when necessary. This allows the iBoss to achieve very high filtering performance without affecting network topology.

In order for the iBoss to perform filtering, it must be configured to have its own IP Address on the local network. The IP Address must be a static IP Address that is available on the network. Before connecting the iBoss to the network, the IP Address settings must be configured to match the network it is being installed on.

Once the address is configured, you will be able to access the iBoss while on the local network by either entering www.myiboss.com in your Web Browser, or entering the IP Address that was configured into the iBoss into your Web Browser.

3.2 iBoss Network Settings Configuration

Before the iBoss can be connected to the network, the IP Address settings that the iBoss will use must be configured. The iBoss must be configured with a static IP Address and will not obtain an IP Address through DHCP.

The iBoss ships with the following default IP Address settings. If these settings are sufficient for the network where it is being installed, you may not need to adjust the IP Address settings and skip this process.

Table 2 - Default iBoss IP Address Settings

IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS 1	192.168.1.1
DNS 2	0.0.0.0

There are two methods for configuring the IP Address settings of the iBoss. The first method involves using the serial console port. The second method involves connecting a single computer to the iBoss LAN port and configuring via the network using your Web Browser. If you have the external Report Manager, the default IP address is 192.168.1.20 for the external Enterprise Reporter.

3.2.1 Configuring Network Settings via Serial Console

To configure the network settings via the console terminal, connect the provided serial cable to the console port on the iBoss. After the iBoss has been powered on (typically full boot-up takes between 3-4 minutes), open a serial console program. On windows, you can use the built-in HyperTerminal program to access the console port.

The settings for the serial console COM connection are shown in the hardware specifications and are re-listed below:

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Once you have connected the serial cable from your computer to the console port and configured the console program, press the <Enter> key repeatedly until the configuration menu is displayed. Follow the options presented to configure the static IP Address settings for the iBoss.

3.2.2 Configuring Network Settings via the Network

You can also configure the iBoss network settings by connecting to the iBoss via a Web Browser. The following instructions apply when initially configuring the iBoss IP Address settings. If you have already configured the IP Address settings and wish to change them, you need to log into the iBoss using its current IP Address settings.

In order to do this, you must configure your computer to have a static IP address within the subnet of the iBoss default network settings. Configure your computer to have the following static IP Address:

Table 3 - Computer IP Address settings used to initially configure iBoss through the network

IP Address	192.168.1.15
Subnet Mask	255.255.255.0

You can leave the Gateway and DNS IP Address blank on your computer as they will not be needed.

With these settings in place, open a web browser and enter 192.168.1.10 into your Web Browser's address bar. This will bring up the iBoss home page. From the homepage, follow the Setup Internet Connection link to configure the iBoss IP Address Settings.

3.2.2.1 Configuring Network Settings via iBoss User Interface

The iBoss does not require any software installation. Instead, its user interface can be accessed directly using a standard Internet web browser. The web-based user interface allows you to configure your iBoss.

1. Verify that your computer has an IP address that is on the same subnet as the iBoss IP address, as stated above.
2. Open a standard Internet web browser application (Internet Explorer®, Firefox®, etc.).
3. In the URL address bar, enter the domain http://myiBoss.com and press <enter>. This will take you to the iBoss interface. If the iBoss interface does not load, enter the configured IP address of the iBoss (default: http://192.168.1.10) and press <enter>.

Note: The http://myiBoss.com webpage is built into the iBoss, so it is always accessible even though the Internet may not be. http://myiBoss.com is the configuration portal for the iBoss. You may access the user interface from any computer connected behind the iBoss.

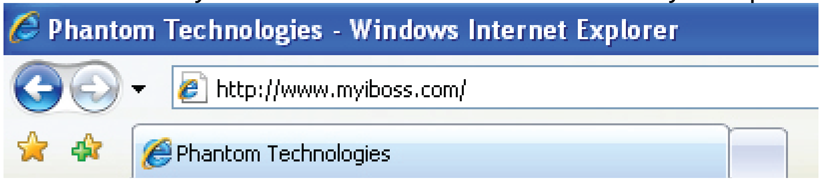
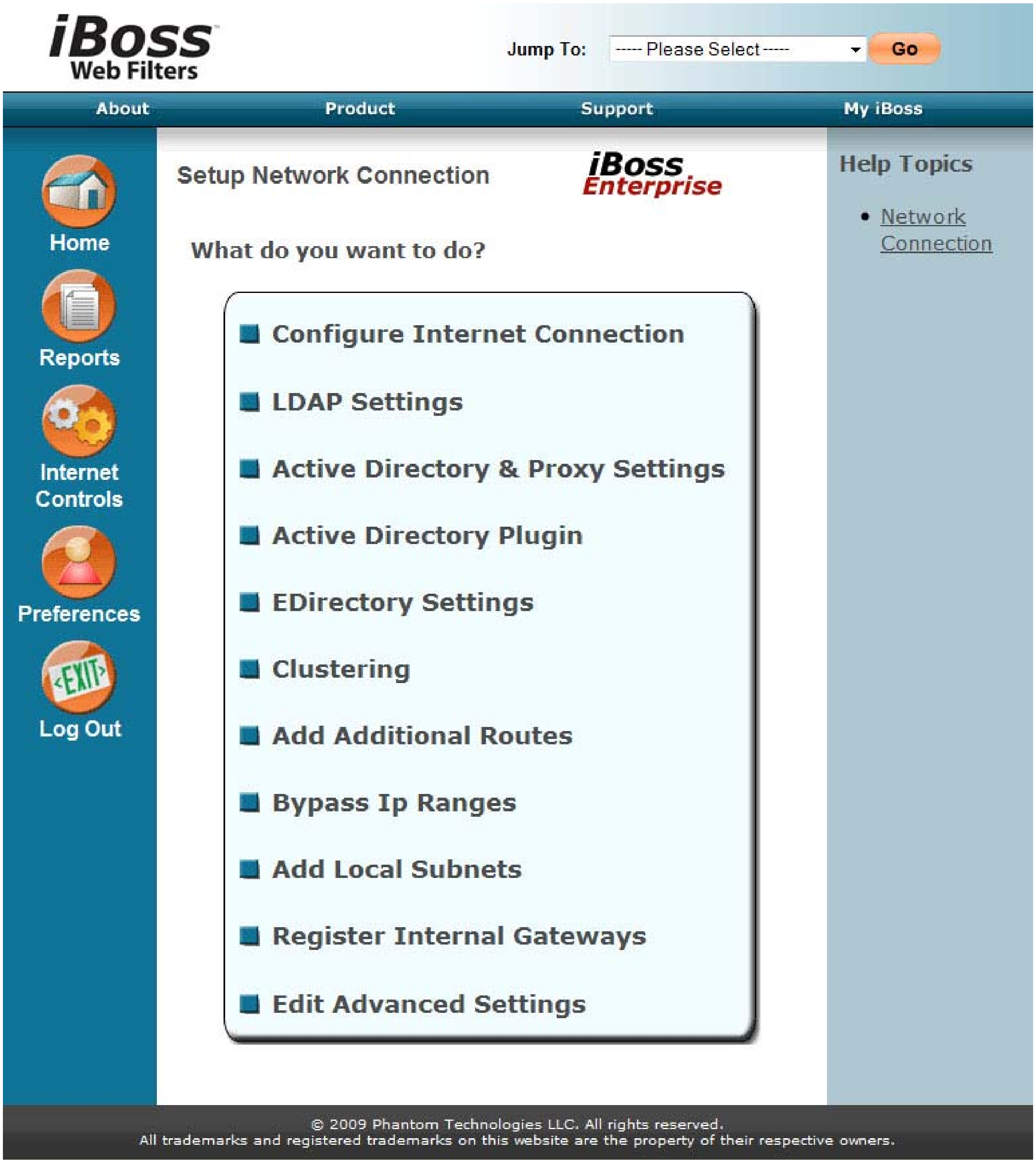


Figure 2 - iBoss User Interface

3.2.3 Setup Network Connection



Setup Network Connection

What do you want to do?

- Configure Internet Connection
- LDAP Settings
- Active Directory & Proxy Settings
- Active Directory Plugin
- EDirectory Settings
- Clustering
- Add Additional Routes
- Bypass Ip Ranges
- Add Local Subnets
- Register Internal Gateways
- Edit Advanced Settings

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 3 - Setup Network Connection

The "Setup Network Connection" menu lets you choose options for configuring the current iBoss connection settings. There are elevent options to choose from: Configure Internet Connection, LDAP Settings, Active Directory & Proxy Settings, Active Directory Plugin, eDirectory Settings, Clustering, Add Additional Routes, Bypass IP Ranges, Add Local Subnets, Register Internal Gateways and Edit Advanced Settings.

Configure Internet Connection - This option allows you to configure the Internet WAN connection.

LDAP Settings - This option allows you to setup your LDAP/Active Directory server so the iBoss can authenticate users from it.

Active Directory & Proxy Settings - This option allows you to setup the iBoss in a Proxy mode. This will allow automatic Active Directory authentication using NTLM.

Active Directory Plugin - This option allows you to setup the iBoss to work with your Active Directory Server using the iBoss Active Directory Plugin. This will allow automatic Active Directory authentication using the plugin on the server.

eDirectory Settings - This option allows you to setup the iBoss with your eDirectory servers for transparent authentication.

Clustering - This option allows you to setup multiple iBoss devices in a clustered environment to have settings synced automatically.

Add Additional Routes - This option allows you to add additional network routes for the iBoss.

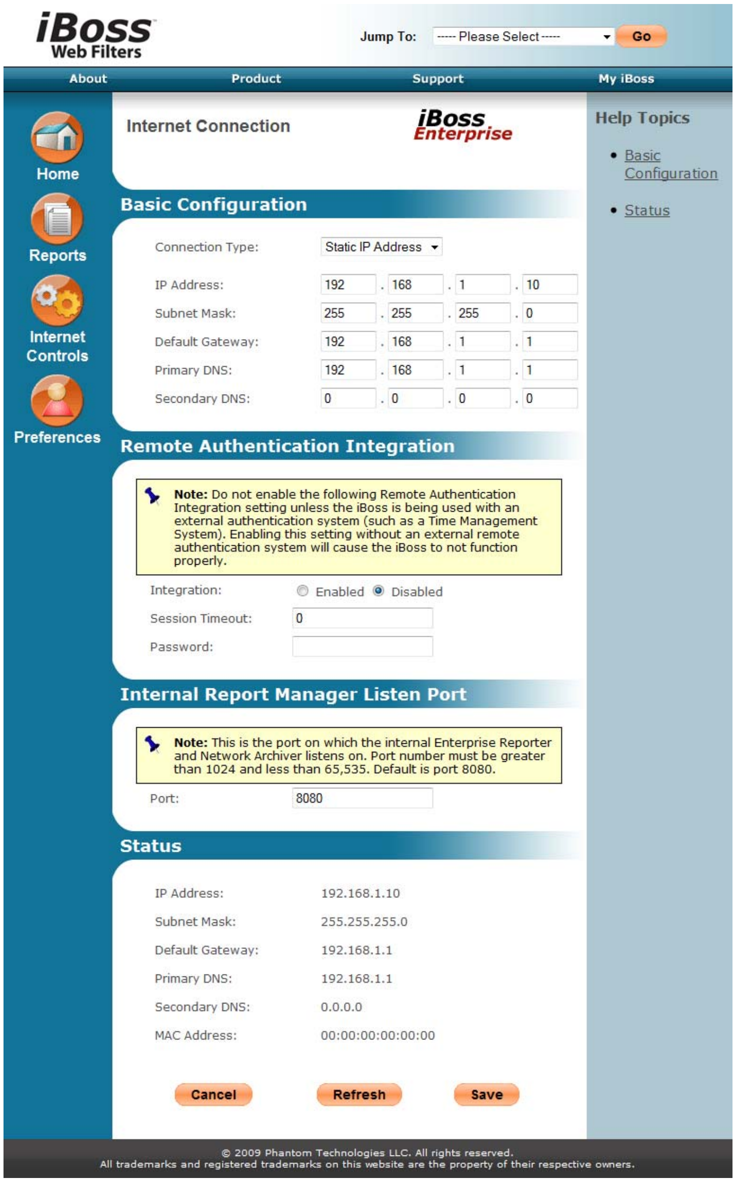
Bypass IP Ranges – This option allows you to bypass IP ranges which you would like to completely bypass the iBoss filtering engine.

Add Additional Local Subnets - This option allows you to add additional local subnets.

Register Internal Gateways - This option allows you to register gateways that are internal to your network (on the LAN side of the iBoss).

Edit Advanced Settings - This option allows you to configure the advanced network settings.

3.2.3.1 Configure Internet Connection



Internet Connection

Basic Configuration

Connection Type: Static IP Address

IP Address: 192 . 168 . 1 . 10

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Primary DNS: 192 . 168 . 1 . 1

Secondary DNS: 0 . 0 . 0 . 0

Remote Authentication Integration

Note: Do not enable the following Remote Authentication Integration setting unless the iBoss is being used with an external authentication system (such as a Time Management System). Enabling this setting without an external remote authentication system will cause the iBoss to not function properly.

Integration: ○ Enabled ● Disabled

Session Timeout: 0

Password:

Internal Report Manager Listen Port

Note: This is the port on which the internal Enterprise Reporter and Network Archiver listens on. Port number must be greater than 1024 and less than 65,535. Default is port 8080.

Port: 8080

Status

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Primary DNS: 192.168.1.1

Secondary DNS: 0.0.0.0

MAC Address: 00:00:00:00:00:00

Cancel Refresh Save

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 4 - Configure Internet Connection

Connection Type – The iBoss will need to be configured to have a static IP address.

Manually enter network settings for your WAN connection. These settings should be a unique IP address and match your local network. If you are using Active Directory or have a domain controller, use this IP address for the DNS 1 address.

Note: Secondary DNS is not required.

Remote Authentication Integration

(PAUL) This feature allows Remote Authentication Integration

Internal Report Manager Listen Port

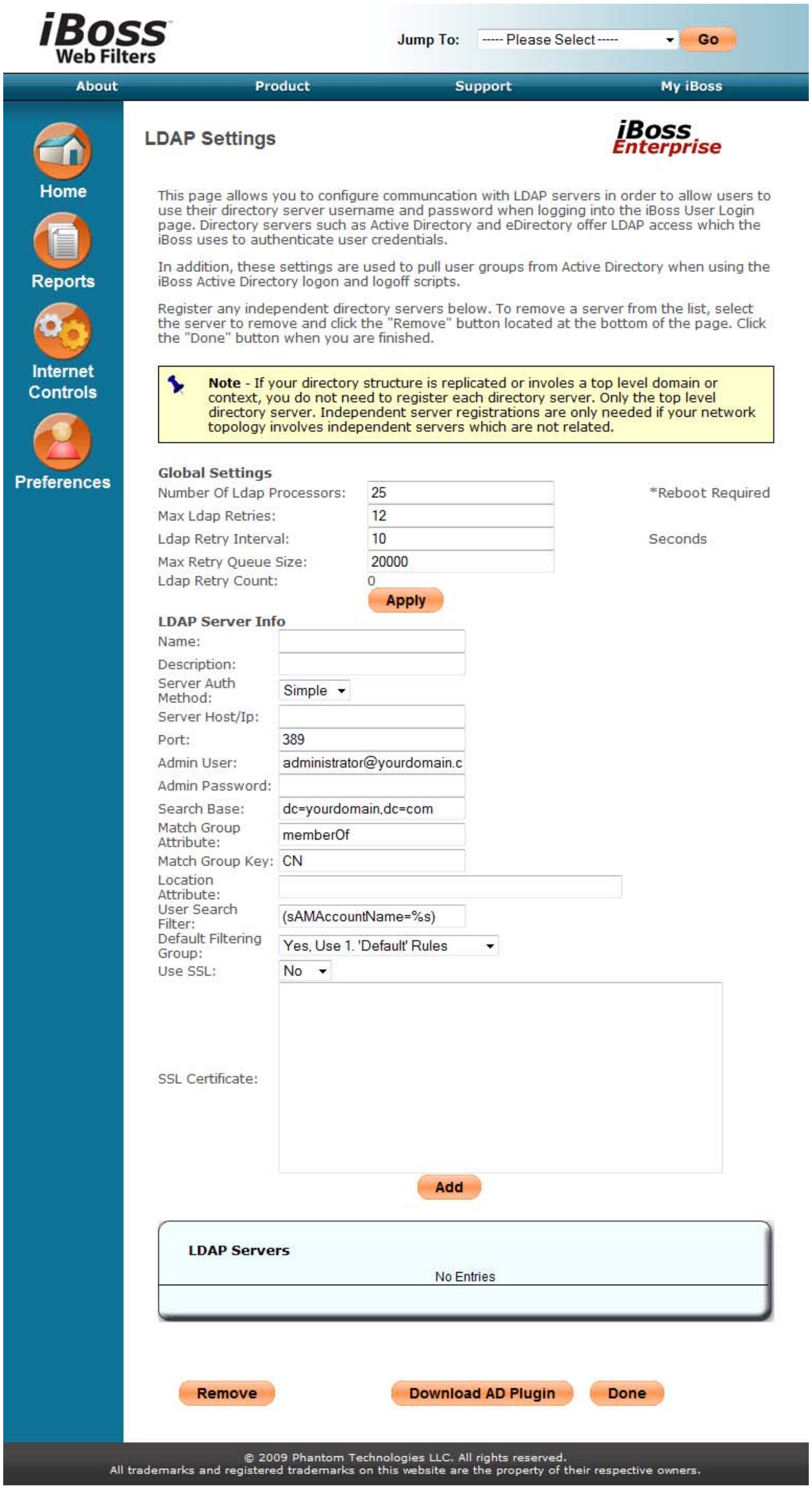
This section allows you to change the port number that the iBoss reports are served from.

Click "**Save**" when you have finished the configuration above. You have completed the WAN configuration for the Static IP Address connection type.

Note: Once the iBoss has been configured, you may return your computer's network settings back to their original settings. Also, if the iBoss has already been configured to have a different IP Address, you must log into the iBoss using these settings. If you do not know what the settings were, you will have to log into the iBoss via the serial console port using the instructions described above.

Important Note: You will also need to bypass your DNS or Domain Controller MAC or IP address within the iBoss. Please refer to Identifying Computers and Bypass IP Ranges section for further information.

3.2.3.2 LDAP Settings



LDAP Settings

This page allows you to configure communcation with LDAP servers in order to allow users to use their directory server username and password when logging into the iBoss User Login page. Directory servers such as Active Directory and eDirectory offer LDAP access which the iBoss uses to authenticate user credentials.

In addition, these settings are used to pull user groups from Active Directory when using the iBoss Active Directory logon and logoff scripts.

Register any independent directory servers below. To remove a server from the list, select the server to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note - If your directory structure is replicated or involes a top level domain or context, you do not need to register each directory server. Only the top level directory server. Independent server registrations are only needed if your network topology involves independent servers which are not related.

Global Settings

Number Of Ldap Processors:	25	*Reboot Required
Max Ldap Retries:	12	
Ldap Retry Interval:	10	Seconds
Max Retry Queue Size:	20000	
Ldap Retry Count:	0	

LDAP Server Info

Name:	
Description:	
Server Auth Method:	Simple
Server Host/Ip:	
Port:	389
Admin User:	administrator@yourdomain.c
Admin Password:	
Search Base:	dc=yourdomain,dc=com
Match Group Attribute:	memberOf
Match Group Key:	CN
Location Attribute:	
User Search Filter:	(sAMAccountName=%s)
Default Filtering Group:	Yes, Use 1. 'Default' Rules
Use SSL:	No
SSL Certificate:	

LDAP Servers

No Entries

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 5 - LDAP Settings

Global Settings – This section allows you to set global LDAP settings.

Number of Ldap Processors – This is how many ldap processors are used within the iBoss for authentication. 25 is the default.

Max Ldap Retries – This is the number of retries before the authentication is no longer tried. 12 is default.

Ldap Retry Interval – This is the interval between retries if authentication is not successful. 10 Seconds is the default.

Max Retry Queue Size – This is the max number of queue spots for Ldap authentication retries.

LDAP Server Info – This section allows you to individually enter each LDAP server's information. You may add multiple LDAP servers here.

Name - This is the name of the server to assist in identification.

Description – This option allows you to set a description for the server that is being added.

Server Authentication Method - This option allows you to configure the server authentication method required by your LDAP server. Simple is recommended.

Server Host/Ip - This is the domain or IP address of the LDAP server. Example: iphantom.com or 10.0.0.1

Port - This allows you to change the port number that is used to communicate to your LDAP server. Port 389 is most common and is recommended.

Admin User - This is the Username of an administrative or root user which has administrative rights to your LDAP server. The user must be able to perform searches on your LDAP server. This user is used to look up user logins. Example: administrator@iphantom.com.

Admin Password – This is the password to your LDAP administrator user above. Some special characters are not accepted.

Search Base - This is the base by which searches for users will be made. If you have a large directory you may choose a base other than the top as long as all users that need to be authenticated are under this base. It is recommended that you set this to the top of your LDAP directory. Example: If your LDAP domain is iphantom.com, you would use the following settings: Active Directory sample: dc=iphantom,dc=com

Match Group Attribute - This option allows you to set the attribute within the user record found to search for groups. The group names are matched to the iBoss filtering groups. The group names must match exactly.

For example, if you have a LDAP group named administrators, the user record found during login would be searched for this attribute. The values found would be compared to your iBoss filtering group. If there is a match, it would use that filtering group for that user.

If a user belongs to multiple groups, they will be filtered using the highest priority group based on lowest number. (ex: filtering group 1 has the highest priority). Example: Active Directory sample: memberOf

Match Group Key - If a filtering group attribute is found and contains many key value pairs, you can limit the group match to a particular key. For example, if a group value contains 'CN=managers,OU=support' you may choose to match groups to the 'CN' key which would match the word 'managers' to the iBoss filtering group. If you leave this field blank, the entire group attribute will be used. Example: Active Directory sample: CN

Location Attribute - This option allows you to put the location field on where the LDAP server is located.

User Search Filter - This is the filter that is used to search for a username in the LDAP server. This filter must result in a single user record. The filter must also contain %s which will be replaced by the username. There must not be any other percent signs in the search filter. Example: Active Directory sample: (sAMAccountName=%s)

Default Filtering Group - This option allows you to use a default filtering group if no LDAP group can be matched with an active iBoss Filtering Group. You can choose to Deny Access if no group match or choose between the different filtering groups.

Use SSL – This option allows you to turn on SSL encryption with your LDAP server

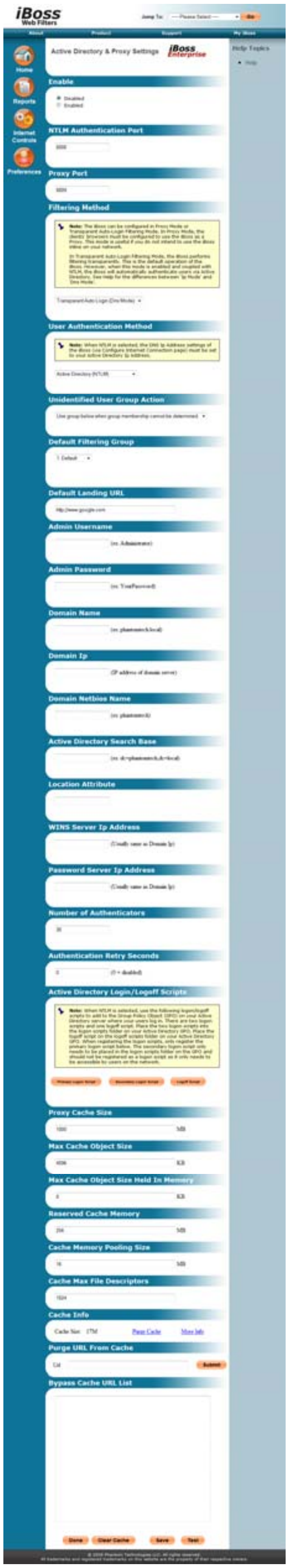
SSL Certificate – This section allows you to paste the Certificate for the SSL Encryption used by your LDAP server.

Once you have finished entering information, click the **Add** button. Once it has been added, click the **Test** button next to the entry in the box. If you would like to edit the server information, click the **Edit** button and the fields will be able to edit. Once updated, click the **Edit** or **Save** button.

3.2.3.2.1.1 Match Active Directory Groups with iBoss Filtering Groups

Once you have the LDAP/Active Directory Settings configured, you will need to match your Active Directory groups with the iBoss filtering groups. You can simply rename the filtering group names to match the Active Directory group names. To do this, from the main menu click on Identify Computers & Users, then click the ‘Groups’ tab. You can import groups by clicking the ‘Import From LDAP/AD’ button. This will ask you to save or open the list of groups from Active Directory. Open it in a text editor and copy the group names. Then click on the ‘Import’ button and paste the groups. The first line corresponds to filtering group 1. If a user belongs to multiple groups, the user will fall under the highest priority filtering group number. Please refer to Filtering Groups section for more details.

3.2.3.3 Active Directory & Proxy Settings



iBoss Web Filters

Jump To: ---- Please Select ---- Go

Active Directory & Proxy Settings

Enable

● Disabled
○ Enabled

NTLM Authentication Port

[illegible]

Proxy Port

[illegible]

Filtering Method

Note: The iBoss can be configured in Proxy Mode or Transparent Auto-Login Filtering Mode. In Proxy Mode, the clients' browsers must be configured to use the iBoss as a Proxy. This mode is useful if you do not intend to use the iBoss inline on your network.

In Transparent Auto-Login Filtering Mode, the iBoss performs filtering transparently. This is the default operation of the iBoss. However, when this mode is enabled and coupled with NTLM, the iBoss will automatically authenticate users via Active Directory. See Help for the differences between 'Ip Mode' and 'Dns Mode'.

Transparent Auto-Login (Dns Mode)

User Authentication Method

Note: When NTLM is selected, the DNS Ip Address settings of the iBoss (via Configure Internet Connection page) must be set to your Active Directory Ip Address.

Active Directory (NTLM)

Unidentified User Group Action

Use group below when group membership cannot be determined

Default Filtering Group

1 Default

Default Landing URL

http://www.google.com

Admin Username

(ex. Administrator)

Admin Password

(ex. YourPassword)

Domain Name

(ex. phantomtech.local)

Domain Ip

(IP address of domain server)

Domain Netbios Name

(ex. phantomtech)

Active Directory Search Base

(ex. dc=phantomtech,dc=local)

Location Attribute

WINS Server Ip Address

(Usually same as Domain Ip)

Password Server Ip Address

(Usually same as Domain Ip)

Number of Authenticators

30

Authentication Retry Seconds

0 (0 = disabled)

Active Directory Login/Logoff Scripts

Note: When NTLM is selected, use the following logon/logoff scripts to add to the Group Policy Object (GPO) on your Active Directory server where your users log in. There are two logon scripts and one logoff script. Place the two logon scripts into the logon scripts folder on your Active Directory GPO. Place the logoff script on the logoff scripts folder on your Active Directory GPO. When registering the logon scripts, only register the primary logon script below. The secondary logon script only needs to be placed in the logon scripts folder on the GPO and should not be registered as a logon script as it only needs to be accessible to users on the network.

Proxy Cache Size

1000 MB

Max Cache Object Size

4096 KB

Max Cache Object Size Held In Memory

8 KB

Reserved Cache Memory

256 MB

Cache Memory Pooling Size

16 MB

Cache Max File Descriptors

1024

Cache Info

Cache Size: 17M Purge Cache More Info

Purge URL From Cache

Url

Bypass Cache URL List

© 2010 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 6 – Active Directory & Proxy Settings

By default, the iBoss works as an inline filter that actively scans Internet streams to and from the Internet. This allows the iBoss to scan web requests and Web 2.0 application streams. In this mode, each computer is typically named after the primary user of the computer. In the reports, the username will represent the computer.

Alternatively, the iBoss can be configured to work as a proxy. This mode is typical of most other filters. In this mode, computers make requests to the iBoss at which point the request is made by the iBoss on their behalf with filtering applied. This requires that proxy settings be placed in the browser through an Active Directory Group Policy Object or manually. In this mode, the proxy will analyze web requests. For applications to be analyzed, the iBoss must be placed inline on the network so that the iBoss can see the streams. For Web 2.0 streams, the policy for that computer will be applied instead of the proxy user.

If using the iBoss in an Active Directory environment, NTLM can be used to transparently log the user onto the proxy using the Active Directory credentials. This will apply to all web requests. The iBoss can still be used in proxy mode in environments that do not use Active Directory. In this case, users will need to be created within the iBoss and the user will be prompted the first time they open a browser for their credentials.

To use the iBoss as a proxy filter, you will need to configure the settings for it. You may configure the settings by going to Configure Proxy Settings under the Setup Network Connections section. You will first need to enable this feature. You may change the port number that it uses (by default it uses port 8008). You may then select which User Authentication Method to use. If you have an Active Directory server, you may select Active Directory (NTLM). If you do not have an Active Directory server, you may still use the iBoss in Proxy mode and authenticate using the iBoss users. Enter all the information for the remaining fields like username and password for your active directory, etc. Please see the examples and help link for further details.

Enable Active Directory & Proxy Support - This option allows you to enable or disable Active Directory & Proxy Support. To use the iBoss as a proxy filter or NTLM transparent authentication with Active Directory, you will need to enable this option.
NTLM Authentication Port – This option allows you to configure the NTLM Port that the iBoss uses to authenticate users.

Proxy Port - This option allows you to configure the port number to use as a proxy port for the users' browser settings.

Filtering Method – The iBoss can be configured in Proxy Mode or Transparent Auto-Login Filtering Mode. In Proxy Mode, the clients' browsers must be configured to use the iBoss as a Proxy. This mode is useful if you do not intend to use the iBoss inline on your network.

In Transparent Auto-Login Filtering Mode, the iBoss performs filtering transparently. This is the default operation of the iBoss. However, when this mode is enabled and coupled with NTLM, the iBoss will automatically authenticate users via Active Directory. See Help for the differences between 'Ip Mode' and 'Dns Mode'.his option allows you to change the filtering method.

The options are **Proxy Mode, Transparent Auto-Login (Dns Mode), Transparent Auto-Login (Ip Mode), Proxy Only (No Filtering).**

User Authentication Method - This option allows you to configure whether to authenticate using Active Directory or iBoss user logins.

Note: When NTLM is selected, the DNS IP Address settings of the iBoss must be set to your Active Directory IP Address.

Unidentified User Group Action - This option allows you to change the action used when an unidentified user is found. You can either choose to block access or use a filtering group.

Default Filtering Group - This option allows you to choose the filtering group that is used when an unidentified user is found.

Default Landing URL - This option allows you to specify where the page is redirected after a successful authentication. This is only the case where NTLM was done without an original destination page was first requested.

Admin Username (Only in Active Directory (NTLM) Authentication Method) **–** This is the username of the LDAP administrator. Ex: Administrator.

Admin Password (Only in Active Directory (NTLM) Authentication Method) **-** This is the password of the administrator user above for your LDAP/Active Directory server.

Domain Name (Only in Active Directory (NTLM) Authentication Method) – This is your Active Directory domain. Ex: phantomtech.local

Domain IP (Only in Active Directory (NTLM) Authentication Method) – This is the Domain IP address of your Domain Controller (Active Directory server)

Domain Netbios Name (Only in Active Directory (NTLM) Authentication Method) – This is the name of your workgroup or Domain Netbios name. This is the what shows up in the drop down menu when users log in. Ex: phantomtech

Active Directory Search Base (Only in Active Directory (NTLM) Authentication Method) – This is the search base of your Active Directory server. Ex: dc=phantomtech,dc=local

Location Attribute (Only in Active Directory (NTLM) Authentication Method) – This is the location Attribute within Active Directory if you have multiple locations.

WINS Server IP Address (Only in Active Directory (NTLM) Authentication Method) – This is the WINS Server IP Address which is commonly the IP address of your Active Directory server.

Password Server IP Address (Only in Active Directory (NTLM) Authentication Method) – This is the Password Server IP Address which is commonly the IP address of your Active Directory server.

Number of Authenticators – This is the number of NTLM authenticators that try to do authentication.

Authentication Retry Seconds – This option allows you to configure how long to retry authentication in seconds. 0 = disabled.

Active Directory Logon/Logoff Scripts – When NTLM is selected, use the following logon/logoff scripts to add to the Group Policy Object (GPO) on your Active Directory server where your users log in. There are two logon scripts and one logoff script. Place the two logon scripts into the logon scripts folder on your Active Directory GPO. Place the logoff script on the logoff scripts folder on your Active Directory GPO. When registering the logon scripts, only register the primary logon script below. The secondary logon script only needs to be placed in the logon scripts folder on the GPO and should not be registered as a logon script as it only needs to be accessible by users on the network.

You can then download the Primary Logon Script, Secondary Logon Script, and Logoff Script. These scripts can be added to your Active Directory Group Policy to transparently authenticate when users log in.

After entering the information, click 'Save' and then 'Test'.

Proxy Cache Size – This option allows you to set the Proxy Cache Size. The default is 1000 MB.

Max Cache Object Size – This option allows you to set the Max Cache Object Size. The default is 4096 KB.

Max Cache Object Size Held In Memory – This option allows you to configure the Max Cache object size held in memory. The default is 8 KB.

Reserved Cache Memory – This option allows you to set the Reserved Cache Memory. The default is 256 MB

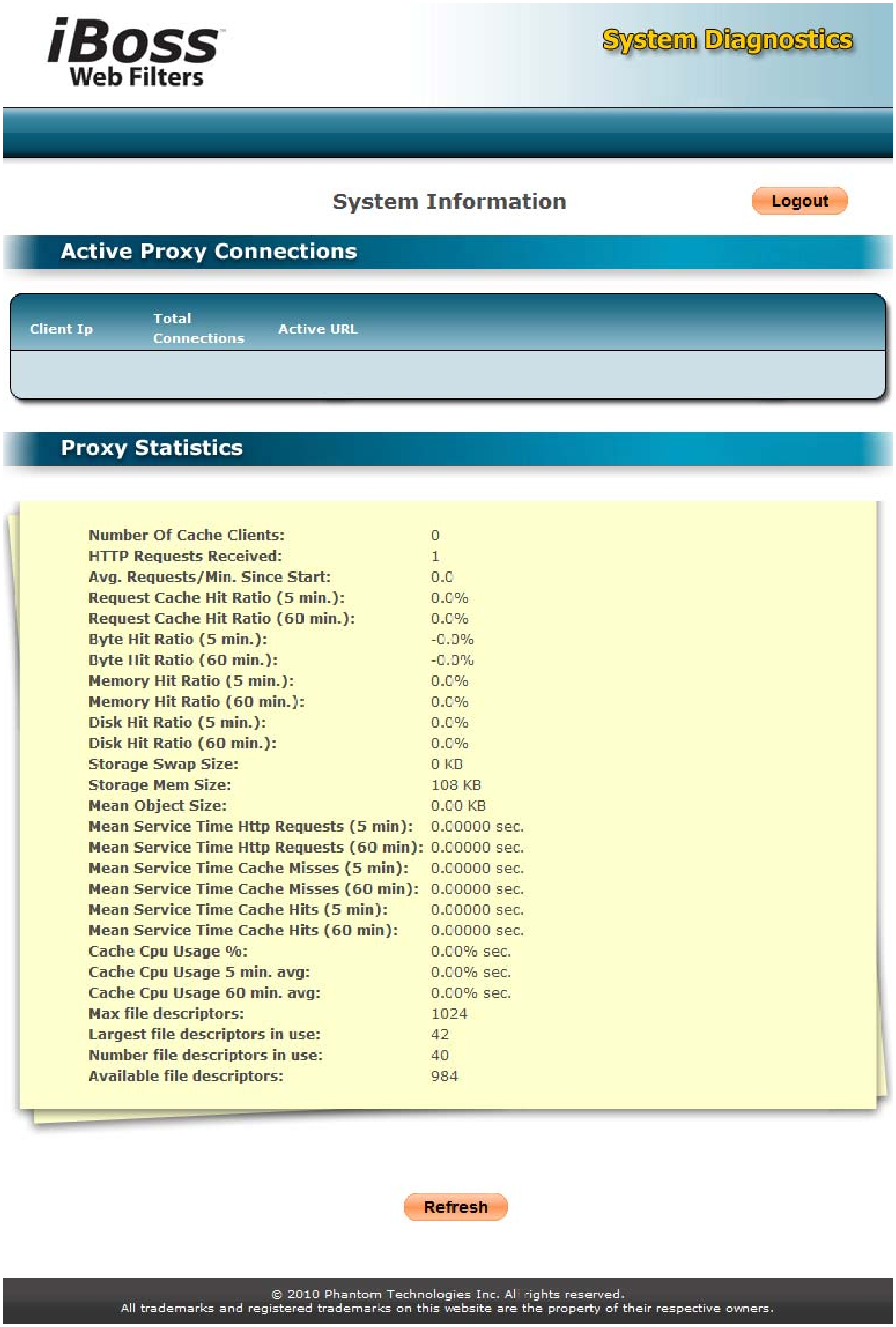
Cache Memory Pooling Size – This option allows you to set the Pooling Size. The default is 16 MB.

Cache Max File Descriptors – This option allows you to set the Cache Max File Descriptors. 1024 is the default.

Cache Info – This shows the size of the Cache. You can choose to Purge Cache or More information about the proxy. See screenshot below for proxy information.

Purge URL From Cache – This option allows you to purge individual URLs from the Proxy cache.

Bypass Cache URL List - This option allows you to bypass URLs in the proxy.



System Information

Active Proxy Connections

Client Ip	Total Connections	Active URL

Proxy Statistics

Number Of Cache Clients:	0
HTTP Requests Received:	1
Avg. Requests/Min. Since Start:	0.0
Request Cache Hit Ratio (5 min.):	0.0%
Request Cache Hit Ratio (60 min.):	0.0%
Byte Hit Ratio (5 min.):	-0.0%
Byte Hit Ratio (60 min.):	-0.0%
Memory Hit Ratio (5 min.):	0.0%
Memory Hit Ratio (60 min.):	0.0%
Disk Hit Ratio (5 min.):	0.0%
Disk Hit Ratio (60 min.):	0.0%
Storage Swap Size:	0 KB
Storage Mem Size:	108 KB
Mean Object Size:	0.00 KB
Mean Service Time Http Requests (5 min):	0.00000 sec.
Mean Service Time Http Requests (60 min):	0.00000 sec.
Mean Service Time Cache Misses (5 min):	0.00000 sec.
Mean Service Time Cache Misses (60 min):	0.00000 sec.
Mean Service Time Cache Hits (5 min):	0.00000 sec.
Mean Service Time Cache Hits (60 min):	0.00000 sec.
Cache Cpu Usage %:	0.00% sec.
Cache Cpu Usage 5 min. avg:	0.00% sec.
Cache Cpu Usage 60 min. avg:	0.00% sec.
Max file descriptors:	1024
Largest file descriptors in use:	42
Number file descriptors in use:	40
Available file descriptors:	984

Figure 7 - Proxy Cache System Information

3.2.3.3.1.1 Automatic GPO Setup for NTLM with Login/Logoff Scripts

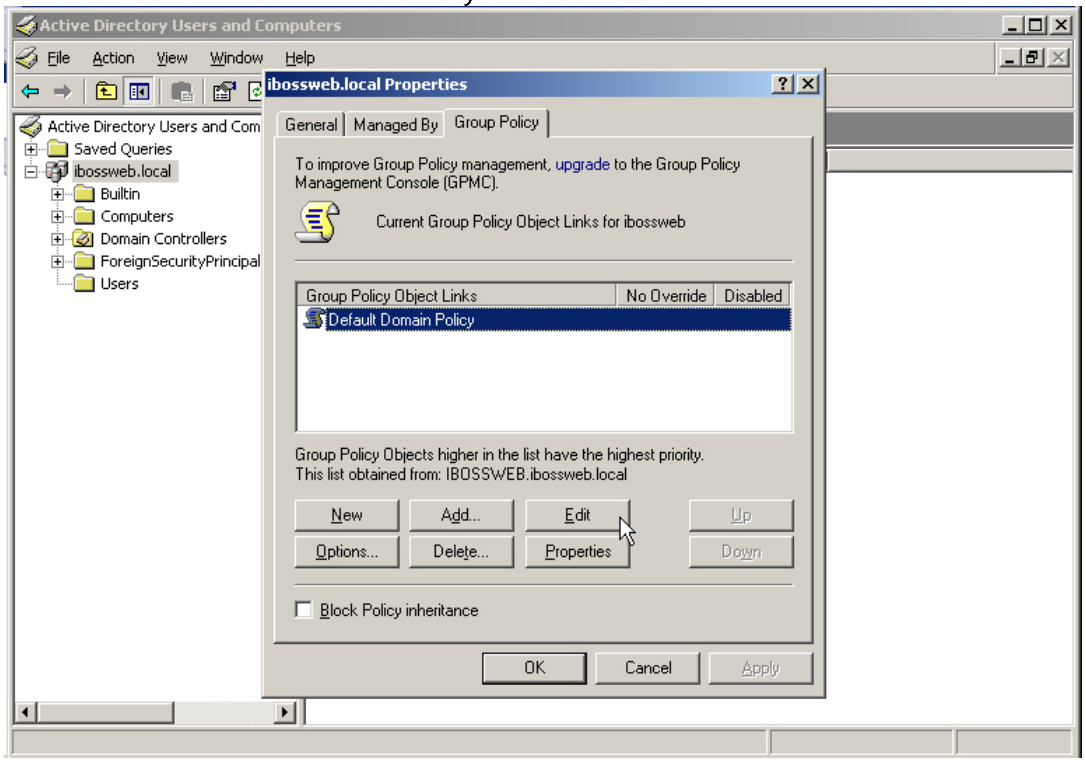
Add the Logon and Logoff scripts to the Active Directory as a group policy when users log in and log off for NTLM Authentication. To do this, follow these steps:

1. From within your Active Directory server, go to Start->Programs->Administrative Tools and click on 'Active Directory Users and Computers'
2. Right-click on the domain and select Properties, then select the Group Policy tab.
3. Select the 'Default Domain Policy' and click Edit.
4. Navigate to User Configuration -> Windows Settings -> Scripts (Logon/Logoff)
5. Double click Logon and click Show Files, move the login files here.
6. Next click add and select the primary logon script
7. Do the same for the Logoff script.

3.2.3.3.1.2 Automatic GPO Setup for NTLM with Internet Explorer

The automatic GPO Setup for NTLM will allow your Active Directory server to setup and distribute the Proxy Settings within the domain clients' Internet Explorer browser for you. To do this, follow these steps:

1. From within your Active Directory server, go to Start->Programs->Administrative Tools and click on 'Active Directory Users and Computers'
2. Right-click on the domain and select Properties, then select the Group Policy tab.
3. Select the 'Default Domain Policy' and click Edit.



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for ibossweb

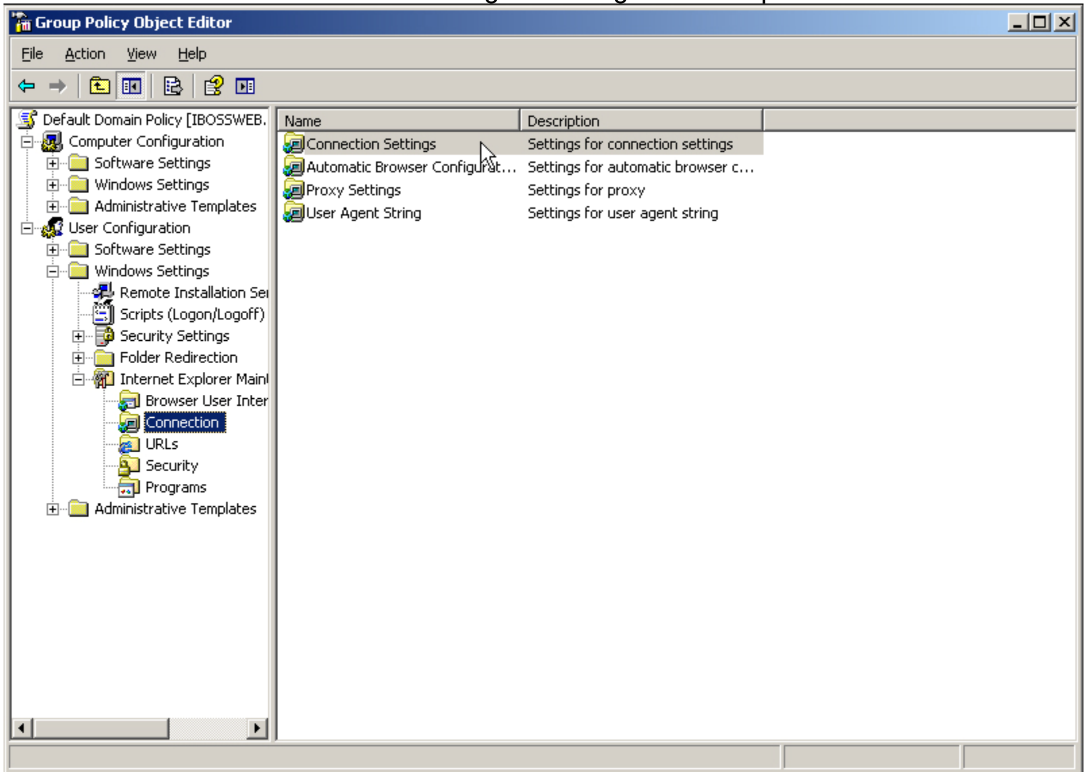
Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: IBOSSWEB.ibossweb.local

□ Block Policy inheritance

Figure 8 - GPO Default Domain Policy

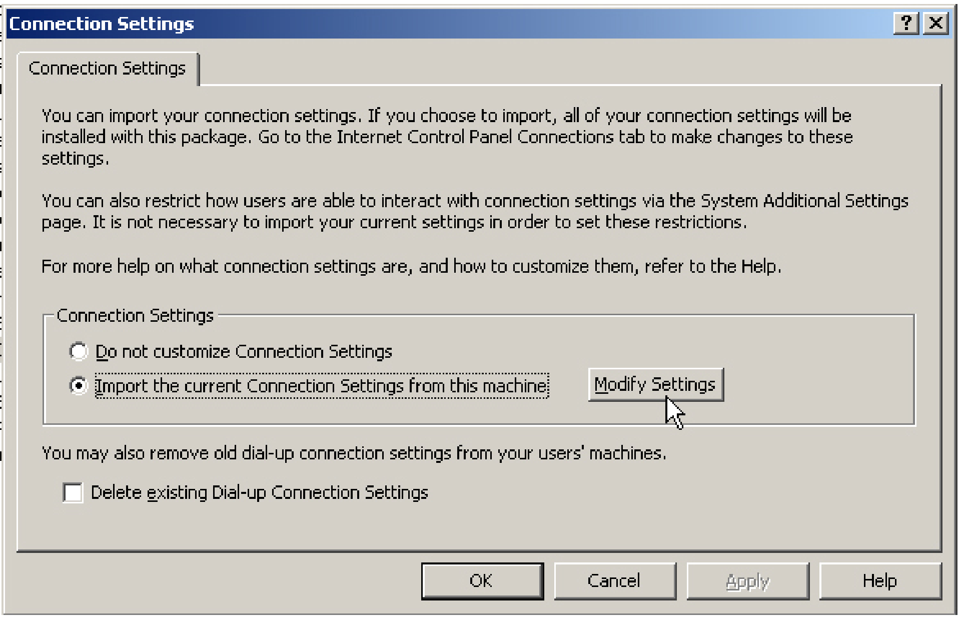
4. Navigate to User Configuration->Windows Settings->Internet Explorer Maintenance->Connection
5. Double-click on Connection Settings in the right window panel.



Name	Description
Connection Settings	Settings for connection settings
Automatic Browser Configurat...	Settings for automatic browser c...
Proxy Settings	Settings for proxy
User Agent String	Settings for user agent string

Figure 9 - GPO Connection Settings

6. Select the option ‘Import the Connection Settings’ and click Modify Settings.



You can import your connection settings. If you choose to import, all of your connection settings will be installed with this package. Go to the Internet Control Panel Connections tab to make changes to these settings.

You can also restrict how users are able to interact with connection settings via the System Additional Settings page. It is not necessary to import your current settings in order to set these restrictions.

For more help on what connection settings are, and how to customize them, refer to the Help.

Connection Settings

○ Do not customize Connection Settings

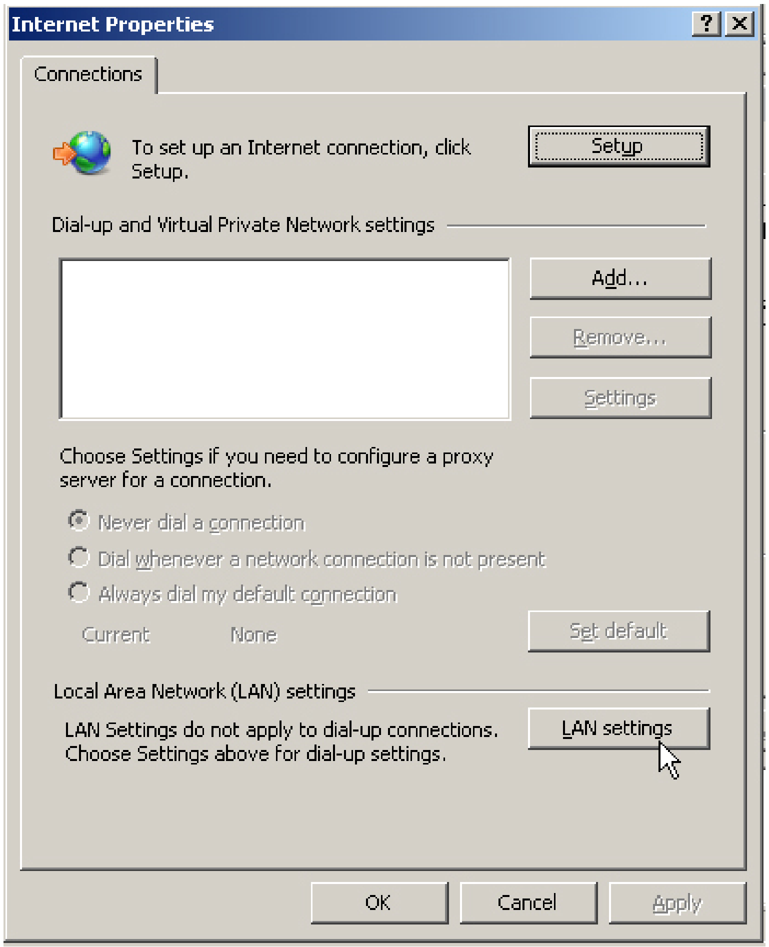
● Import the current Connection Settings from this machine

You may also remove old dial-up connection settings from your users' machines.

☐ Delete existing Dial-up Connection Settings

Figure 10 - GPO Import the Connection Settings

7. Click ‘LAN Settings’ and check ‘Use a proxy server’.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

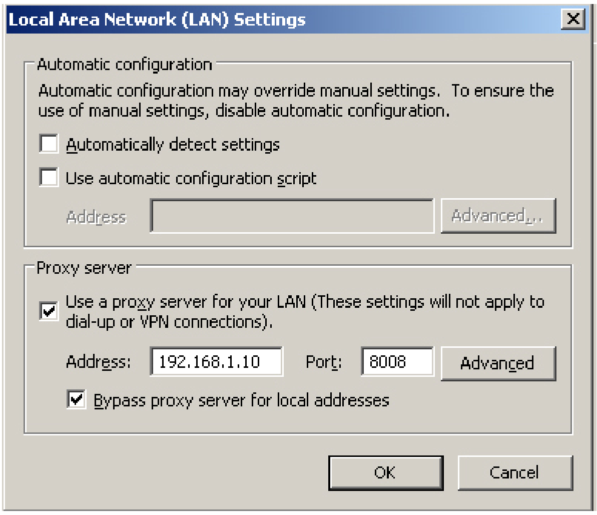
Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Figure 11 - GPO Use Proxy Server

8. Enter the IP address of the iBoss and the Proxy port that is setup on the iBoss (default 8008) and click OK.



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 192.168.1.10 Port: 8008

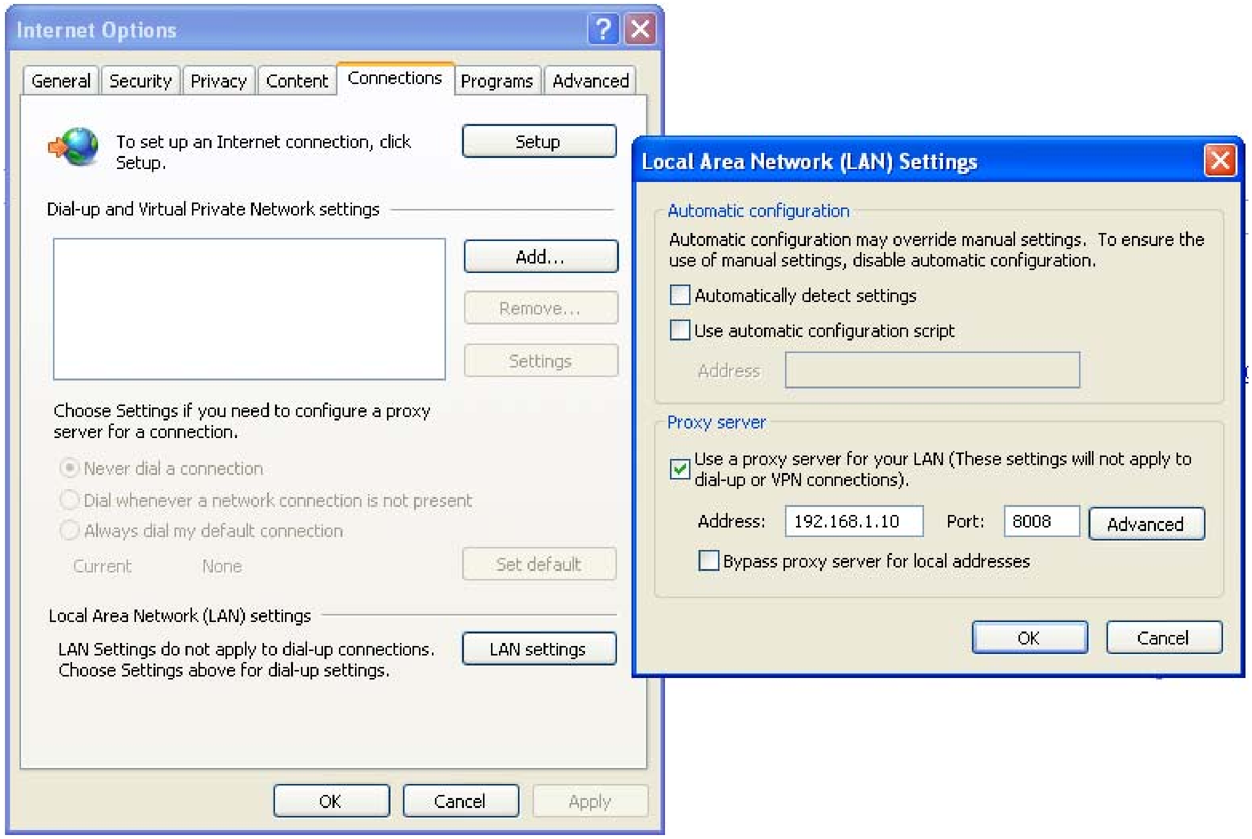
☑ Bypass proxy server for local addresses

Figure 12 - GPO Local Area Network Settings

9. This setting will now be enforced and the next policy update.

3.2.3.3.1.3 Manually Setup Proxy Browser Settings

If you are not using the Active Directory/NTLM features, but still want to use the iBoss as a proxy filter, you will need to manually setup the Proxy Settings for the browser. To do this with Internet Explorer, click on Tools->Internet Options-> Connections Tab->LAN Settings and then check Use a proxy server for your LAN. Enter the IP address of the iBoss and the proxy port number (default 8008) and click OK. To do this in Firefox web browser, click Tools-> Options -> Advanced -> Network Tab -> Settings Button -> Select Manual proxy configuration. Enter the IP address under the HTTP Proxy setting for the iBoss IP address and the proxy port (default 8008) and click OK. This will now prompt a user to login before using the Internet.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Automatic configuration

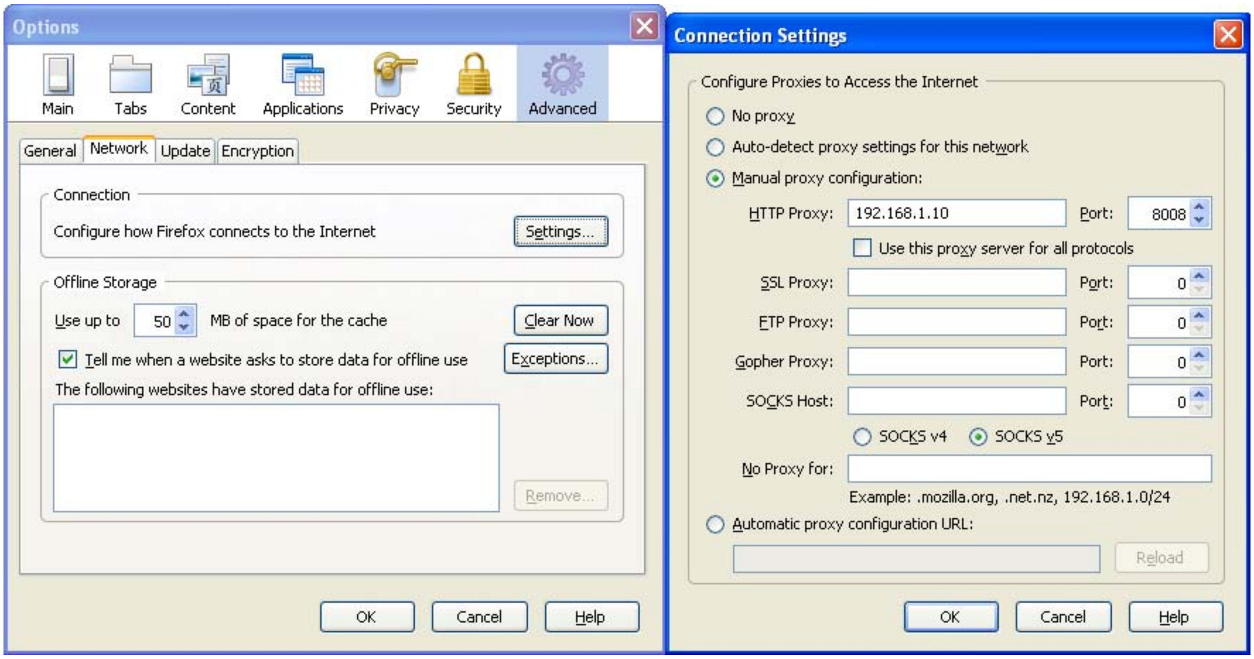
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings
□ Use automatic configuration script
Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 192.168.1.10 Port: 8008
□ Bypass proxy server for local addresses

Figure 13 - Manual Proxy with Internet Explorer



Connection

Configure how Firefox connects to the Internet

Offline Storage

Use up to 50 MB of space for the cache

☑ Tell me when a website asks to store data for offline use

The following websites have stored data for offline use:

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy:	192.168.1.10	Port:	8008
	□ Use this proxy server for all protocols		
SSL Proxy:		Port:	0
FTP Proxy:		Port:	0
Gopher Proxy:		Port:	0
SOCKS Host:		Port:	0
	○ SOCKS v4 ● SOCKS v5		
No Proxy for:			

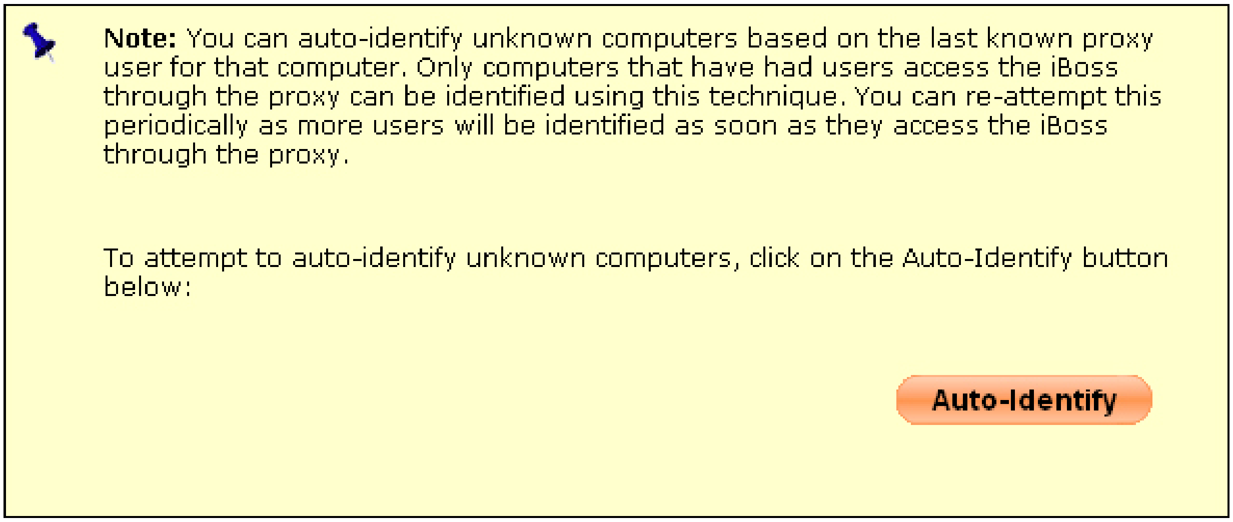
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Figure 14 - Manual Proxy with Mozilla Firefox

3.2.3.3.1.4 Automatic Identify of Unknown Computers

The automatic Identify of Unknown Computers can be found under Identify Computers & Users. You can auto-identify unknown computers based on the last known proxy user for that computer. Only computers that have had users access the iBoss through the proxy can be identified using this technique. You can re-attempt this periodically as more users will be identified as soon as they access the iBoss through the proxy. To attempt to auto-identify unknown computers, click the Auto-Identify button. This will identify the computers which proxy users have logged in to and place the identified computer under the Identified Computers table. The Computer Nick Name will show up with the last known user with a star in front of it.

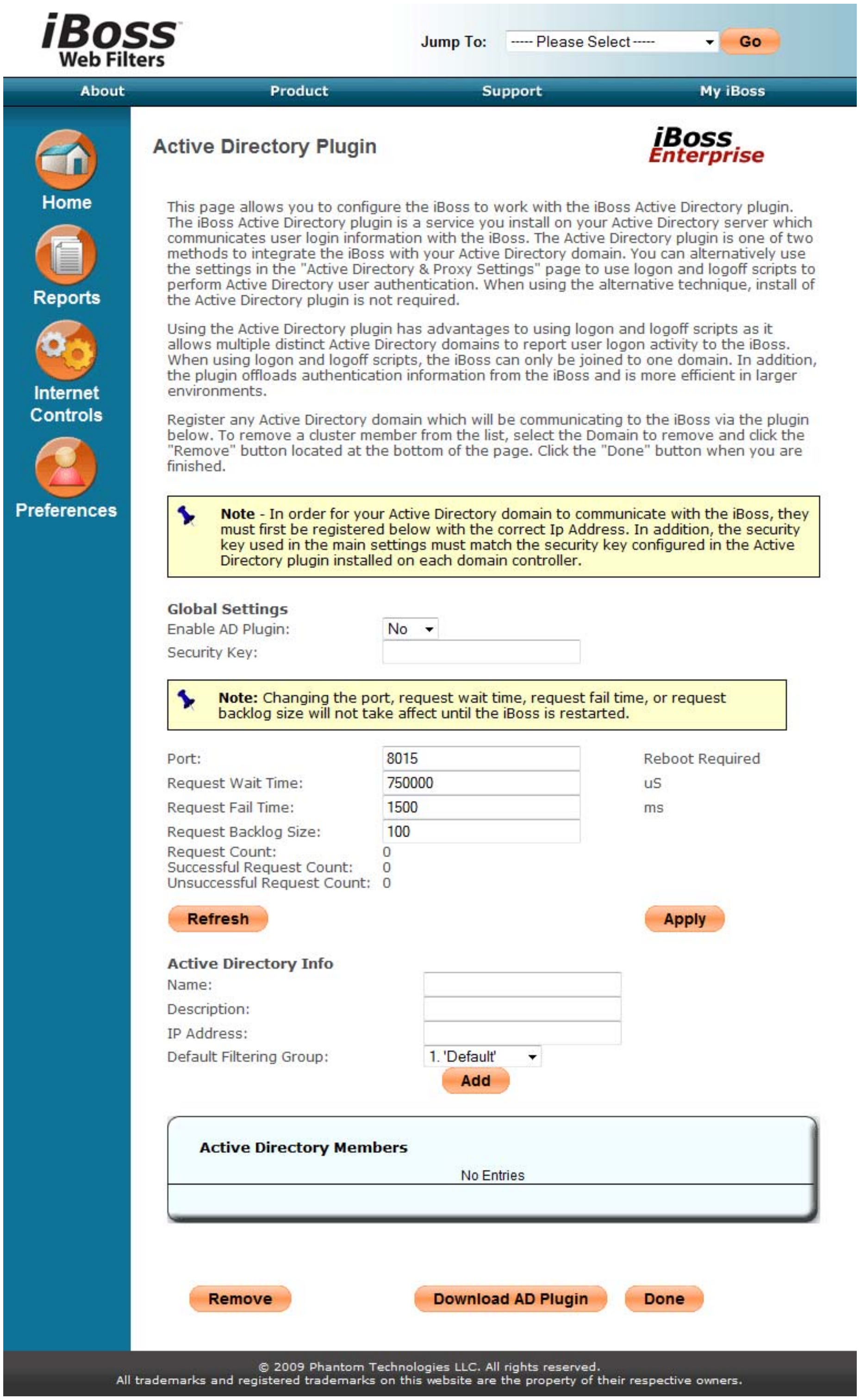


Note: You can auto-identify unknown computers based on the last known proxy user for that computer. Only computers that have had users access the iBoss through the proxy can be identified using this technique. You can re-attempt this periodically as more users will be identified as soon as they access the iBoss through the proxy.

To attempt to auto-identify unknown computers, click on the Auto-Identify button below:

Figure 15 - Automatic Identify of Unknown Computers

3.2.3.4 Active Directory Plugin



Active Directory Plugin

This page allows you to configure the iBoss to work with the iBoss Active Directory plugin. The iBoss Active Directory plugin is a service you install on your Active Directory server which communicates user login information with the iBoss. The Active Directory plugin is one of two methods to integrate the iBoss with your Active Directory domain. You can alternatively use the settings in the "Active Directory & Proxy Settings" page to use logon and logoff scripts to perform Active Directory user authentication. When using the alternative technique, install of the Active Directory plugin is not required.

Using the Active Directory plugin has advantages to using logon and logoff scripts as it allows multiple distinct Active Directory domains to report user logon activity to the iBoss. When using logon and logoff scripts, the iBoss can only be joined to one domain. In addition, the plugin offloads authentication information from the iBoss and is more efficient in larger environments.

Register any Active Directory domain which will be communicating to the iBoss via the plugin below. To remove a cluster member from the list, select the Domain to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note - In order for your Active Directory domain to communicate with the iBoss, they must first be registered below with the correct Ip Address. In addition, the security key used in the main settings must match the security key configured in the Active Directory plugin installed on each domain controller.

Global Settings

Enable AD Plugin: No

Security Key:

Note: Changing the port, request wait time, request fail time, or request backlog size will not take affect until the iBoss is restarted.

Port:	8015	Reboot Required
Request Wait Time:	750000	uS
Request Fail Time:	1500	ms
Request Backlog Size:	100	
Request Count:	0	
Successful Request Count:	0	
Unsuccessful Request Count:	0	

Active Directory Info

Name:

Description:

IP Address:

Default Filtering Group: 1. 'Default'

Active Directory Members

No Entries

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 16 - Active Directory Plugin

This feature allows you to configure the iBoss to work with the iBoss Active Directory plugin. The iBoss Active Directory plugin is a service you install on your Active Directory server which communicates user login information with the iBoss. The Active Directory plugin is one of two methods to integrate the iBoss with your Active Directory domain. You can alternatively use the settings in the "Active Directory & Proxy Settings" page to use logon and logoff scripts to perform Active Directory user authentication. When using the alternative technique, install of the Active Directory plugin is not required.

You may download the latest iBoss Active Directory Plugin at: www.ibosswebfilters.com/adplugin/adplugin.zip

Using the Active Directory plugin has advantages to using logon and logoff scripts as it allows multiple distinct Active Directory domains to report user logon activity to the iBoss. When using logon and logoff scripts, the iBoss can only be joined to one domain. In addition, the plugin offloads authentication information from the iBoss and is more efficient in larger environments.

Register any Active Directory domain which will be communicating to the iBoss via the plugin. To remove a cluster member from the list, select the Domain to remove and click the "**Remove**" button located at the bottom of the page. Click the "**Done**" button when you are finished.

Note: In order for your Active Directory domain to communicate with the iBoss, they must first be registered below with the correct Ip Address. In addition, the security key used in the main settings must match the security key configured in the Active Directory plugin installed on each domain controller.

Global Settings

Enable AD Plugin - Enable this option if you are going to be using the Active Directory Plugin
Security Key - This is the security key used to communicate with the domain controller and iBoss. They must match exactly.

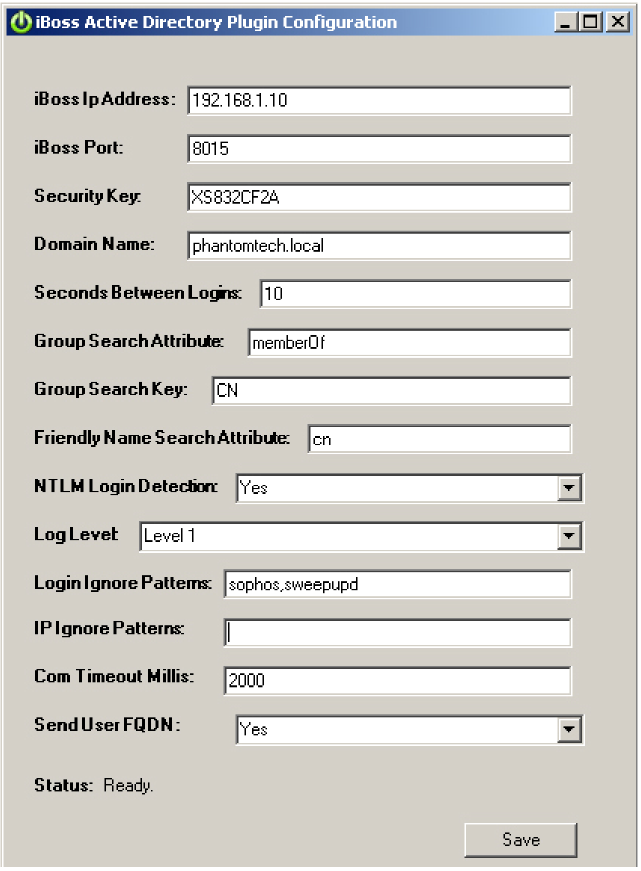
Note: Changing the port, request wait time, request fail time, or request backlog size will not take effect until the iBoss is restarted.

Port - This is the port number used for the active directory plugin. Default is 8015.
Request Wait Time - This is the Request Wait time for how long the Plugin will wait to respond to the iBoss.
Request Fail Time - This is the Request Fail time for how long until the request fails to the iBoss.
Request Backlog Size - This is the backlog size for requests that are waiting to process.
Request Count - Current Request Count
Successful Request Count - Current Successful Request Count
Unsuccessful Request Count - Current Unsuccessful Request Count

Active Directory Info

Name – This is for reference of which Active Directory server you are adding.
Description – A description can be added for reference.
IP Address – This is the IP address of the Active Directory server.
Default Filtering Group – This is the default filtering group for this active directory domain.
Once finished, click “Add” to add the Active Directory server.

3.2.3.4.1.1 iBoss Active Directory Plugin Configuration



iBoss Ip Address: 192.168.1.10
iBoss Port: 8015
Security Key: XS832CF2A
Domain Name: phantomtech.local
Seconds Between Logins: 10
Group Search Attribute: memberOf
Group Search Key: CN
Friendly Name Search Attribute: cn
NTLM Login Detection: Yes
Log Level: Level 1
Login Ignore Patterns: sophos,sweepupd
IP Ignore Patterns:
Com Timeout Millis: 2000
Send User FQDN: Yes
Status: Ready.

Figure 17 - iBoss Active Directory Plugin Configuration

This is the configuration of the iBoss Active Directory Plugin. Enter in the information for your iBoss. These settings work in conjunction with the Active Directory Plugin configuration within the iBoss interface.

iBoss IP Address – The IP address of the iBoss
iBoss Port – This is the port used for communication. Default is 8015.
Security Key – This is the key that matches in the iBoss Active Directory Plugin page.
Domain Name – This is the domain of the Active Directory Domain that the plugin is on.
Seconds Between Logins – This is the seconds between waiting on duplicate login requests.
Group Search Attribute – This attribute is for looking up group names. Default is **memberOf**.
Group Search Key – This is the field within Active Directory where group names are saved.
Friendly Name Search Attribute – This is the field that shows the friendly name of the users.
NTLM Login Detection – This will detect NTLM authentication when users log in.
Log Level – This is the amount of login information will be logged on the Domain Controller.
Login Ignore Patterns – These are ignore patterns that shouldn't log users in with.
IP Ignore Patterns – These are IP addresses that should be ignored.
Com Timeout Millis – This is the communication timeout in milliseconds.
Send User FQDN – This is the user Fully Qualified Domain Name. ex user@domain.local.

Once finished, click **Save** and close the window. Follow the next steps to audit logon events.

3.2.3.4.1.2 Active Directory Audit Logon Events

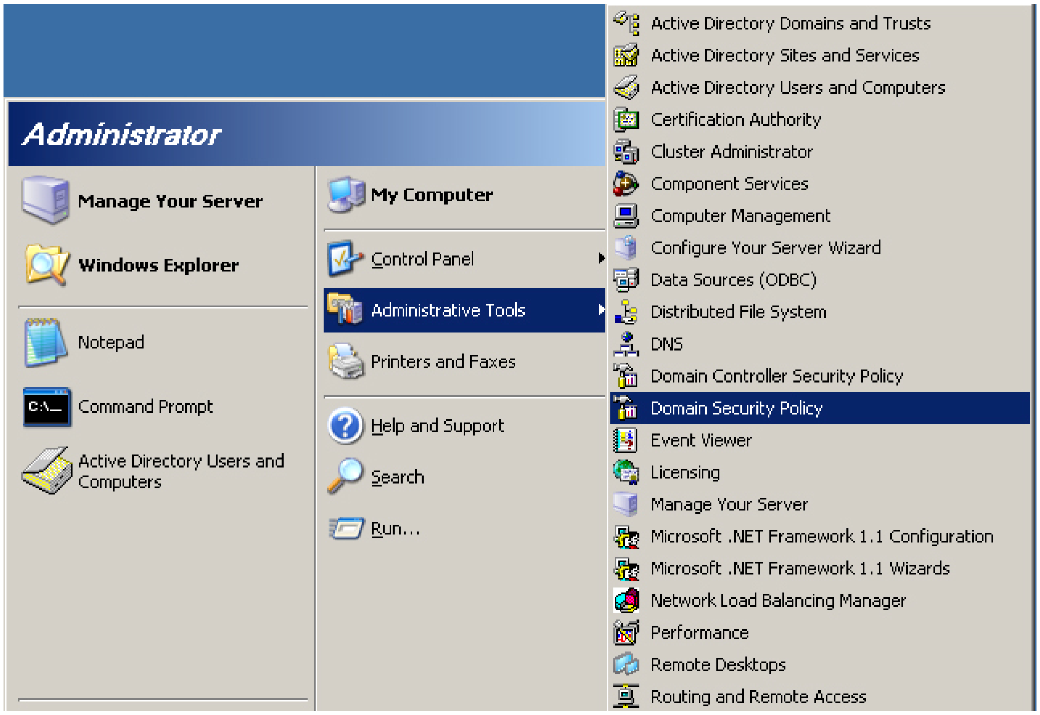
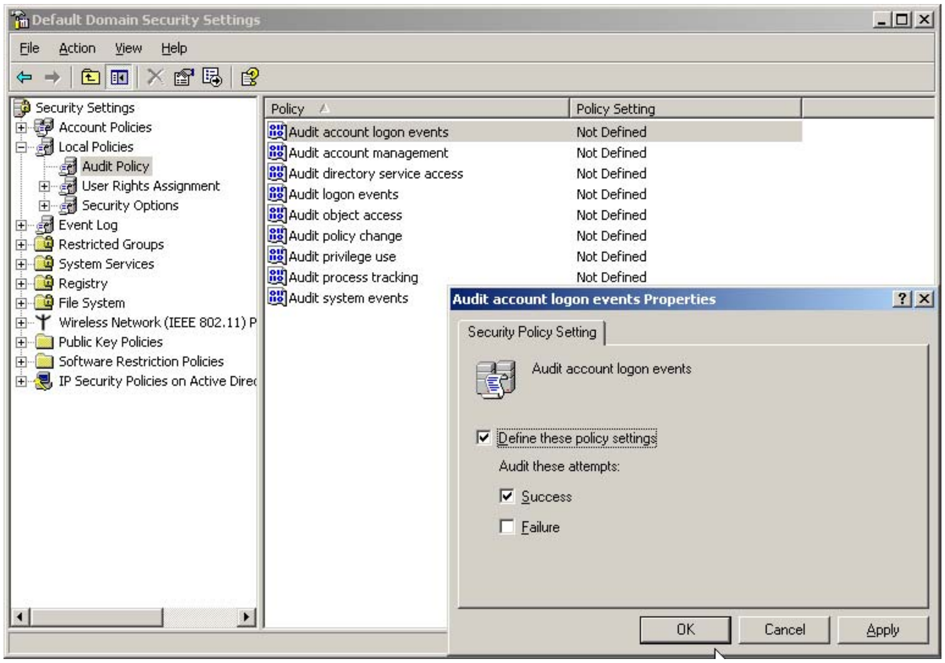


Figure 18 - Domain Security Policy

To ensure the Active Directory Plugin is working correctly, you will need to audit logon events. To do this, click on **Domain Security Policy** within your **Administrative Tools** as shown in the figure above.



Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	

Audit account logon events

☑ Define these policy settings

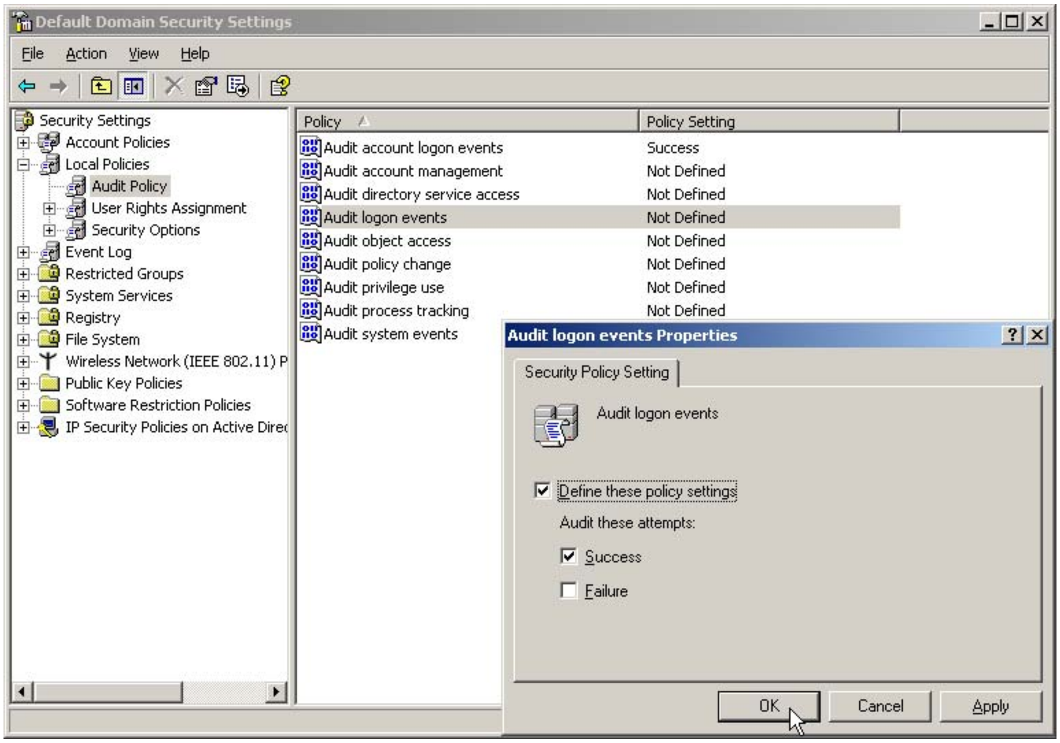
Audit these attempts:

☑ Success

☐ Failure

Figure 19 - Audit Account Logon Events

Expand under Security Settings → Local Policies → Audit Policy. Double click the first option **Audit account logon events** and make sure the checkbox for **Define these policy settings** and **Success** is checked and click **OK**.



Policy	Policy Setting
Audit account logon events	Success
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	

Audit logon events Properties

Security Policy Setting

Audit logon events

☑ Define these policy settings

Audit these attempts:

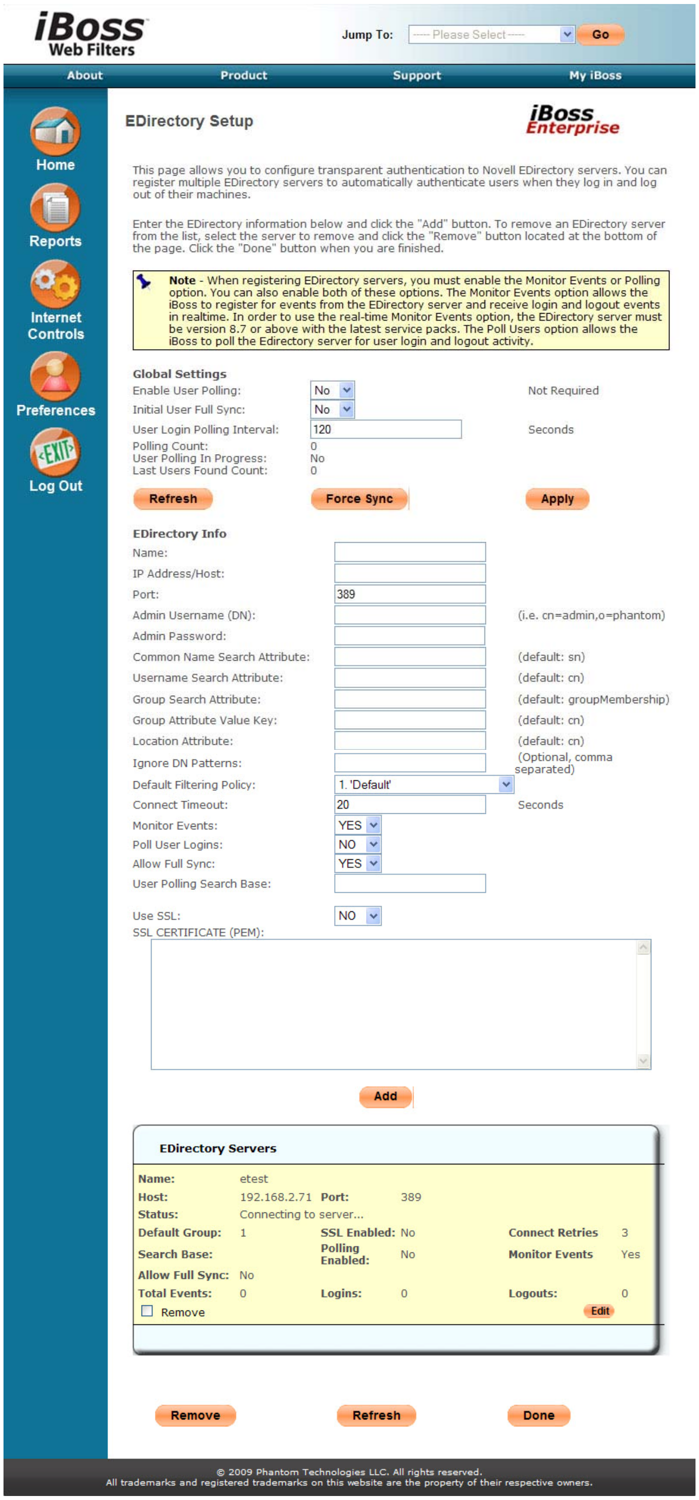
☑ Success

□ Failure

Figure 20 - Audit Logon Events

Next, double-click on **Audit logon events** (4th option down) and make sure the checkbox for **Define these policy settings** and **Success** is checked and click **OK**.

3.2.3.5 eDirectory Settings



EDirectory Setup

This page allows you to configure transparent authentication to Novell EDirectory servers. You can register multiple EDirectory servers to automatically authenticate users when they log in and log out of their machines.

Enter the EDirectory information below and click the "Add" button. To remove an EDirectory server from the list, select the server to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note - When registering EDirectory servers, you must enable the Monitor Events or Polling option. You can also enable both of these options. The Monitor Events option allows the iBoss to register for events from the EDirectory server and receive login and logout events in realtime. In order to use the real-time Monitor Events option, the EDirectory server must be version 8.7 or above with the latest service packs. The Poll Users option allows the iBoss to poll the Edirectory server for user login and logout activity.

Global Settings

Enable User Polling:	No	Not Required
Initial User Full Sync:	No	
User Login Polling Interval:	120	Seconds
Polling Count:	0	
User Polling In Progress:	No	
Last Users Found Count:	0	

EDirectory Info

Name:		
IP Address/Host:		
Port:	389	
Admin Username (DN):		(i.e. cn=admin,o=phantom)
Admin Password:		
Common Name Search Attribute:		(default: sn)
Username Search Attribute:		(default: cn)
Group Search Attribute:		(default: groupMembership)
Group Attribute Value Key:		(default: cn)
Location Attribute:		(default: cn)
Ignore DN Patterns:		(Optional, comma separated)
Default Filtering Policy:	1. 'Default'	
Connect Timeout:	20	Seconds
Monitor Events:	YES	
Poll User Logins:	NO	
Allow Full Sync:	YES	
User Polling Search Base:		
Use SSL:	NO	

SSL CERTIFICATE (PEM):

EDirectory Servers

Name:	etest				
Host:	192.168.2.71	**Port:**	389		
Status:	Connecting to server...				
Default Group:	1	**SSL Enabled:**	No	**Connect Retries**	3
Search Base:		**Polling Enabled:**	No	**Monitor Events**	Yes
Allow Full Sync:	No				
Total Events:	0	**Logins:**	0	**Logouts:**	0

□ Remove

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 21 - eDirectory Settings

3.2.3.6 iBoss eDirectory Transparent Integration

Overview

The iBoss Enterprise integrates natively with Novell eDirectory servers to provide seamless transparent authentication of users on the network. Integration with eDirectory allows administrators to manage policies based on a user's eDirectory group membership. In addition, integration unifies web filtering administration with an existing Novell eDirectory infrastructure.

Key Features

- Live Real-Time eDirectory event monitoring
- eDirectory user polling support
- Multiple simultaneous eDirectory monitoring support
- Compatible with Suse and Netware based eDirectory platforms
- Web policy enforcement based on eDirectory group membership

Getting Started

This section describes how to configure the iBoss to work within an eDirectory network infrastructure.

Overview

The iBoss can integrate with eDirectory with two different modes. Only one of the two modes are required and the end result is the same. The eDirectory version must be noted as not all modes are supported on older eDirectory firmware releases. Listed below are the two modes and their description:

Mode 1: eDirectory login/logout event monitoring

In this mode, the iBoss monitors login and logout events sent by the eDirectory server in real-time. As users login and logout of their workstations, eDirectory sends these events and iBoss uses them to associate the user with the workstation and apply dynamic filtering policy depending on which user is logged into the station. To use this mode, eDirectory 8.7 and above is required.

Mode 2: eDirectory user polling

In this mode, the iBoss polls the eDirectory server at the configured interval (usually every 2 minutes) for any users that have logged in within the last interval time. For example, if the polling interval is set to 2 minutes, the iBoss will query eDirectory for any users that have logged in within the last 2 minutes (repeating this every 2 minutes). Because this mode is not receiving events in real-time, user association to iBoss filtering group can take as long as the configured interval. This mode is supported across all eDirectory versions.

iBoss eDirectory Configuration

eDirectory configuration is performed via the menu option Home->Setup Network Connection->eDirectory Settings.

Global Settings

The global settings section contains configuration settings that apply across all registered eDirectory servers. The iBoss supports the registration of multiple eDirectory servers with independent settings and allows simultaneous monitoring of all registered servers. The global settings are general settings that apply to all servers.

Enable User Polling

This option specifies whether user polling should be used to process user logins from eDirectory. With polling, the iBoss will check for logins within a specified polling interval. If using eDirectory events, this option is not required and can be set to No.

Initial User Full Sync

This option specifies whether the iBoss should fully synchronize users from eDirectory with the iBoss after an iBoss reboot. This option is only available if user polling is enabled. When the iBoss is restarted, all users are disassociated and fall within the default filtering policy. With this option, iBoss will pull all users from the eDirectory tree after a reboot.

User Login Polling Interval

This is the interval at which iBoss will check for any new logon events from eDirectory. At this interval, iBoss will query the eDirectory tree for any new logon events that have occurred and associate the user with the eDirectory filtering policy. This option only applies when using eDirectory polling. When using eDirectory events, this option is not used.

User Polling In Progress

Indicates whether the iBoss is polling the eDirectory server for logged in users.

Last Users Found Count

Used to indicate how many new users the iBoss found during the last sync with eDirectory. Below the global settings, there is a “Force Sync” button which will cause the iBoss to immediately start pulling users from eDirectory and associating them with iBoss filtering policy. You can use this status count to determine how many users the iBoss found in eDirectory. You should click the “Refresh” button while performing a full synch to get updated status on this value.

eDirectory Info - Server Registration Settings

This section allows you to add and edit settings for individual eDirectory servers. Typically, you can add the top level master eDirectory replicas. However, if possible, it is recommended that all eDirectory servers to which users authenticate are registered in this section.

The following describes the settings within the eDirectory Info section used to register the eDirectory server.

Name

Use this setting to specify the server name. You can also use a friendly name for the server. This setting does not affect connection to the eDirectory server and is only used for your reference.

Ip Address/Host

The IP Address or host name of the eDirectory server.

Port

The port to which the iBoss will connect to the eDirectory server. Typically this is port 389 when ssl is not being used and 636 when SSL is being used.

Admin Username (DN)

The username that the iBoss will use to search the eDirectory server tree. This user must have search privileges. In addition, if event monitoring is being used, the user must have monitor event privileges set in eDirectory. Typically, a user with administrative privileges is used.

Admin Password

The password for the admin user specified above.

Common Name Search Attribute

The eDirectory LDAP attribute used to extract the full name of the user (First and Last Name).

Default: sn

Username Search Attribute

The eDirectory LDAP attribute used to extract the username for the logged in user.

Default: cn

Group Search Attribute

The LDAP attribute that the iBoss will use to match group membership. When the user is found in eDirectory, the iBoss will compare all groups specified in this attribute to the iBoss group names. When the iBoss finds a match, the iBoss will associate the user with that iBoss filtering group policy. If a user is part of more than 1 group that matches an iBoss group name, the iBoss will use the group with a lower group number (Group 1 match will override Group 3 match). Filtering group names can be found in Home->Identify Computers & Users->Groups Tab. Make sure to name the iBoss group exactly like the eDirectory group name that you would like to match.

Default: groupMembership

Group Attribute Value Key

When the group search attribute above is found (for example groupMembership), this value specifies the tokens that separate the group names. For example, using the default value of cn, the groupMembership LDAP attribute looks like cn=Staff,cn=Wireless User. With cn in this option, the groups that the iBoss would extract are Staff and Wireless User. It would then compare those to the iBoss groups.

Default: cn

Location Attribute

An optional LDAP attribute that can be used to specify the users location for generating reports. Typically this is left blank.

Ignore DN Pattern

The iBoss will ignore any user logins/logoffs that contain the patterns specified in this option. Any automated service accounts should be specified here. If they are not, whenever the service account (such as an antivirus account) logs into a computer that contains a logged in user, that username will override the logged in user. Eventually, it will appear as if the service account is the only user logged into the network. Enter these automated user accounts here so that whenever the iBoss receives a logon or logoff event from these users, it ignores them and preserves the currently logged in user. Values should be specified separated with a comma.

Default Filtering Policy

If the iBoss cannot find a matching iBoss group name to eDirectory group name, this specifies the default policy the iBoss should apply to the user.

Connect Timeout

This is the timeout (specified in seconds) that the iBoss should use when connecting to an eDirectory server. If an eDirectory server is down, this will prevent the iBoss from waiting too long before trying to connect again.

Default: 20

Monitor Events

Specifies whether eDirectory event polling should be used for this server. This is recommended as login and logout events will be sent in real-time to the iBoss.

Poll User Logins

Specifies whether the iBoss should use the polling method to poll the eDirectory server for login events. The settings specified in the global settings apply to this mode. This is typically set to No when Monitor Events is set to Yes as the iBoss will receive login/logout events in real-time.

Allow Full Sync

Specifies whether this server will participate in the full user synchronization triggered when “Force Full Sync” above is clicked. Typically, set this to “Yes” only for the master eDirectory replica as not all servers need to be queried during a full sync.

User Polling Search Base

This is the level in the eDirectory tree the iBoss should use to search for logged in users. When using “Force Full Sync” or enabling the option for “Poll User Logins”, this value is required. Typically this is set to the top of the tree (for example, o=iboss).

User SSL / SSL Certificate

This option specifies whether the iBoss should use SSL to connect to the eDirectory server. Typically SSL for eDirectory communicates via port 636 and this should be configured in Port Settings. When using SSL, paste your SSL certificate by extracting the contents of the certificate in PEM format. SSL is not required and involves more maintenance as you must monitor your certificates expiration dates to confirm that your certificates do not expire. If your certificate expires, the iBoss will no longer be able to communicate with the eDirectory server and the certificate will have to be updated. The default setting for use SSL is usually set to “No”

Add The Server

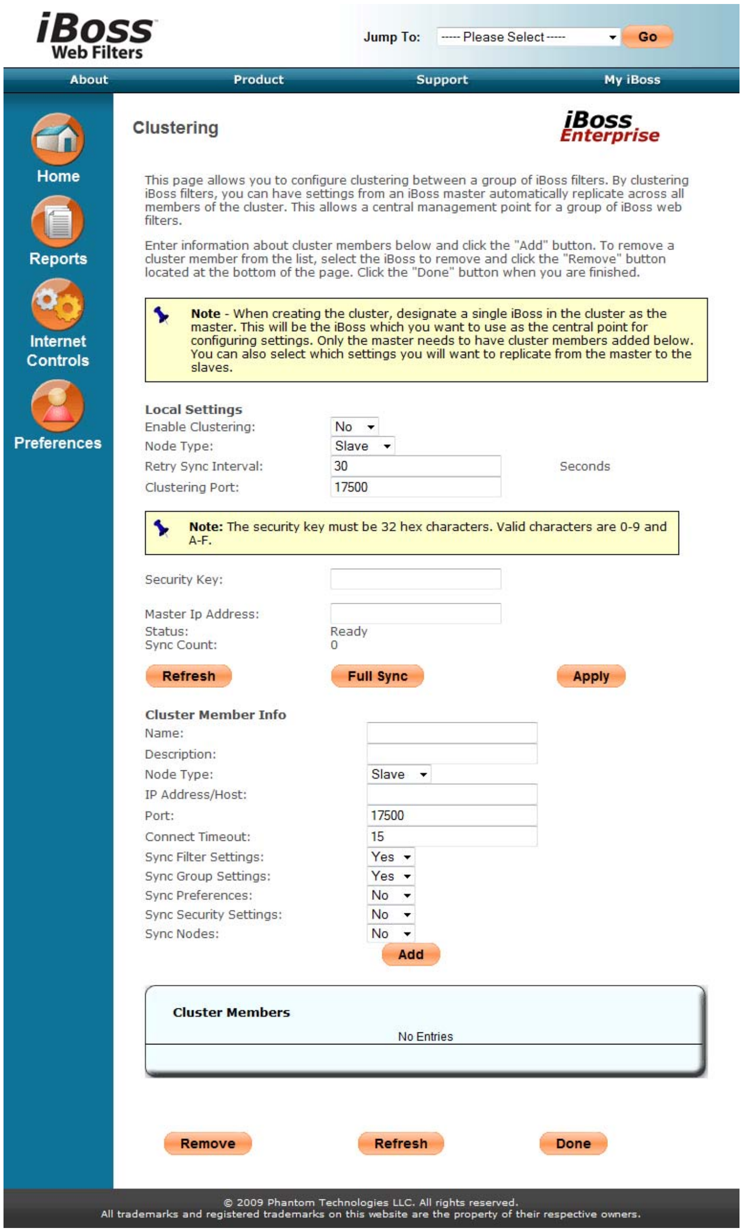
Once you have configured all of your settings, click the Add button to add the server to the registered eDirectory list.

You should refresh the page using the “Refresh” button after adding the server. This will update the “Status” field for the server that was just added to the list. You will want to confirm that the status is “Running…” for eDirectory servers registered to receive eDirectory events and no error is specified.

Conclusion

Once all of your eDirectory servers are registered, you can seamless manage policies within the iBoss and manage group membership in your eDirectory server. The iBoss will dynamically apply the appropriate policy whenever the user logs in using their eDirectory login credentials.

3.2.3.7 Clustering



Clustering

This page allows you to configure clustering between a group of iBoss filters. By clustering iBoss filters, you can have settings from an iBoss master automatically replicate across all members of the cluster. This allows a central management point for a group of iBoss web filters.

Enter information about cluster members below and click the "Add" button. To remove a cluster member from the list, select the iBoss to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note - When creating the cluster, designate a single iBoss in the cluster as the master. This will be the iBoss which you want to use as the central point for configuring settings. Only the master needs to have cluster members added below. You can also select which settings you will want to replicate from the master to the slaves.

Local Settings

Enable Clustering:	No	
Node Type:	Slave	
Retry Sync Interval:	30	Seconds
Clustering Port:	17500	

Note: The security key must be 32 hex characters. Valid characters are 0-9 and A-F.

Security Key:	
Master Ip Address:	
Status:	Ready
Sync Count:	0

Cluster Member Info

Name:	
Description:	
Node Type:	Slave
IP Address/Host:	
Port:	17500
Connect Timeout:	15
Sync Filter Settings:	Yes
Sync Group Settings:	Yes
Sync Preferences:	No
Sync Security Settings:	No
Sync Nodes:	No

Cluster Members

No Entries

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 22 – Clustering

This feature allows you to configure clustering between a group of iBoss filters. By clustering iBoss filters, you can have settings from an iBoss master automatically replicate across all members of the cluster. This allows a central management point for a group of iBoss web filters.

Enter information about cluster members in the required fields and click the "**Add**" button. To remove a cluster member from the list, select the iBoss to remove and click the "**Remove**" button located at the bottom of the page. Click the "**Done**" button when you are finished.

Note - When creating the cluster, designate a single iBoss in the cluster as the master. This will be the iBoss which you want to use as the central point for configuring settings. Only the master needs to have cluster members added below. You can also select which settings you will want to replicate from the master to the slaves.

Local Settings – These are local settings for the iBoss you are configuring.
Enable Clustering – This option turns on clustering globally.
Node Type – This field specifies the device node type whether it is a slave or master iBoss device.
Retry Sync Interval in Seconds – This field is the interval which the settings are synced.
Clustering Port – This field specifies the port used for syncing settings.
Note: The security key must be 32 hex characters. Valid characters are 0-9 and A-F.

Security Key – This field specifies the security key used when communicating with other clustered iBoss devices.
Master Ip Address – This field specifies the master iBoss IP address of the cluster.
Status – This is the status of the clustering with this device.
Sync Count – This is the number of the sync count.

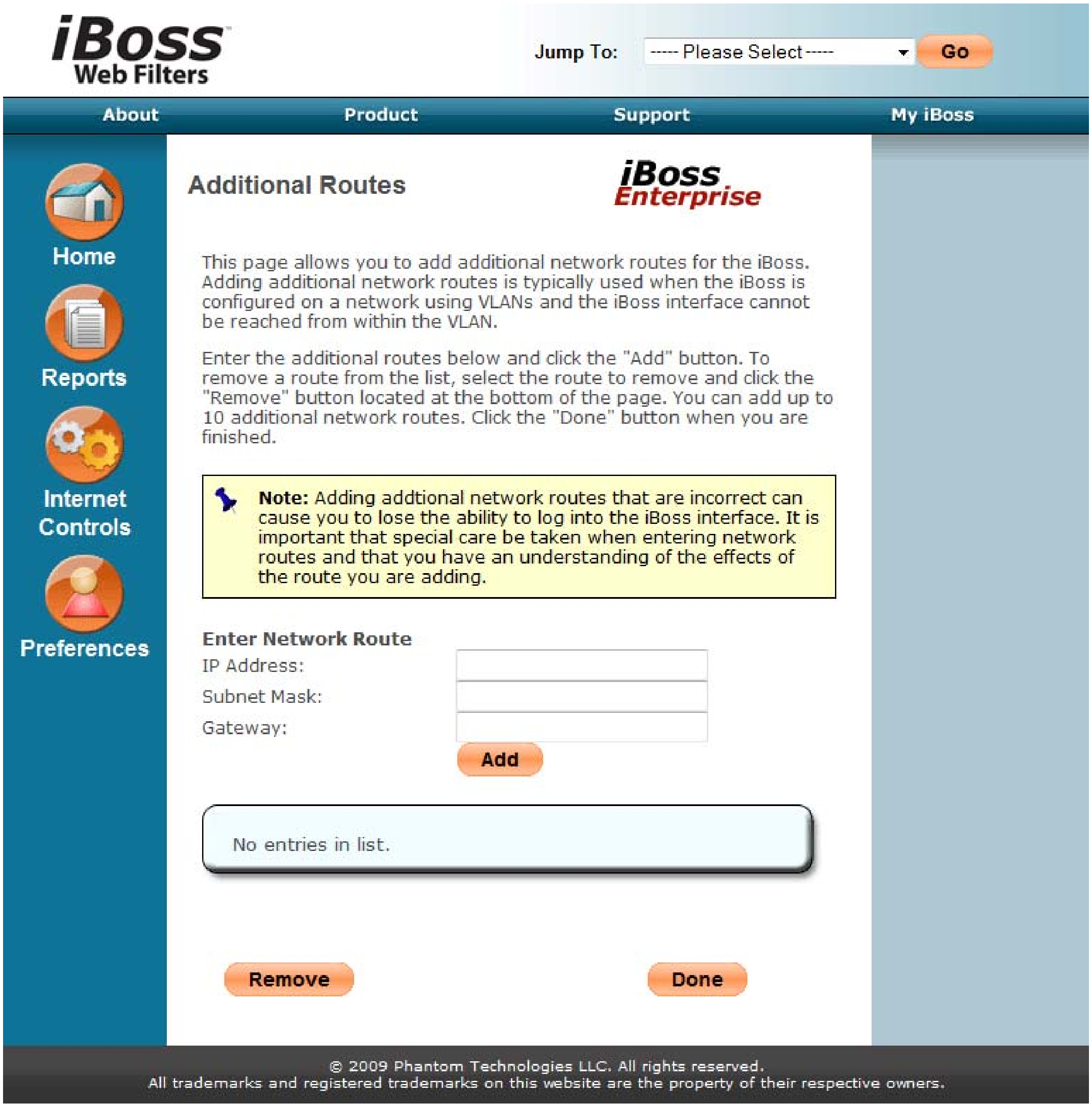
Once you have entered all required information click the "**Apply**" button.

The sync count should increase as the intervals are reached and settings are synced. To check current status, refresh the page to check the sync count by clicking the "**Refresh**" button. You can manually sync settings by clicking the "**Full Sync**" button.

Cluster Member Info – These are settings which you may add for each iBoss device you are adding to the cluster.
Name – This field is to put the name of the iBoss you are adding for reference.
Description – This is the description for the iBoss device you are adding.
Node Type – This field indicates whether this device is the master or slave.
IP Address/Host – This is the field for the IP of the iBoss you are adding.
Port – This is the port number that is used to communicate.
Connect Timeout – This is the timeout if the response is taking too long.
Sync Filter Settings – This is option to sync the filtering settings.
Sync Group Settings – This is option to sync the groups.
Sync Preferences - This is option to sync the preference settings.
Sync Security Settings - This is option to sync the security settings.
Sync Nodes - This is option to sync the computer nodes.

Once finished, click the "**Add**" button to add the iBoss cluster device.

3.2.3.8 Add Additional Routes



Additional Routes

This page allows you to add additional network routes for the iBoss. Adding additional network routes is typically used when the iBoss is configured on a network using VLANs and the iBoss interface cannot be reached from within the VLAN.

Enter the additional routes below and click the "Add" button. To remove a route from the list, select the route to remove and click the "Remove" button located at the bottom of the page. You can add up to 10 additional network routes. Click the "Done" button when you are finished.

Note: Adding addtional network routes that are incorrect can cause you to lose the ability to log into the iBoss interface. It is important that special care be taken when entering network routes and that you have an understanding of the effects of the route you are adding.

Enter Network Route

IP Address:

Subnet Mask:

Gateway:

No entries in list.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 23 - Add Additional Routes

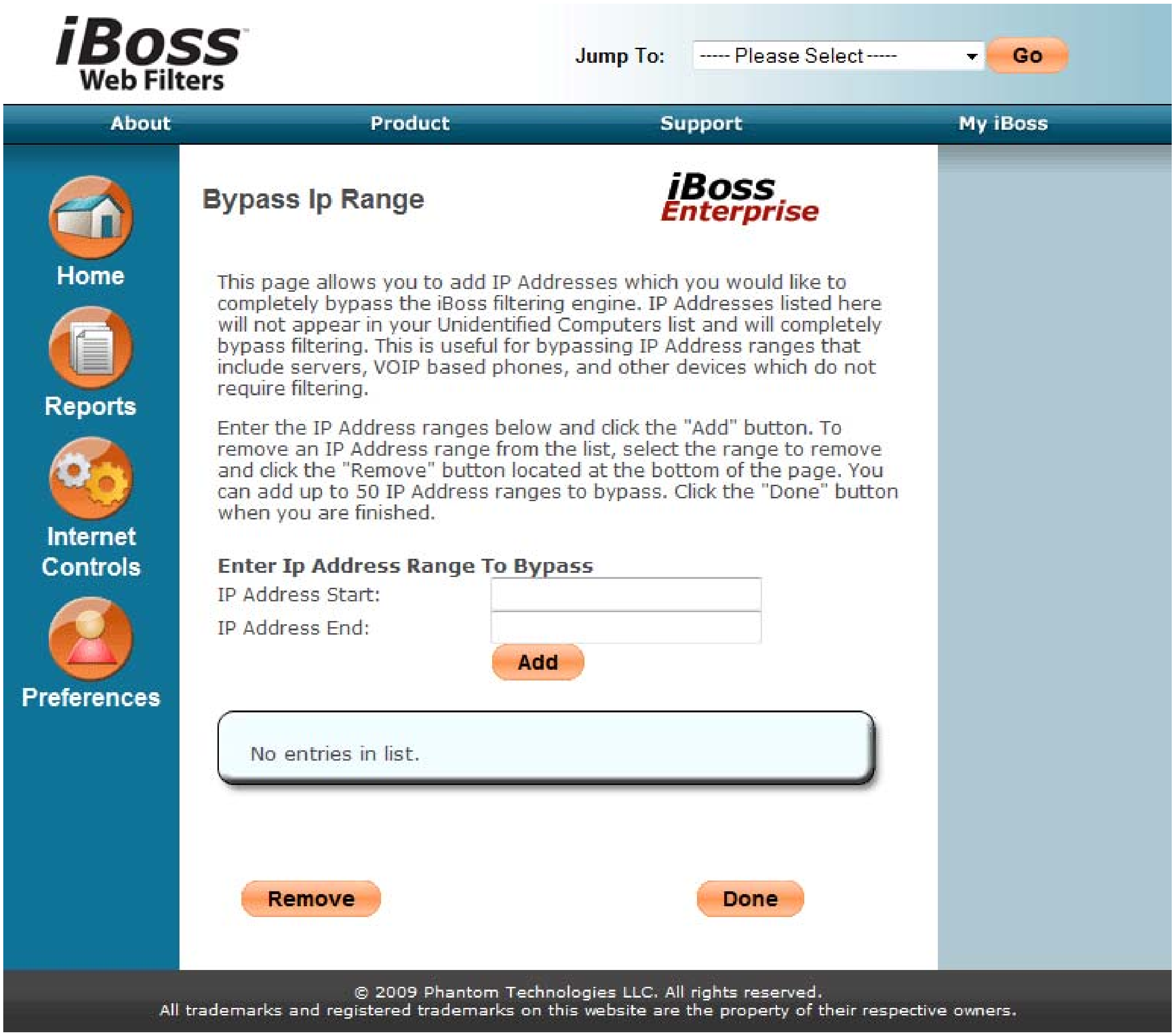
This page allows you to register gateways that are internal to your network (on the LAN side of the iBoss). Typically the iBoss is placed between a Layer 2 switch and the outter network Gateway/Firewall. If your network has any additional internal (non-NAT) gateways that are used to route internal local subnets, you can register those gateways here. The iBoss will automatically integrate with the internal gateways so that you may identify and apply filtering rules to computers behind the gateway.

The global settings apply to all internal gateways added. **You must enable internal gateway integration in the global settings below for any of the settings on this page to take affect.**
Enter the internal gateway below and click the "Add" button. To remove a gateway from the list, select the gateway to remove and click the "Remove" button located at the bottom of the page. You can add up to 1000 internal gateways. Click the "Done" button when you are finished.

Note - Do not add any gateways if your network is configured with a single outter gateway. Place the iBoss between the outter gateway/router and the internal switch to which all of the computers are connected.

If you register internal gateways on this page, you must add the subnet which is routed by this gateway on the "Additional Local Subnets" page. When adding the additional local subnet, make sure the option "Routed Through Gateway" is set to yes.

3.2.3.9 Bypass IP Ranges



Bypass Ip Range

This page allows you to add IP Addresses which you would like to completely bypass the iBoss filtering engine. IP Addresses listed here will not appear in your Unidentified Computers list and will completely bypass filtering. This is useful for bypassing IP Address ranges that include servers, VOIP based phones, and other devices which do not require filtering.

Enter the IP Address ranges below and click the "Add" button. To remove an IP Address range from the list, select the range to remove and click the "Remove" button located at the bottom of the page. You can add up to 50 IP Address ranges to bypass. Click the "Done" button when you are finished.

Enter Ip Address Range To Bypass

IP Address Start:

IP Address End:

No entries in list.

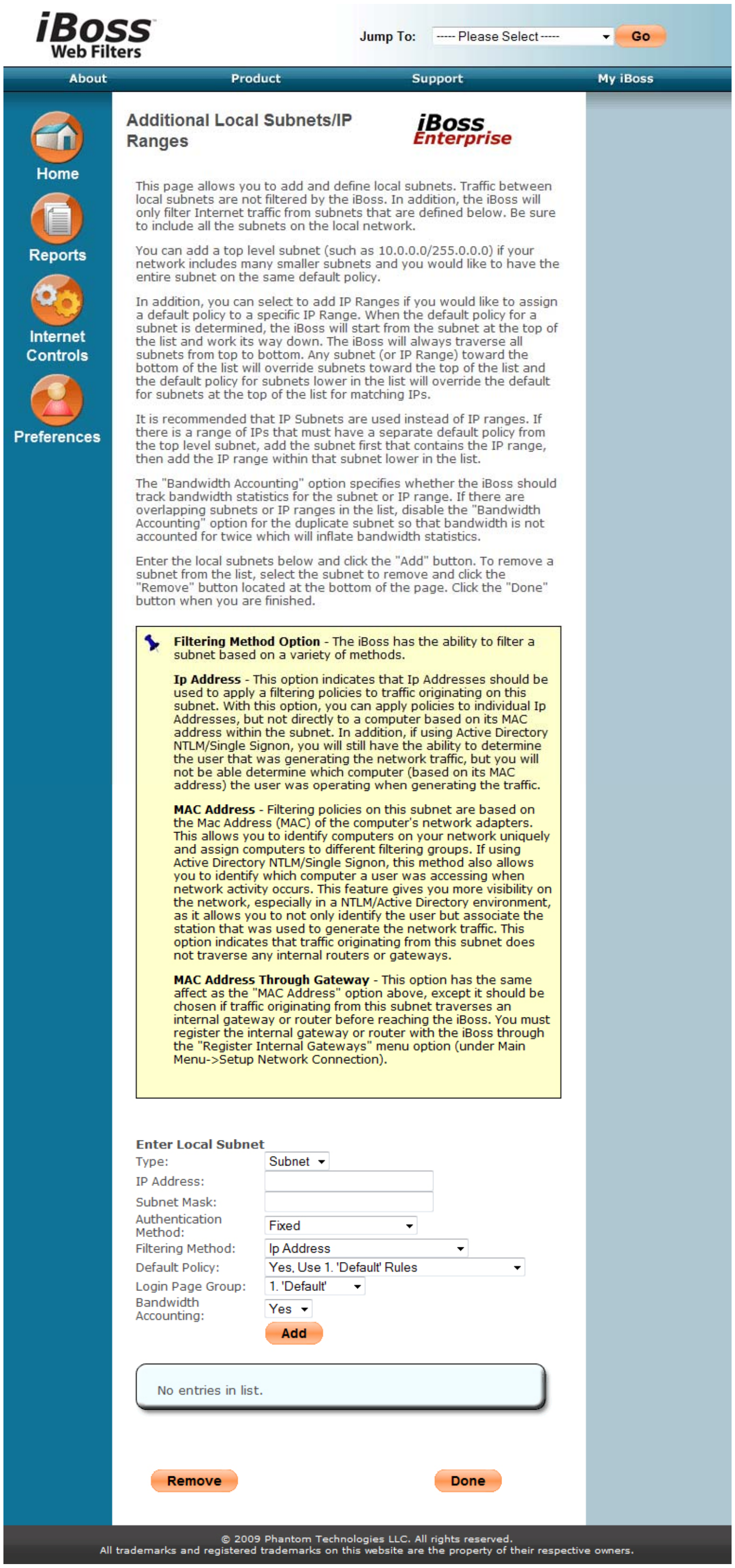
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 24 - Bypass IP Range

This page allows you to add IP Addresses which you would like to completely bypass the iBoss filtering engine. IP Addresses listed here will not appear in your Unidentified Computers list and will completely bypass filtering. This is useful for bypassing IP Address ranges that include servers, VOIP based phones, and other devices which do not require filtering.

Enter the IP Address ranges below and click the "**Add**" button. To remove an IP Address range from the list, select the range to remove and click the "Remove" button located at the bottom of the page. You can add up to 50 IP Address ranges to bypass. Click the "Done" button when you are finished.

3.2.3.10 Add Additional Local Subnets



Additional Local Subnets/IP Ranges

This page allows you to add and define local subnets. Traffic between local subnets are not filtered by the iBoss. In addition, the iBoss will only filter Internet traffic from subnets that are defined below. Be sure to include all the subnets on the local network.

You can add a top level subnet (such as 10.0.0.0/255.0.0.0) if your network includes many smaller subnets and you would like to have the entire subnet on the same default policy.

In addition, you can select to add IP Ranges if you would like to assign a default policy to a specific IP Range. When the default policy for a subnet is determined, the iBoss will start from the subnet at the top of the list and work its way down. The iBoss will always traverse all subnets from top to bottom. Any subnet (or IP Range) toward the bottom of the list will override subnets toward the top of the list and the default policy for subnets lower in the list will override the default for subnets at the top of the list for matching IPs.

It is recommended that IP Subnets are used instead of IP ranges. If there is a range of IPs that must have a separate default policy from the top level subnet, add the subnet first that contains the IP range, then add the IP range within that subnet lower in the list.

The "Bandwidth Accounting" option specifies whether the iBoss should track bandwidth statistics for the subnet or IP range. If there are overlapping subnets or IP ranges in the list, disable the "Bandwidth Accounting" option for the duplicate subnet so that bandwidth is not accounted for twice which will inflate bandwidth statistics.

Enter the local subnets below and click the "Add" button. To remove a subnet from the list, select the subnet to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Filtering Method Option - The iBoss has the ability to filter a subnet based on a variety of methods.

Ip Address - This option indicates that Ip Addresses should be used to apply a filtering policies to traffic originating on this subnet. With this option, you can apply policies to individual Ip Addresses, but not directly to a computer based on its MAC address within the subnet. In addition, if using Active Directory NTLM/Single Signon, you will still have the ability to determine the user that was generating the network traffic, but you will not be able determine which computer (based on its MAC address) the user was operating when generating the traffic.

MAC Address - Filtering policies on this subnet are based on the Mac Address (MAC) of the computer's network adapters. This allows you to identify computers on your network uniquely and assign computers to different filtering groups. If using Active Directory NTLM/Single Signon, this method also allows you to identify which computer a user was accessing when network activity occurs. This feature gives you more visibility on the network, especially in a NTLM/Active Directory environment, as it allows you to not only identify the user but associate the station that was used to generate the network traffic. This option indicates that traffic originating from this subnet does not traverse any internal routers or gateways.

MAC Address Through Gateway - This option has the same affect as the "MAC Address" option above, except it should be chosen if traffic originating from this subnet traverses an internal gateway or router before reaching the iBoss. You must register the internal gateway or router with the iBoss through the "Register Internal Gateways" menu option (under Main Menu->Setup Network Connection).

Enter Local Subnet

Type:	Subnet
IP Address:	
Subnet Mask:	
Authentication Method:	Fixed
Filtering Method:	Ip Address
Default Policy:	Yes, Use 1. 'Default' Rules
Login Page Group:	1. 'Default'
Bandwidth Accounting:	Yes

No entries in list.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 25 - Add Additional Local Subnets

This feature allows you to add and define local subnets. Traffic between local subnets are not filtered by the iBoss. In addition, the iBoss will only filter Internet traffic from subnets that are defined below. Be sure to include all the subnets on the local network.

You can add a top level subnet (such as 10.0.0.0/255.0.0.0) if your network includes many smaller subnets and you would like to have the entire subnet on the same default policy.

In addition, you can select to add IP Ranges if you would like to assign a default policy to a specific IP Range. When the default policy for a subnet is determined, the iBoss will start from the subnet at the top of the list and work its way down. The iBoss will always traverse all subnets from top to bottom. Any subnet (or IP Range) toward the bottom of the list will override subnets toward the top of the list and the default policy for subnets lower in the list will override the default for subnets at the top of the list for matching IPs.

It is recommended that IP Subnets are used instead of IP ranges. If there is a range of IPs that must have a separate default policy from the top level subnet, add the subnet first that contains the IP range, then add the IP range within that subnet lower in the list.

The "**Bandwidth Accounting**" option specifies whether the iBoss should track bandwidth statistics for the subnet or IP range. If there are overlapping subnets or IP ranges in the list, disable the "**Bandwidth Accounting**" option for the duplicate subnet so that bandwidth is not accounted for twice which will inflate bandwidth statistics.

Enter the local subnets and click the "**Add**" button. To remove a subnet from the list, select the subnet to remove and click the "**Remove**" button located at the bottom of the page. Click the "**Done**" button when you are finished.

Filtering Method Option - The iBoss has the ability to filter a subnet based on a variety of methods.

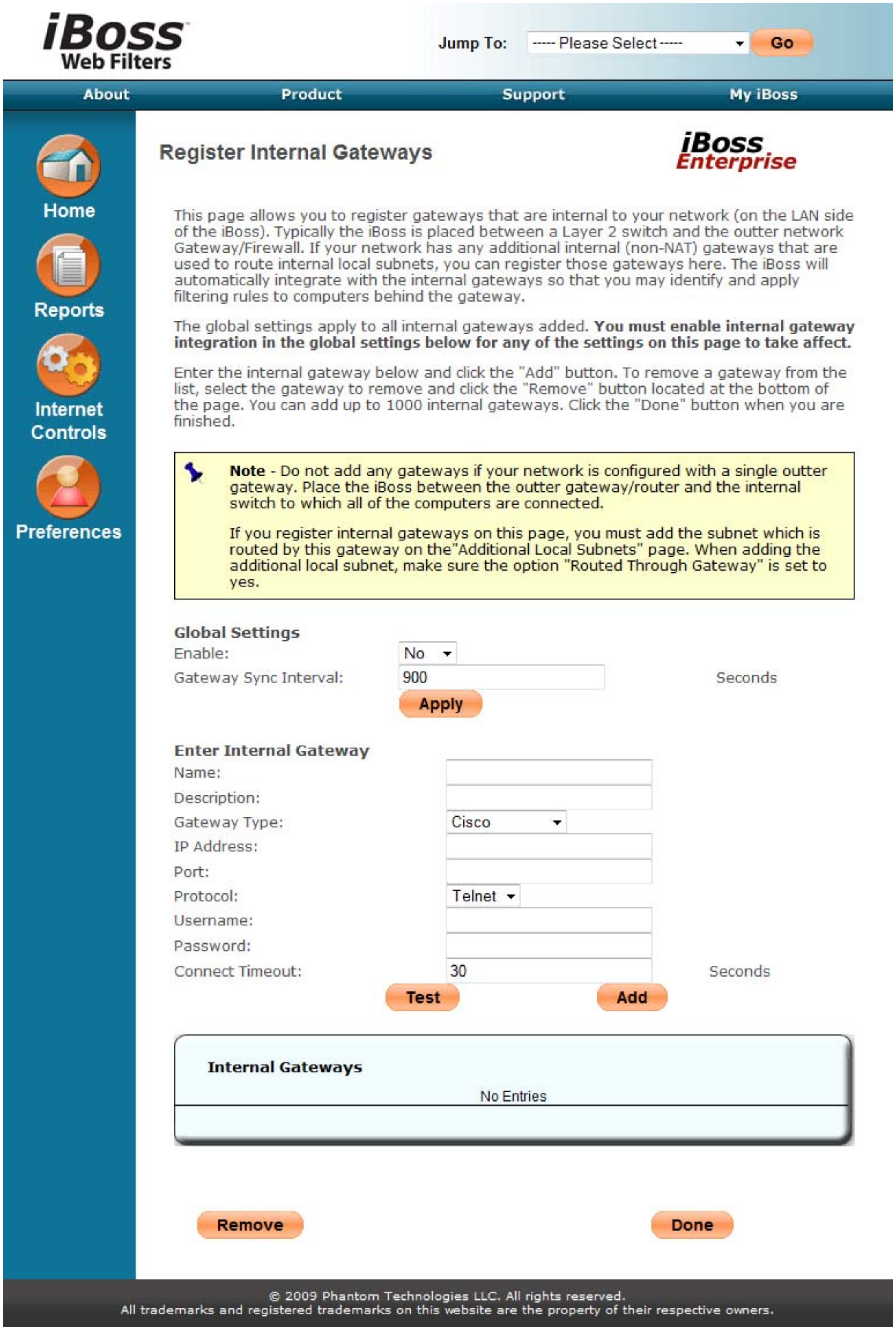
Ip Address - This option indicates that Ip Addresses should be used to apply a filtering policies to traffic originating on this subnet. With this option, you can apply policies to individual Ip Addresses, but not directly to a computer based on its MAC address within the subnet. In addition, if using Active Directory NTLM/Single Signon, you will still have the ability to determine the user that was generating the network traffic, but you will not be able determine which computer (based on its MAC address) the user was operating when generating the traffic.

MAC Address - Filtering policies on this subnet are based on the Mac Address (MAC) of the computer's network adapters. This allows you to identify computers on your network uniquely and assign computers to different filtering groups. If using Active Directory NTLM/Single Signon, this method also allows you to identify which computer a user was accessing when network activity occurs. This feature gives you more visibility on the network, especially in a NTLM/Active Directory environment, as it allows you to not only identify the user but associate the station that was used to generate the network traffic. This option indicates that traffic originating from this subnet does not traverse any internal routers or gateways.

MAC Address Through Gateway - This option has the same effect as the "MAC Address" option above, except it should be chosen if traffic originating from this subnet traverses an internal gateway or router before reaching the iBoss. You must register the internal gateway or router with the iBoss through the "Register Internal Gateways" menu option (under Main Menu->Setup Network Connection).

Enter Local Subnet – This is the section to add local subnet information.
Type – This is the option to choose whether it is a Range or Subnet.
IP Start (Range option) – This is the start IP address of the IP range you are adding.
IP End (Range option) – This is the end IP address of the IP range you are adding.
IP Address (Subnet option) – This is an IP address of the IP subnet you are adding; typically you enter the broadcast address.
Subnet Mask (Subnet option) – This is the subnet mask for the IP subnet you are adding.
Authentication Method – This is the option whether to authenticate with fixed filtering or NTLM with Active Directory.
Filtering Method – This is the option to choose whether this IP range or subnet are filtered and identified by IP address, Mac Address, or Mac Address through an internal gateway.
Default Policy – This is the default filtering policy for the IP range or subnet you are adding.
Login Page Group – This is the Login group page for user login used for the IP range or subnet you are adding.
Bandwidth Accounting – This option is to choose whether to account for bandwidth for the IP range or subnet you are adding.

3.2.3.11 Register Internal Gateways



Register Internal Gateways

This page allows you to register gateways that are internal to your network (on the LAN side of the iBoss). Typically the iBoss is placed between a Layer 2 switch and the outter network Gateway/Firewall. If your network has any additional internal (non-NAT) gateways that are used to route internal local subnets, you can register those gateways here. The iBoss will automatically integrate with the internal gateways so that you may identify and apply filtering rules to computers behind the gateway.

The global settings apply to all internal gateways added. **You must enable internal gateway integration in the global settings below for any of the settings on this page to take affect.**

Enter the internal gateway below and click the "Add" button. To remove a gateway from the list, select the gateway to remove and click the "Remove" button located at the bottom of the page. You can add up to 1000 internal gateways. Click the "Done" button when you are finished.

Note - Do not add any gateways if your network is configured with a single outter gateway. Place the iBoss between the outter gateway/router and the internal switch to which all of the computers are connected.

If you register internal gateways on this page, you must add the subnet which is routed by this gateway on the"Additional Local Subnets" page. When adding the additional local subnet, make sure the option "Routed Through Gateway" is set to yes.

Global Settings

Enable:	No	
Gateway Sync Interval:	900	Seconds

Apply

Enter Internal Gateway

Name:		
Description:		
Gateway Type:	Cisco	
IP Address:		
Port:		
Protocol:	Telnet	
Username:		
Password:		
Connect Timeout:	30	Seconds

Test Add

Internal Gateways

No Entries

Remove Done

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 26 - Register Internal Gateways

This page allows you to register gateways that are internal to your network (on the LAN side of the iBoss). Typically the iBoss is placed between a Layer 2 switch and the outter network Gateway/Firewall. If your network has any additional internal (non-NAT) gateways that are used to route internal local subnets, you can register those gateways here. The iBoss will automatically integrate with the internal gateways so that you may identify and apply filtering rules to computers behind the gateway.

The global settings apply to all internal gateways added. **You must enable internal gateway integration in the global settings below for any of the settings on this page to take effect.**

Enter the internal gateway below and click the "Add" button. To remove a gateway from the list, select the gateway to remove and click the "Remove" button located at the bottom of the page. You can add up to 1000 internal gateways. Click the "Done" button when you are finished.

Note - Do not add any gateways if your network is configured with a single outter gateway. Place the iBoss between the outter gateway/router and the internal switch to which all of the computers are connected.
If you register internal gateways on this page, you must add the subnet which is routed by this gateway on the"Additional Local Subnets" page. When adding the additional local subnet, make sure the option "Routed Through Gateway" is set to yes.

Global Settings – These are the global settings for adding an Internal Gateway.
Enable – This is the option to globally turn on this feature.
Gateway Sync Interval – This is the sync interval with the gateways that are adding in seconds.

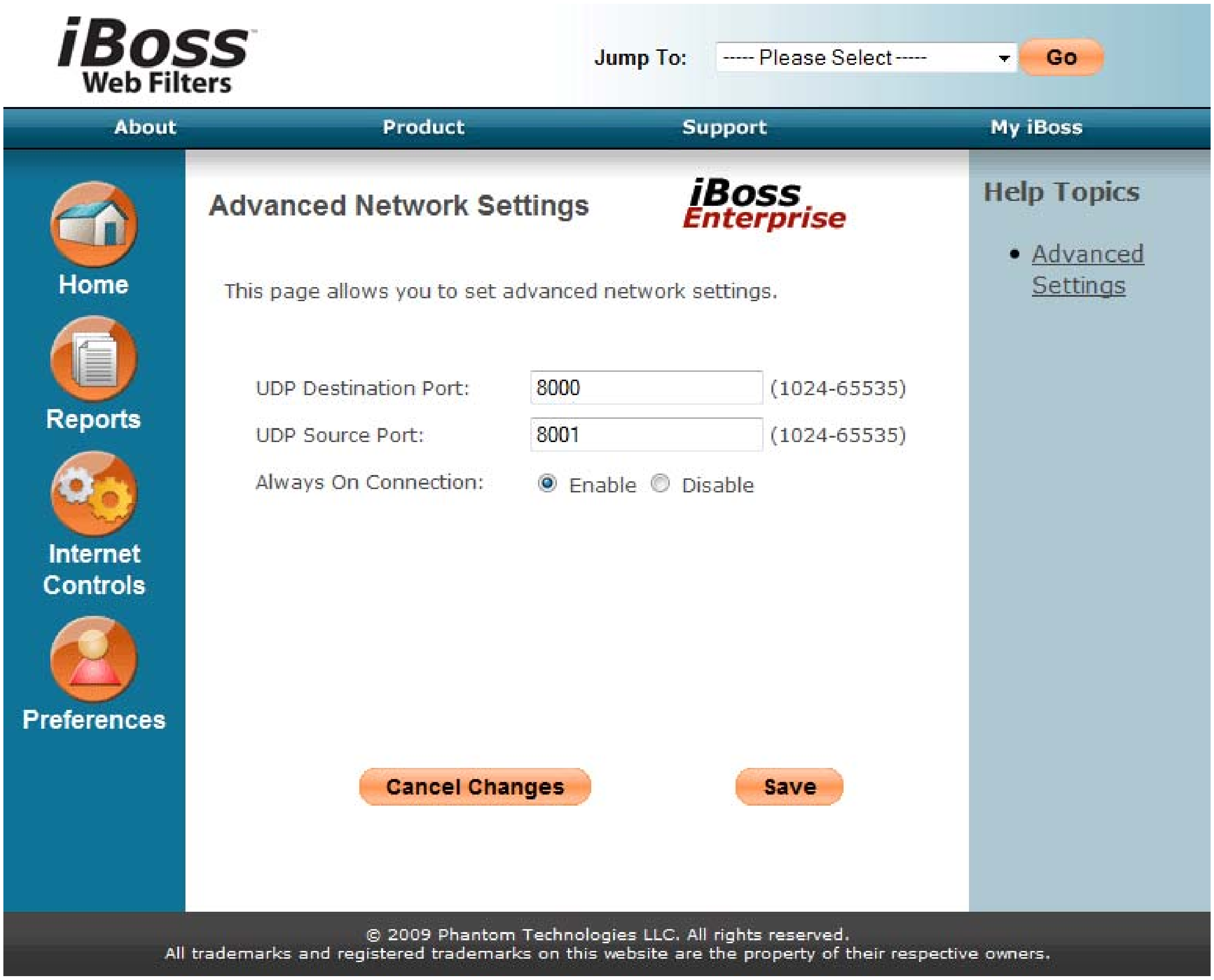
Once you have changed any of these options, click the “**Apply**” button.

Enter Internal Gateway – These are the individual gateway settings.
Name – This is the name for reference for the gateway you are adding.
Description – This is the field to add a description for the gateway you are adding.
Gateway Type – This is the gateway type. Options are **Cisco, HP Switch, Linux, Cisco FWSM, Dlink Switch.**
IP Address – This is the IP address for the internal gateway you are adding.
Port – This is the port used for communication, typically it is port 23 for telnet communication or port 22 for SSH communication.
Protocol – This is the option to choose whether communication is through telnet or SSH.
Username – This is the username to log into the internal gateway.
Password - This is the password to log into the internal gateway.
Connect Timeout – This is the connection timeout if no response is received specified in seconds.

Once you have finished adding these settings click the “**Add**” button. It will add it to the Internal Gateways list. To test these settings click the “**Edit**” button next to the entry and it will populate the fields again that you have entered. Next, click the “Test” button to test this entry.

To remove an entry click the “**Remove**” button next to the gateway entry. Once you are finished, click the **“Done**” button.

3.2.3.12 Edit Advanced Network Settings


iBoss Web Filters
Jump To: ----- Please Select ----- Go
About
Product
Support
My iBoss
Home
Reports
Internet Controls
Preferences
iBoss Enterprise
Help Topics
Advanced Settings
Cancel Changes
Save
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Advanced Network Settings

This page allows you to set advanced network settings.

UDP Destination Port: 8000 (1024-65535)

UDP Source Port: 8001 (1024-65535)

Always On Connection: ● Enable ○ Disable

Figure 27 - Edit Advanced Network Settings

The iBoss connects to the Phantom servers via UDP. You may select which ports it connects through. The default destination port is 8000 and default source port is 8001.

Always On Connection - This option allows you to still have Internet access even if it loses connection with our servers. This function will work after the first time that it has established a connection.

3.3 Installing the iBoss on the Network

Once the network settings have been configured, the iBoss is ready to be installed on the network. The two ports you will be using are the “LAN” port and the “WAN” port located on the iBoss.

Place the iBoss between an existing switch on the network and an existing firewall. For example, if the network has a switch to which computers are connected to, and that switch is connected to the network firewall, the iBoss will be placed between the switch and the firewall.

Disconnect the switch from the firewall and connect the switch to the “LAN” port on the iBoss. Connect the firewall to the “WAN” port on the iBoss.

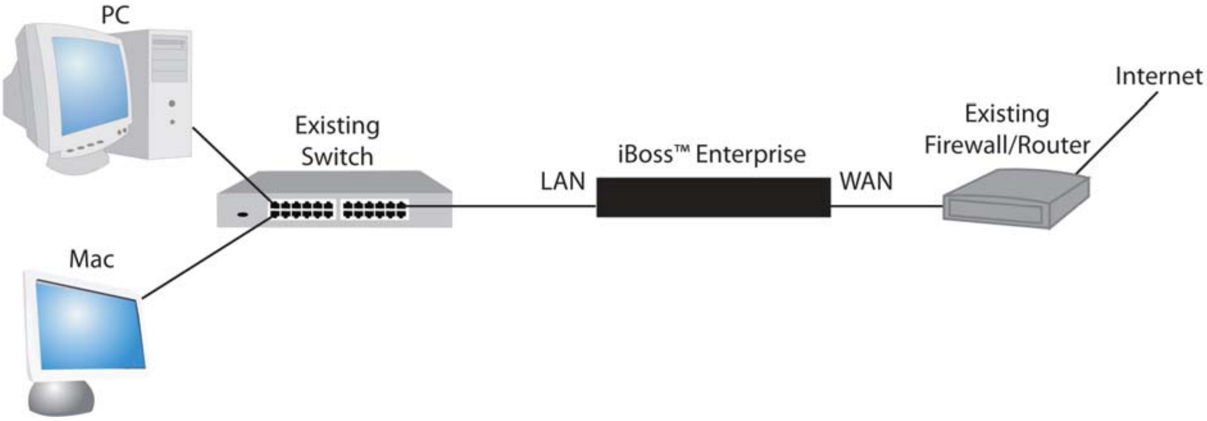


Figure 28 - iBoss Hardware Installation

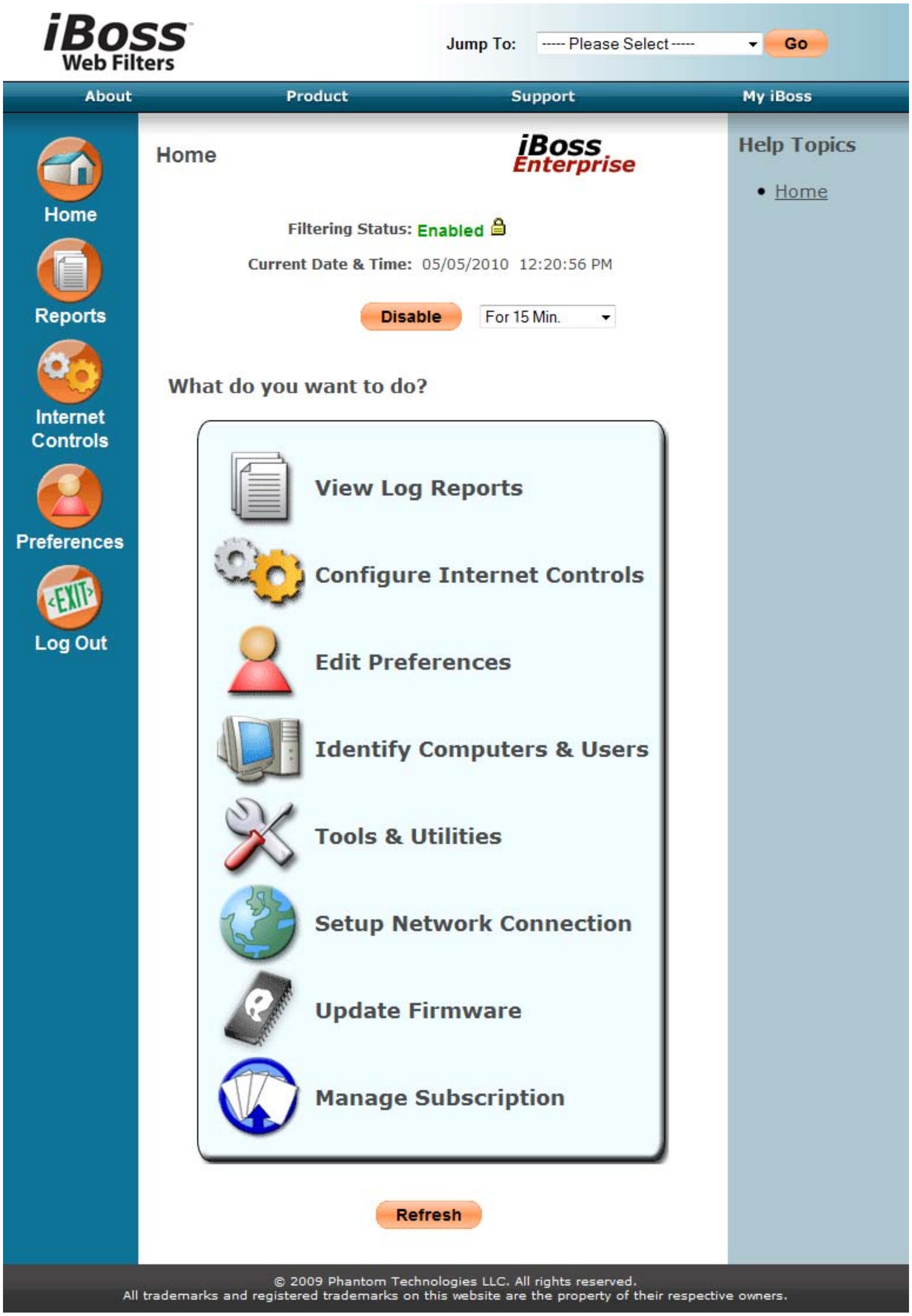
This completes the physical installation of the iBoss on your network. You can access the iBoss interface from any computer on the local network by opening a Web Browser and typing the IP address of the iBoss into your Web Browser’s address bar.

3.3.1 Additional Setup Steps and Notes

After setting up the iBoss, there are some steps you will need to do. We recommend adding IP addresses to the bypass range for any servers or IP addresses that you do not want filtered. For example, any DNS servers or VoIP phones.

4 INTERFACE

4.1 Home Page



Home

Filtering Status: Enabled

Current Date & Time: 05/05/2010 12:20:56 PM

What do you want to do?

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 29 - Home Page

4.1.1 Filtering Status

This indicates the filtering status of your iBoss. The following values may be displayed:

Enabled - Indicates that your iBoss is Enabled and Active.

Disabled - Indicates that your iBoss is not enabled.

Connecting - When the iBoss is enabled, it must first establish a connection to the gateway. This indicates that the iBoss is attempting to establish a connection.

Must Activate or Subscription Expired - If you have a new iBoss and need to activate your subscription, or if your iBoss subscription has expired, the "Activate" button will appear next to the filtering status field. Click the "Activate" button to proceed with your iBoss activation.

Current Date & Time - Indicates the current date and time. The date and time are synchronized when the iBoss establishes a connection to the gateway, and are important for performing Internet scheduling and report logging. The local time zone settings may be set from the "Edit My Time Zone" page under "My Preferences".

Note: The date & time will only be displayed when the iBoss status is "Enabled".

Enable/Disable Button - The "Enable/Disable" button is located next to the Filtering Status field. It is useful for quickly enabling and disabling your iBoss filtering. If your status reads "Not Enabled", clicking the "Enable" button will enabled the iBoss filtering. You may also choose to Disable for time periods such as 15 Min, 30 Min, 1 Hour, 2 Hours, 12 Hours, 24 Hours or Until Re-enabled.

4.1.2 Main Menu

The "**Home**" menu allows you to choose options for configuring the current iBoss settings. There are eight options to choose from: **View Log Reports, Configure Internet Controls, Edit My Preferences, Identify Computers & Users, Tools & Utilities, Setup Network Connection, Update Firmware** and **Manage Subscription.**

View Log Reports - This option allows you to view your iBoss report logs.

Configure Internet Controls - This option allows you to configure different iBoss filtering controls.

Edit My Preferences - This option allows you to edit preferences including E-mail options, password, time zone and custom block messages.

Identify Computers & Users - This option allows you to identify computers and individual user login on your network for computer specific management control.

Tools & Utilities - This option allows you to configure use utilities for quick lookups or backup & restore options.

Setup Network Connection - This option allows you to configure your iBoss network settings.

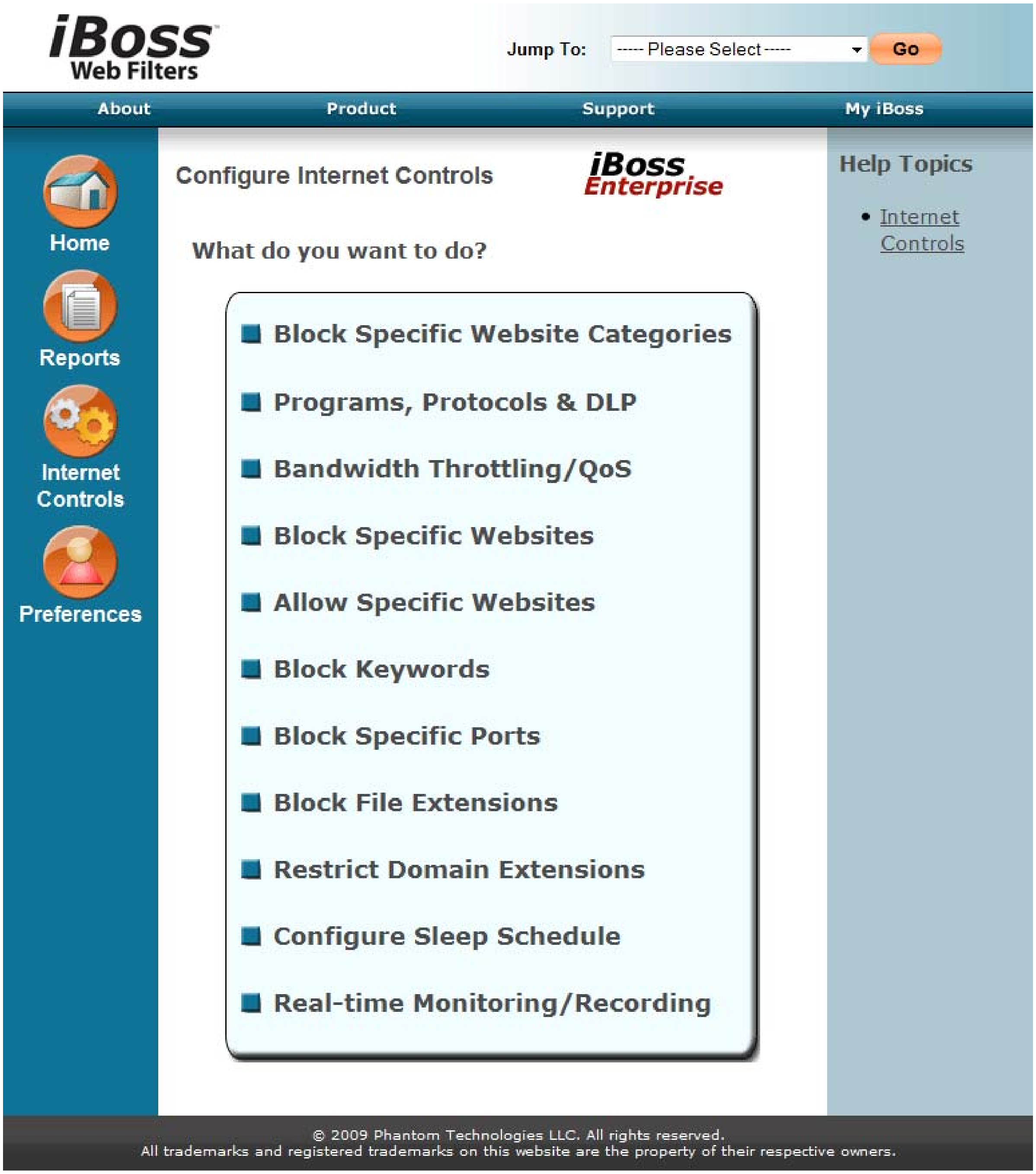
Update Firmware - This option allows you to update the firmware for your iBoss whenever updates are available.

Manage Subscription - This option allows you to update the subscription for your iBoss.

4.1.3 Shortcut Bar

Use this shortcut bar to quickly navigate through the iBoss interface. The shortcut bar has 4 options to choose: Home, Reports, Internet Controls, and My Preferences. Once you set a password for the iBoss, a Logout button will also appear.

4.2 Configure Internet Controls



iBoss Web Filters
Jump To: ----- Please Select ----- Go
About
Product
Support
My iBoss
Home
Reports
Internet Controls
Preferences
iBoss Enterprise
Help Topics
Internet Controls
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Configure Internet Controls

What do you want to do?

- Block Specific Website Categories
- Programs, Protocols & DLP
- Bandwidth Throttling/QoS
- Block Specific Websites
- Allow Specific Websites
- Block Keywords
- Block Specific Ports
- Block File Extensions
- Restrict Domain Extensions
- Configure Sleep Schedule
- Real-time Monitoring/Recording

Figure 30 - Configure Internet Controls

The "**Configure Internet Controls**" menu lets you choose options for configuring the current iBoss Internet controls. These are the options to choose from: Block Specific Website Categories, Programs, Protocols & DLP, Bandwidth Throttling/QoS, Block Specific Websites, Allows Specific Websites, Block Keywords, Block Specific Ports, Block File Extensions, Restrict Domain Extensions, Configure Sleep Schedule, and Real-time Monitoring /Recording.

Block Specific Website Categories - This option allows you to block or allow website content based on categories.

Programs, Protocols & DLP - This option allows you to configure access to web applications that the iBoss can manage. You may choose to block Chat (Instant messenger) programs, File Sharing programs, FTP & other protocols for Data Leakage Protection (DLP).

Bandwidth Throttling/QoS - This option allows you to set bandwidth throttles on users, groups, domains, or web categories.

Block Specific Websites - This option allows you to block access to specific websites by adding them to the Block List.

Allow Specific Websites - This option allows you to permit access to specific websites by adding them to the Allow List.

Block Specific Keywords - This option allows you to block specific keywords from searches or full URL's by adding them to the Keyword list.

Block Specific Ports - This option allows you to block specific ports or port ranges with Protocol and Direction.

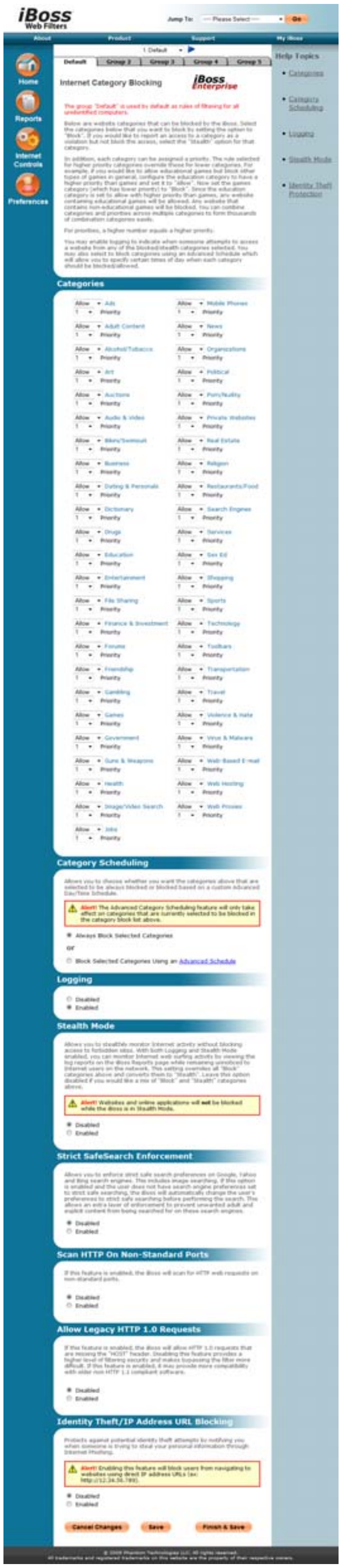
Block File Extensions - This option allows you to block specific file extensions from being downloaded on your network.

Restrict Domain Extensions - This option allows you to block or allow specific domain extensions from being accessed.

Configure Sleep Schedule - This option allows you to schedule access to the Internet on a schedule.

Real-time Monitoring/Recording - This option allows you to set notification alerts for real-time monitoring and recording thresholds.

4.2.1 Block Specific Website Categories



Internet Category Blocking

The group "Default" is used by default as rules of filtering for all unidentified computers.

Below are website categories that can be blocked by the iBoss. Select the categories below that you want to block by setting the option to "Block". If you would like to report an access to a category as a violation but not block the access, select the "Stealth" option for that category.

In addition, each category can be assigned a priority. The rule selected for higher priority categories override those for lower categories. For example, if you would like to allow educational games but block other types of games in general, configure the education category to have a higher priority than games and set it to "Allow". Now set the games category (which has lower priority) to "Block". Since the education category is set to allow with higher priority than games, any website containing educational games will be allowed. Any website that contains non-educational games will be blocked. You can combine categories and priorities across multiple categories to form thousands of combination categories easily.

For priorities, a higher number equals a higher priority.

You may enable logging to indicate when someone attempts to access a website from any of the blocked/stealth categories selected. You may also select to block categories using an advanced schedule which will allow you to specify certain times of day when each category should be blocked/allowed.

Categories

Allow ▾ Ads 1 ▾ Priority	Allow ▾ Mobile Phones 1 ▾ Priority
Allow ▾ Adult Content 1 ▾ Priority	Allow ▾ News 1 ▾ Priority
Allow ▾ Alcohol/Tobacco 1 ▾ Priority	Allow ▾ Organizations 1 ▾ Priority
Allow ▾ Art 1 ▾ Priority	Allow ▾ Political 1 ▾ Priority
Allow ▾ Auctions 1 ▾ Priority	Allow ▾ Porn/Nudity 1 ▾ Priority
Allow ▾ Audio & Video 1 ▾ Priority	Allow ▾ Private Websites 1 ▾ Priority
Allow ▾ Bikini/Swimsuit 1 ▾ Priority	Allow ▾ Real Estate 1 ▾ Priority
Allow ▾ Business 1 ▾ Priority	Allow ▾ Religion 1 ▾ Priority
Allow ▾ Dating & Personals 1 ▾ Priority	Allow ▾ Restaurants/Food 1 ▾ Priority
Allow ▾ Dictionary 1 ▾ Priority	Allow ▾ Search Engines 1 ▾ Priority
Allow ▾ Drugs 1 ▾ Priority	Allow ▾ Services 1 ▾ Priority
Allow ▾ Education 1 ▾ Priority	Allow ▾ Sex Ed 1 ▾ Priority
Allow ▾ Entertainment 1 ▾ Priority	Allow ▾ Shopping 1 ▾ Priority
Allow ▾ File Sharing 1 ▾ Priority	Allow ▾ Sports 1 ▾ Priority
Allow ▾ Finance & Investment 1 ▾ Priority	Allow ▾ Technology 1 ▾ Priority
Allow ▾ Forums 1 ▾ Priority	Allow ▾ Toolbars 1 ▾ Priority
Allow ▾ Friendship 1 ▾ Priority	Allow ▾ Transportation 1 ▾ Priority
Allow ▾ Gambling 1 ▾ Priority	Allow ▾ Travel 1 ▾ Priority
Allow ▾ Games 1 ▾ Priority	Allow ▾ Violence & Hate 1 ▾ Priority
Allow ▾ Government 1 ▾ Priority	Allow ▾ Virus & Malware 1 ▾ Priority
Allow ▾ Guns & Weapons 1 ▾ Priority	Allow ▾ Web Based E-mail 1 ▾ Priority
Allow ▾ Health 1 ▾ Priority	Allow ▾ Web Hosting 1 ▾ Priority
Allow ▾ Image/Video Search 1 ▾ Priority	Allow ▾ Web Proxies 1 ▾ Priority
Allow ▾ Jobs 1 ▾ Priority	

Category Scheduling

Allows you to choose whether you want the categories above that are selected to be always blocked or blocked based on a custom Advanced Day/Time Schedule.

⚠ Alert! The Advanced Category Scheduling feature will only take effect on categories that are currently selected to be blocked in the category block list above.

● Always Block Selected Categories

or

○ Block Selected Categories Using an Advanced Schedule

Logging

○ Disabled
● Enabled

Stealth Mode

Allows you to stealthily monitor Internet activity without blocking access to forbidden sites. With both Logging and Stealth Mode enabled, you can monitor Internet web surfing activity by viewing the log reports on the iBoss Reports page while remaining unnoticed to Internet users on the network. This setting overrides all "Block" categories above and converts them to "Stealth". Leave this option disabled if you would like a mix of "Block" and "Stealth" categories above.

⚠ Alert! Websites and online applications will **not** be blocked while the iBoss is in Stealth Mode.

● Disabled
○ Enabled

Strict SafeSearch Enforcement

Allows you to enforce strict safe search preferences on Google, Yahoo and Bing search engines. This includes image searching. If this option is enabled and the user does not have search engine preferences set to strict safe searching, the iBoss will automatically change the user's preferences to strict safe searching before performing the search. This allows an extra layer of enforcement to prevent unwanted adult and explicit content from being searched for on these search engines.

● Disabled
○ Enabled

Scan HTTP On Non-Standard Ports

If this feature is enabled, the iBoss will scan for HTTP web requests on non-standard ports.

● Disabled
○ Enabled

Allow Legacy HTTP 1.0 Requests

If this feature is enabled, the iBoss will allow HTTP 1.0 requests that are missing the "HOST" header. Disabling this feature provides a higher level of filtering security and makes bypassing the filter more difficult. If this feature is enabled, it may provide more compatibility with older non HTTP 1.1 compliant software.

● Disabled
○ Enabled

Identity Theft/IP Address URL Blocking

Protects against potential identity theft attempts by notifying you when someone is trying to steal your personal information through Internet Phishing.

⚠ Alert! Enabling this feature will block users from navigating to websites using direct IP address URLs (ex: http://12.34.56.789).

● Disabled
○ Enabled

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 31 - Block Specific Website Categories

The "Internet Category Blocking" page allows you to configure the current iBoss Internet website category blocking settings, log settings, Stealth Mode, and Identity Theft Detection options.

Categories - These are categories from which Internet websites are grouped. You may choose categories from this list that you wish to block on your network. In addition to blocking access to these website categories, the iBoss will also log attempted access violations if logging is enabled.
Examples of website categories are:

Ads
Adult Content
Alcohol/Tobacco
Art
Auctions
Audio & Video
Bikini/Swimsuit
Business
Dating & Personals
Dictionary
Drugs
Education
Entertainment
File Sharing
Finance & Investment
Forums
Friendship
Gambling
Games
Government
Guns & Weapons
Health
Image/Video Search
Jobs
Mobile Phones
News
Organizations
Political
Porn/Nudity
Private Websites
Real Estate
Religion
Restaurants/Food
Search Engines
Services
Sex Ed
Shopping
Sports
Technology
Toolbars
Transportation
Travel
Violence & Hate
Virus & Malware
Web-Based E-mail
Web Hosting
Web Proxies

Category Scheduling - Allows you to choose whether you want the categories above that are selected to be always blocked or blocked based on a custom Advanced Day/Time Schedule.

Note: The Advanced Category Scheduling feature will only take effect on categories that are currently selected to be blocked in the category block list above.

Logging - Allows you to enable and disable logging of violation attempts for the current set of blocked website categories. Log reports may be viewed on the iBoss Reports page. The report information includes date, time, user, website address, and category of the violation.

Stealth Mode - Allows you to stealthily monitor Internet activity without blocking access to forbidden sites. With both Logging and Stealth Mode enabled, you can monitor Internet web surfing activity by viewing the log reports on the iBoss Reports page while remaining unnoticed to Internet users on the network.

Note: Websites and online applications will not be blocked while the iBoss is in "Stealth Mode".

Strict SafeSearch Enforcement - Allows you to enforce strict safe search on the Google and Yahoo search engines. This includes image searching. If this option is enabled and the user does not have search engine preferences set to strict safe searching, the search will be blocked. This allows an extra layer of enforcement to prevent unwanted adult and explicit content from being search on these search engines.

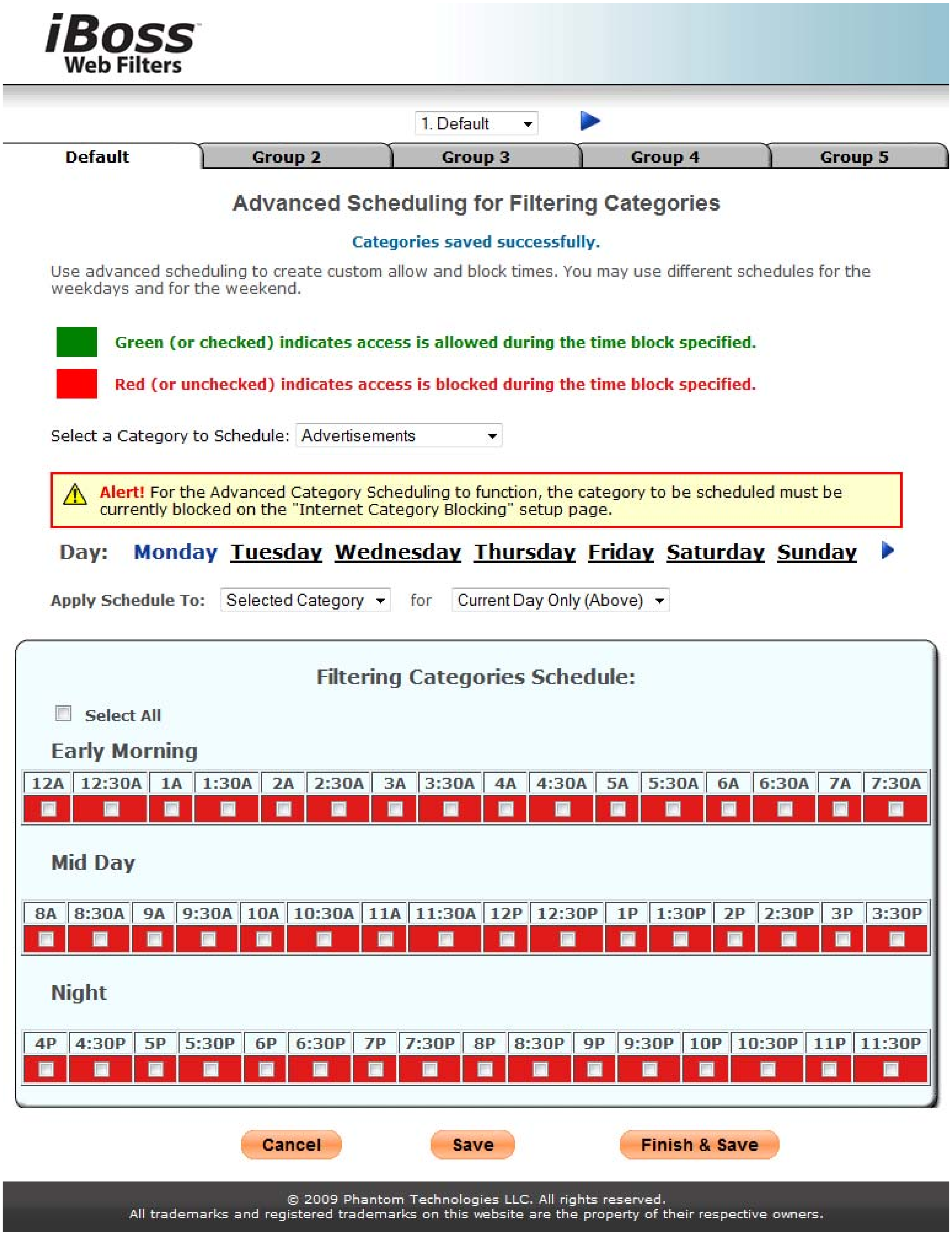
This setting only applies to Yahoo and Google search engines. For Yahoo, the search preference for "SafeSearch" Filter must be set to "Filter out adult Web, video, and image search results" if this option is enabled. For Google, the SafeSearch filtering preference must be set to "Use strict filtering (Filter both explicit text and explicit images)" when this option is enabled.

Scan HTTP On Non-Standard Ports - If this feature is enabled, the iBoss will scan for HTTP web requests on non-standard ports.

Allow Legacy HTTP 1.0 Requests - If this feature is enabled, the iBoss will allow HTTP 1.0 requests that are missing the "HOST" header. Disabling this feature provides a higher level of filtering security and makes bypassing the filter more difficult. If this feature is enabled, it may provide more compatibility with older non HTTP 1.1 compliant software.

Identity Theft (Phishing) / IP Address URL Blocking - Protects against potential identity theft attempts by notifying you when someone is trying to steal your personal information through Internet Phishing. Enabling this feature will also block users from navigating to websites using IP address URL's.

4.2.1.1 Advanced Scheduling



Advanced Scheduling for Filtering Categories

Categories saved successfully.

Use advanced scheduling to create custom allow and block times. You may use different schedules for the weekdays and for the weekend.

🟩 Green (or checked) indicates access is allowed during the time block specified.

🟥 Red (or unchecked) indicates access is blocked during the time block specified.

Select a Category to Schedule: Advertisements

⚠ **Alert!** For the Advanced Category Scheduling to function, the category to be scheduled must be currently blocked on the "Internet Category Blocking" setup page.

Day: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Apply Schedule To: Selected Category for Current Day Only (Above)

Filtering Categories Schedule:

□ Select All

Early Morning

12A	12:30A	1A	1:30A	2A	2:30A	3A	3:30A	4A	4:30A	5A	5:30A	6A	6:30A	7A	7:30A
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Mid Day

8A	8:30A	9A	9:30A	10A	10:30A	11A	11:30A	12P	12:30P	1P	1:30P	2P	2:30P	3P	3:30P
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Night

4P	4:30P	5P	5:30P	6P	6:30P	7P	7:30P	8P	8:30P	9P	9:30P	10P	10:30P	11P	11:30P
□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Figure 32 - Advanced Scheduling

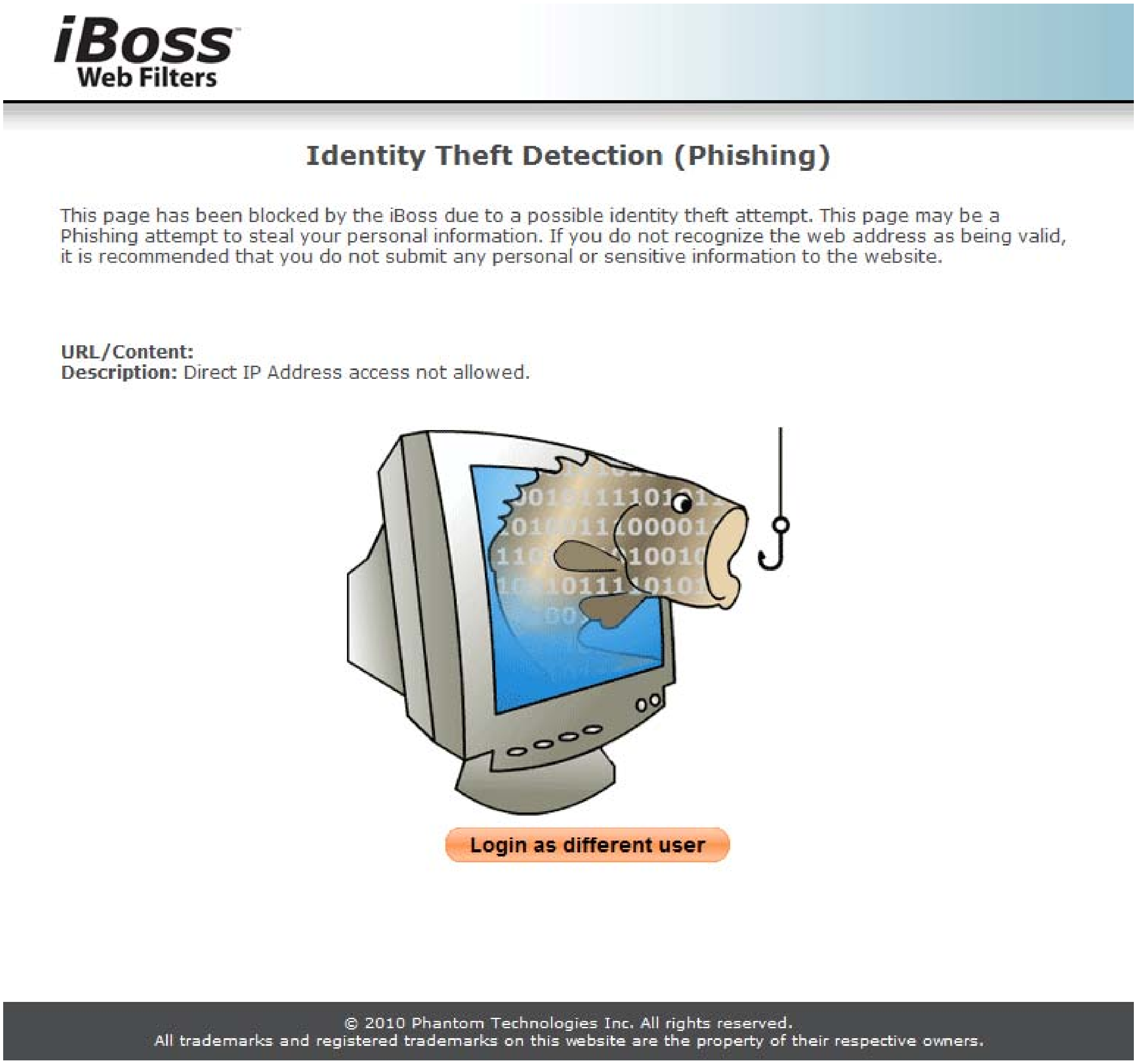
You may use advanced scheduling to create custom allow and block times for Filtering Categories, Web Programs, and the Sleep Schedule. You may use different schedules for the different days of the week, simply select the day and set the schedule. For Filtering Categories you will have to select a Category to Schedule:

Green (or checked) indicates access is allowed during the time block specified.

Red (or unchecked) indicates access is blocked during the time block specified.

Note: For the Advanced Category Scheduling to function, the category to be scheduled must be currently blocked on the "**Internet Category Blocking**" setup page.

4.2.1.2 Identify Theft (Phishing)/ IP Address Blocking Page



Identity Theft Detection (Phishing)

This page has been blocked by the iBoss due to a possible identity theft attempt. This page may be a Phishing attempt to steal your personal information. If you do not recognize the web address as being valid, it is recommended that you do not submit any personal or sensitive information to the website.

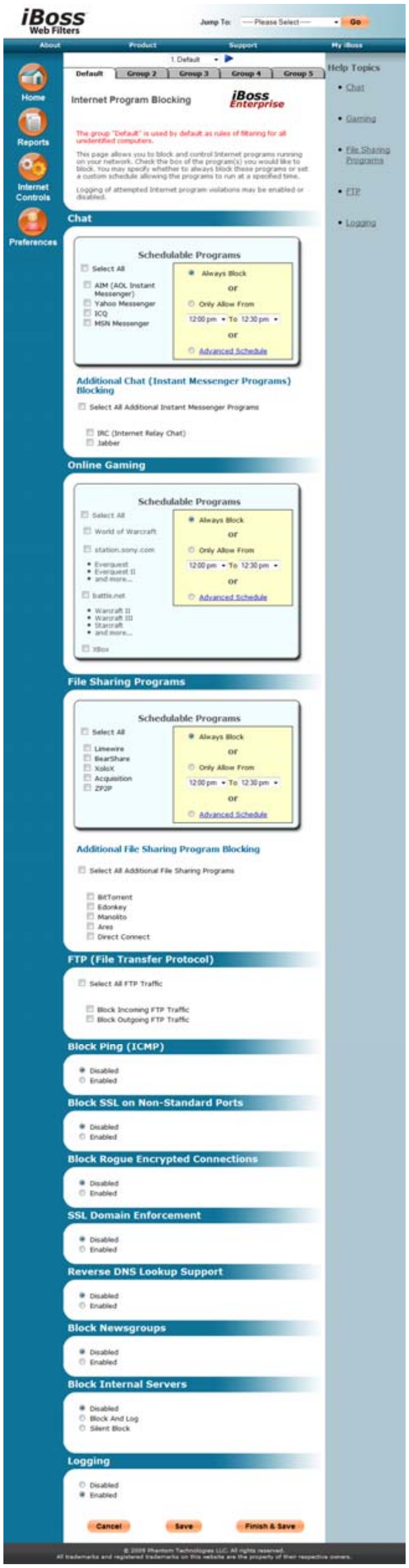
URL/Content:
Description: Direct IP Address access not allowed.

© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 33 - Identity Theft Detection Page

When a page is blocked from of the iBoss due to detection of Identity Theft (Phishing)/IP Address URL Blocking, this page will show up in the web browser to the user. You may manually login and add the blocked Identity theft page (IP address) to the allowlist if you feel that you have received the Identity Theft Detection in error by typing in the password and pressing Login.

4.2.2 Programs, Protocols & DLSP (Data Leakage Protection)



Internet Program Blocking

The group "Default" is used by default as rules of filtering for all unidentified computers.

This page allows you to block and control Internet programs running on your network. Check the box of the program(s) you would like to block. You may specify whether to always block these programs or set a custom schedule allowing the programs to run at a specified time.

Logging of attempted Internet program violations may be enabled or disabled.

Chat

Schedulable Programs

- □ Select All
- □ AIM (AOL Instant Messenger)
- □ Yahoo Messenger
- □ ICQ
- □ MSN Messenger

● Always Block
or
○ Only Allow From 12:00 pm To 12:30 pm
or
○ Advanced Schedule

Additional Chat (Instant Messenger Programs) Blocking

□ Select All Additional Instant Messenger Programs

- □ IRC (Internet Relay Chat)
- □ Jabber

Online Gaming

Schedulable Programs

- □ Select All
- □ World of Warcraft
- □ station.sony.com
  - Everquest
  - Everquest II
  - and more...
- □ battle.net
  - Warcraft II
  - Warcraft III
  - Starcraft
  - and more...
- □ XBox

● Always Block
or
○ Only Allow From 12:00 pm To 12:30 pm
or
○ Advanced Schedule

File Sharing Programs

Schedulable Programs

- □ Select All
- □ Limewire
- □ BearShare
- □ XoloX
- □ Acquisition
- □ ZP2P

● Always Block
or
○ Only Allow From 12:00 pm To 12:30 pm
or
○ Advanced Schedule

Additional File Sharing Program Blocking

□ Select All Additional File Sharing Programs

- □ BitTorrent
- □ Edonkey
- □ Manolito
- □ Ares
- □ Direct Connect

FTP (File Transfer Protocol)

□ Select All FTP Traffic

- □ Block Incoming FTP Traffic
- □ Block Outgoing FTP Traffic

Block Ping (ICMP)

● Disabled
○ Enabled

Block SSL on Non-Standard Ports

● Disabled
○ Enabled

Block Rogue Encrypted Connections

● Disabled
○ Enabled

SSL Domain Enforcement

● Disabled
○ Enabled

Reverse DNS Lookup Support

● Disabled
○ Enabled

Block Newsgroups

● Disabled
○ Enabled

Block Internal Servers

● Disabled
○ Block And Log
○ Silent Block

Logging

○ Disabled
● Enabled

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 34 - Block Specific Web Programs

The "Internet Program Blocking" section allows you to configure the current iBoss program blocking settings.

Chat - This category contains applications used for online messaging and chat. The iBoss can block the selected program(s) and log attempted violations. Examples of applications in this category are:

AIM (AOL Instant Messenger)
Yahoo Messenger
ICQ
MSN Messenger
IRC (Internet Relay Chat)
Jabber

Chat Schedule - Allows you to schedule daily access for selected chat programs. This option will bypass blocking for chat and instant messenger programs during the specified time.

Gaming
This category contains online gaming applications. The iBoss can block the selected program(s) and log attempted access violations. Examples of applications in this category are:

World of Warcraft
StarCraft
Everquest/Everquest II
XBox

Gaming Schedule - Allows you to schedule daily access for selected online gaming programs. This option will bypass blocking for online gaming programs during the specified time.

File Sharing Programs - This category contains online file sharing applications. The iBoss can block the selected program(s) and log attempted access violations. Examples of applications in this category are:

Limewire
XoloX
ZP2P
BearShare
Acquisition
BitTorrent
Edonkey
Manolito
Ares
Direct Connect

File Sharing Schedule - Allows you to schedule daily access for selected file sharing programs. This option will bypass blocking for file sharing programs during the specified time.

FTP (File Sharing Protocol) - You may choose to enable blocking for incoming and outgoing FTP Traffic. Enabling this feature will allow you to block incoming, outgoing, or all FTP Traffic.

Block Ping (ICMP) - You may choose to enable blocking for outgoing Ping (ICMP) Traffic.

Block SSL on Non-Standard Ports - You may choose to enable blocking SSL on Non-Standard Ports. This feature is useful for blocking File Sharing programs which use encryption over non-standard ports.

Block Rogue Encrypted Connections – You may choose to enable blocking for Rogue Encrypted Connections. This option blocks invalid SSL certificates and blocks programs that use Rogue Encryptions such as UltraSurf.

SSL Domain Enforcement – This option validates domains with the SSL certificate.

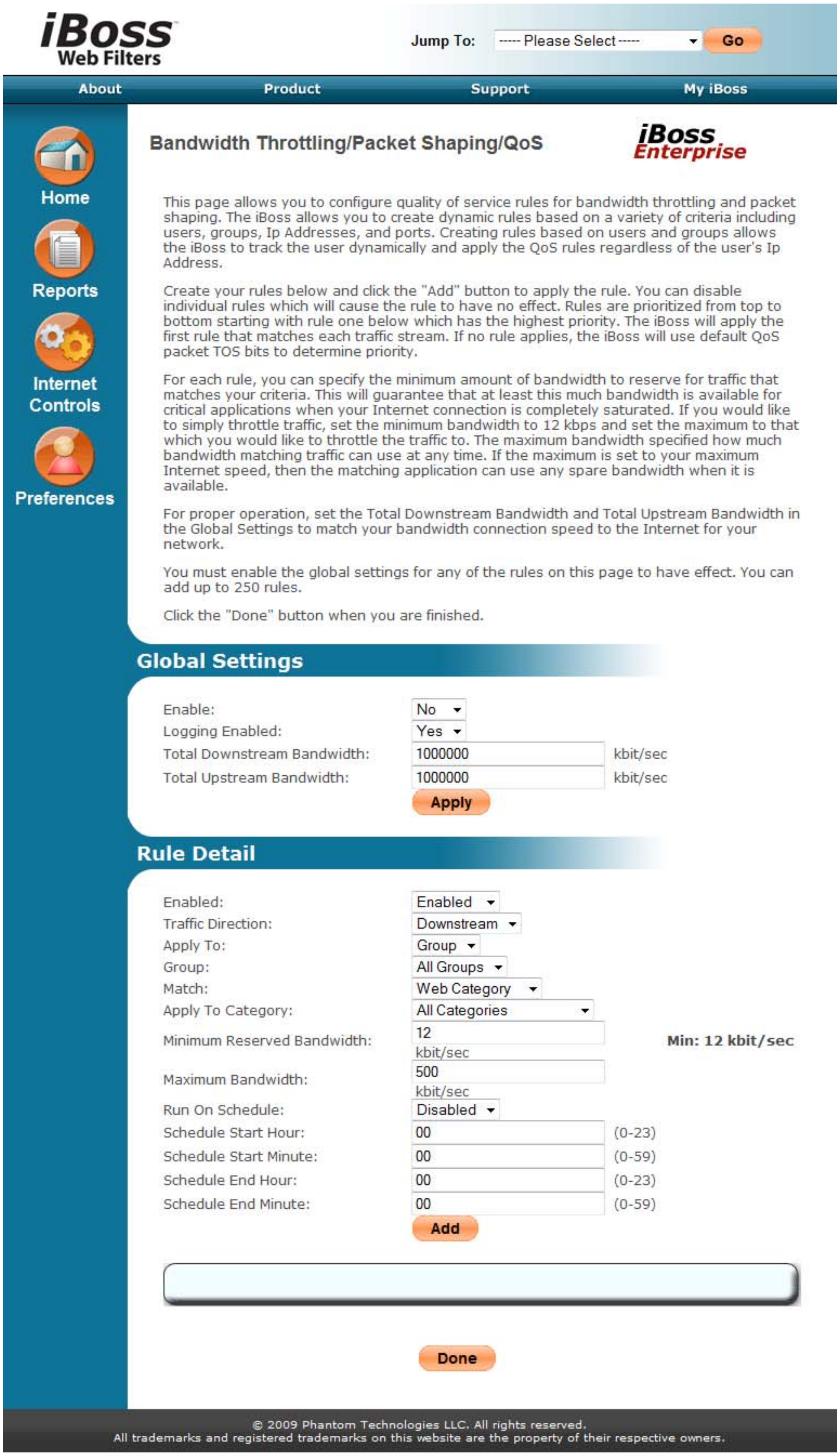
Reverse DNS Lookup Support – This option allows for Reverse DNS lookup support.

Block Newsgroups - You may choose to enable blocking newsgroup traffic.

Block Internal Servers - You may choose to enable blocking for internal Servers. This option helps block programs like BitTorrent which upload as well.

Logging - Allows you to enable or disable logging of attempted program access violations. This log is found on the Reports page. The logging includes date, time, and category. Logging can be enabled while in stealth mode. This is useful for monitoring your Internet usage while remaining unnoticed on the network. Without logging, the iBoss program blocking will still work however violations will not be logged.

4.2.3 Bandwidth Throttling/QoS



Bandwidth Throttling/Packet Shaping/QoS

This page allows you to configure quality of service rules for bandwidth throttling and packet shaping. The iBoss allows you to create dynamic rules based on a variety of criteria including users, groups, Ip Addresses, and ports. Creating rules based on users and groups allows the iBoss to track the user dynamically and apply the QoS rules regardless of the user's Ip Address.

Create your rules below and click the "Add" button to apply the rule. You can disable individual rules which will cause the rule to have no effect. Rules are prioritized from top to bottom starting with rule one below which has the highest priority. The iBoss will apply the first rule that matches each traffic stream. If no rule applies, the iBoss will use default QoS packet TOS bits to determine priority.

For each rule, you can specify the minimum amount of bandwidth to reserve for traffic that matches your criteria. This will guarantee that at least this much bandwidth is available for critical applications when your Internet connection is completely saturated. If you would like to simply throttle traffic, set the minimum bandwidth to 12 kbps and set the maximum to that which you would like to throttle the traffic to. The maximum bandwidth specified how much bandwidth matching traffic can use at any time. If the maximum is set to your maximum Internet speed, then the matching application can use any spare bandwidth when it is available.

For proper operation, set the Total Downstream Bandwidth and Total Upstream Bandwidth in the Global Settings to match your bandwidth connection speed to the Internet for your network.

You must enable the global settings for any of the rules on this page to have effect. You can add up to 250 rules.

Click the "Done" button when you are finished.

Global Settings

Enable:	No	
Logging Enabled:	Yes	
Total Downstream Bandwidth:	1000000	kbit/sec
Total Upstream Bandwidth:	1000000	kbit/sec

Apply

Rule Detail

Enabled:	Enabled	
Traffic Direction:	Downstream	
Apply To:	Group	
Group:	All Groups	
Match:	Web Category	
Apply To Category:	All Categories	
Minimum Reserved Bandwidth:	12 kbit/sec	Min: 12 kbit/sec
Maximum Bandwidth:	500 kbit/sec	
Run On Schedule:	Disabled	
Schedule Start Hour:	00	(0-23)
Schedule Start Minute:	00	(0-59)
Schedule End Hour:	00	(0-23)
Schedule End Minute:	00	(0-59)

Add

Done

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 35 - Bandwidth Throttling / QoS

This feature allows you to configure quality of service rules for bandwidth throttling and packet shaping. The iBoss allows you to create dynamic rules based on a variety of criteria including users, groups, Ip Addresses, and ports. Creating rules based on users and groups allows the iBoss to track the user dynamically and apply the QoS rules regardless of the user's Ip Address.

Create your rules and click the "**Add**" button to apply the rule. You can disable individual rules which will cause the rule to have no effect. Rules are prioritized from top to bottom starting with rule one below which has the highest priority. The iBoss will apply the first rule that matches each traffic stream. If no rule applies, the iBoss will use default QoS packet TOS bits to determine priority.

For each rule, you can specify the minimum amount of bandwidth to reserve for traffic that matches your criteria. This will guarantee that at least this much bandwidth is available for critical applications when your Internet connection is completely saturated. If you would like to simply throttle traffic, set the minimum bandwidth to **12 kbps** and set the maximum to that which you would like to throttle the traffic to. The maximum bandwidth specified how much bandwidth matching traffic can use at any time. If the maximum is set to your maximum Internet speed, then the matching application can use any spare bandwidth when it is available.

For proper operation, set the Total Downstream Bandwidth and Total Upstream Bandwidth in the Global Settings to match your bandwidth connection speed to the Internet for your network.

You must enable the global settings for any of the rules on this page to have effect. You can add up to 250 rules.

Click the "**Done**" button when you are finished.

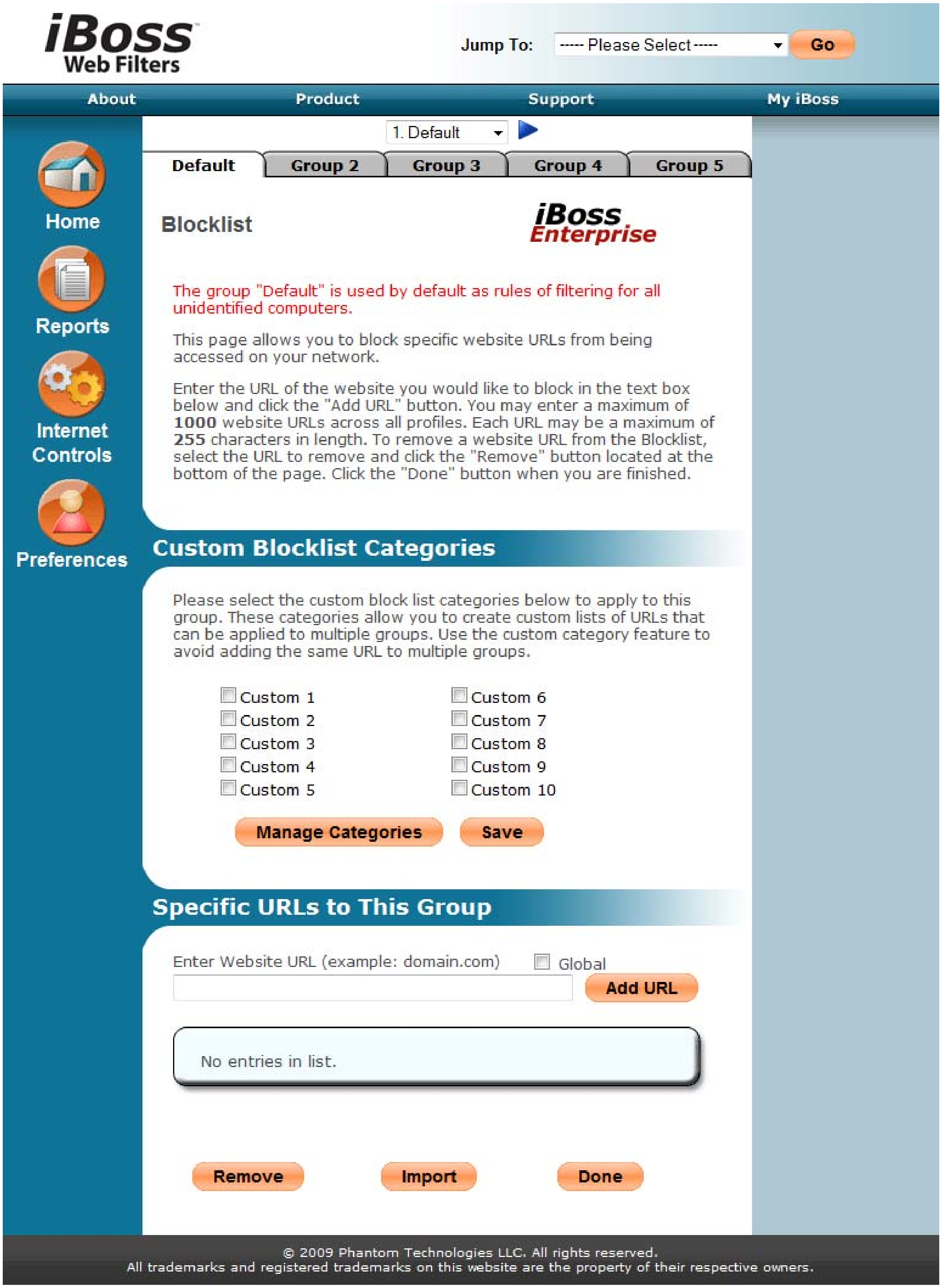
Global Settings - These are global settings for the bandwidth throttling.
Enable – This is a global option to turn this feature on or off.
Logging Enabled – This option logs the bandwidth throttles in the reports.
Total Downstream Bandwidth – This sets the total amount of Downstream bandwidth on your network in kbit/sec.
Total Upstream Bandwidth - This sets the total amount of Upstream bandwidth on your network in kbit/sec.

Once you have finished with changes any of these settings, click “**Apply**”.

Rule Detail – These are the individual settings for the bandwidth throttles you set.
Enabled – This option is to turn this throttle on or off.
Traffic Direction – This is the direction in which the throttle takes place, either upstream or downstream.
Apply To – This field allows you to specify if this rule is for a group or user.

Group (only if applied to Groups) – This allows you to choose the group in which this rule is set for.
Group (only if applied to User) – This allows you to choose the username in which this rule is set for.
Match – This is the rule in which this rule is set for. You may choose Web Category, Domain, IP Addresses, or TCP/UDP ports.
Apply To Category – This allows you to choose which web category to apply this rule to.
Minimum Reserved Bandwidth – This is the minimum reserved bandwidth for this rule in kbit/sec. Min: 12 kbit/sec
Maximum Bandwidth – This is the Maximum cap of this rule in kbit/sec.
Run On Schedule – This option allows you to set a schedule time for this rule.
Schedule Start Hour – Start time for this rule in hours on 24 hour format (0-23)
Schedule Start Minute – Start minute for this rule (0-59)
Schedule End Hour – End hour for this rule (0-23)
Schedule End Minute – End minute for this rule (0-59)

4.2.4 Block Specific Websites



Blocklist

The group "Default" is used by default as rules of filtering for all unidentified computers.

This page allows you to block specific website URLs from being accessed on your network.

Enter the URL of the website you would like to block in the text box below and click the "Add URL" button. You may enter a maximum of **1000** website URLs across all profiles. Each URL may be a maximum of **255** characters in length. To remove a website URL from the Blocklist, select the URL to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Custom Blocklist Categories

Please select the custom block list categories below to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

□ Custom 1
□ Custom 2
□ Custom 3
□ Custom 4
□ Custom 5
□ Custom 6
□ Custom 7
□ Custom 8
□ Custom 9
□ Custom 10

Specific URLs to This Group

Enter Website URL (example: domain.com) □ Global

No entries in list.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

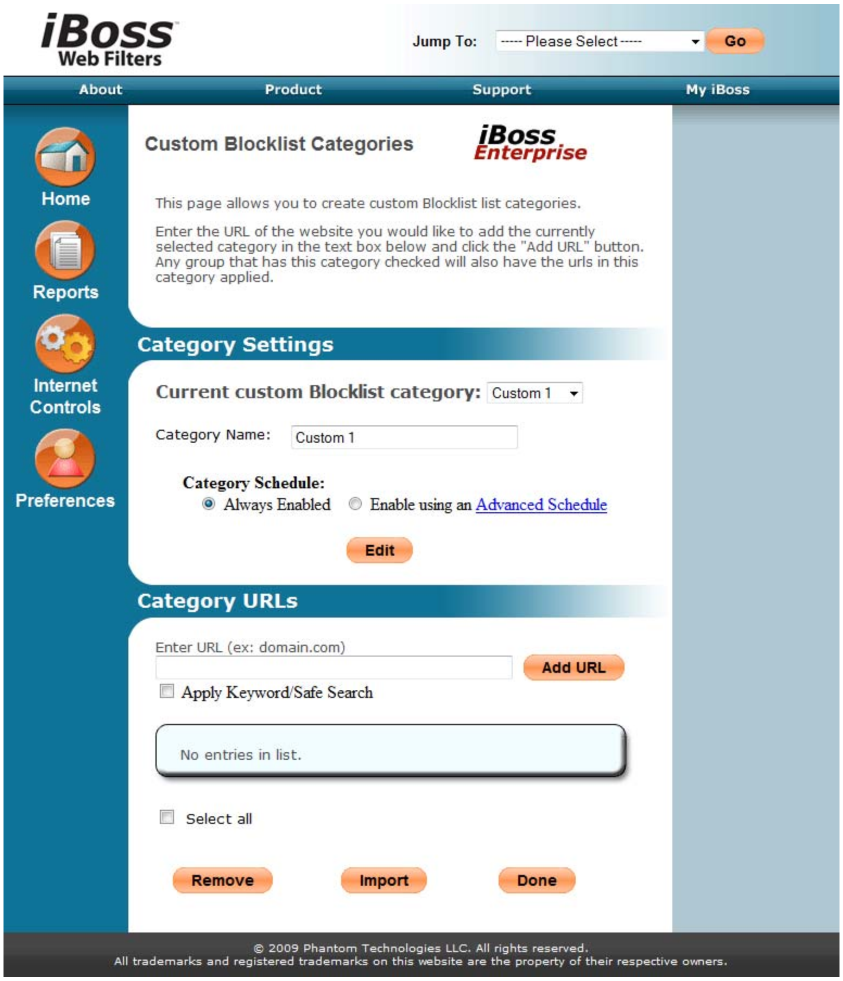
Figure 36 - Block Specific Websites

]

This page allows you to block specific website URLs from being accessed on your network.

Enter the URL of the website you would like to block in the text box below and click the "**Add URL**" button. You may enter a maximum of 1000 website URLs across all profiles. Each URL may be a maximum of 255 characters in length. To remove a website URL from the Blocklist, select the URL to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

4.2.4.1 Custom Blocklist Categories



Custom Blocklist Categories

This page allows you to create custom Blocklist list categories.

Enter the URL of the website you would like to add the currently selected category in the text box below and click the "Add URL" button. Any group that has this category checked will also have the urls in this category applied.

Category Settings

Current custom Blocklist category: Custom 1

Category Name: Custom 1

Category Schedule:
● Always Enabled ○ Enable using an Advanced Schedule

Category URLs

Enter URL (ex: domain.com)

□ Apply Keyword/Safe Search

No entries in list.

□ Select all

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

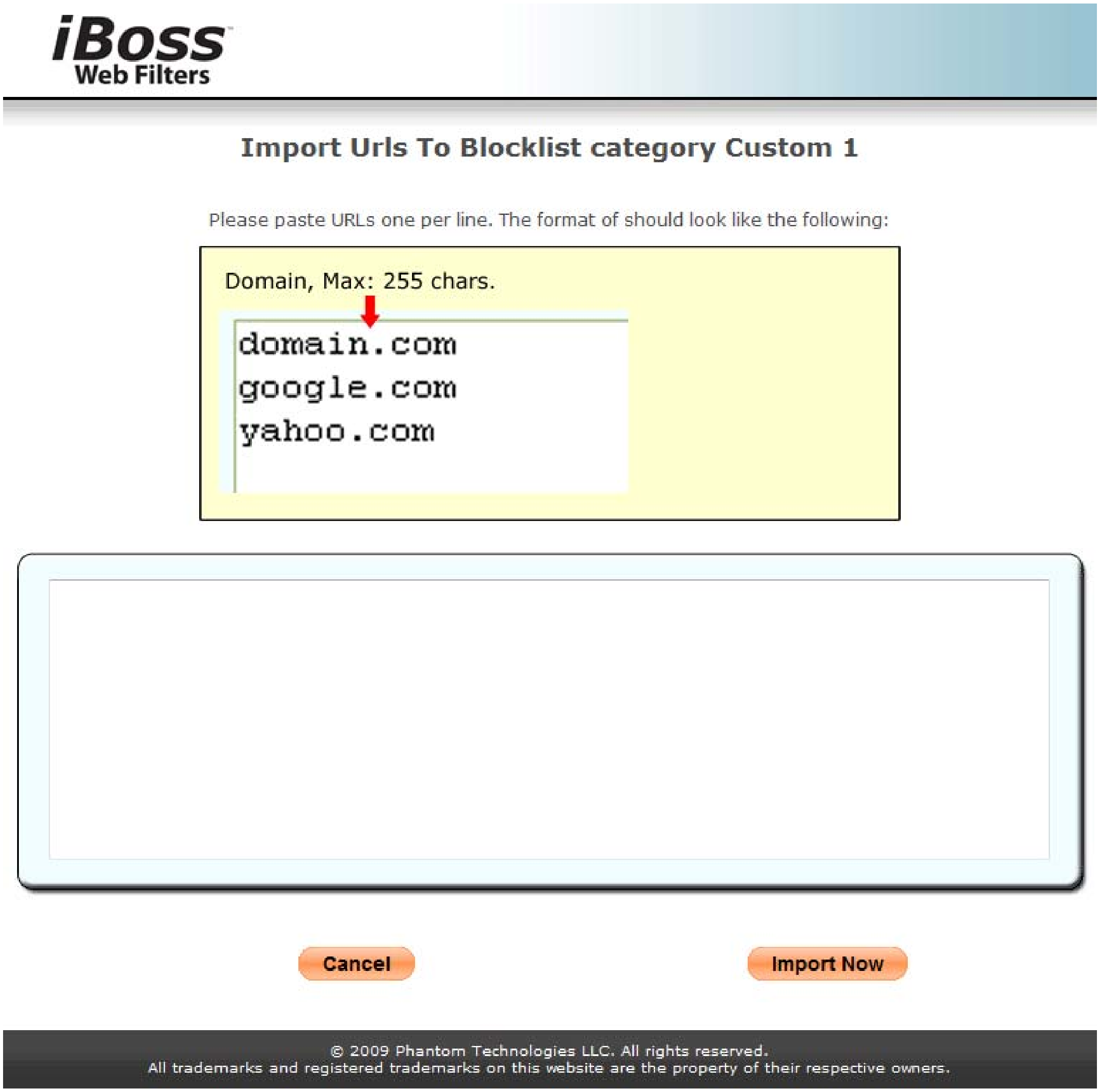
Figure 37 - Custom Blocklist Categories

Select the custom block list categories to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

This feature allows you to create custom Blocklist list categories.

Enter the URL of the website you would like to add the currently selected category in the text box below and click the "Add URL" button. Any group that has this category checked will also have the URLs in this category applied.

4.2.4.2 Blocklist Import



Import Urls To Blocklist category Custom 1

Please paste URLs one per line. The format of should look like the following:

Domain, Max: 255 chars.

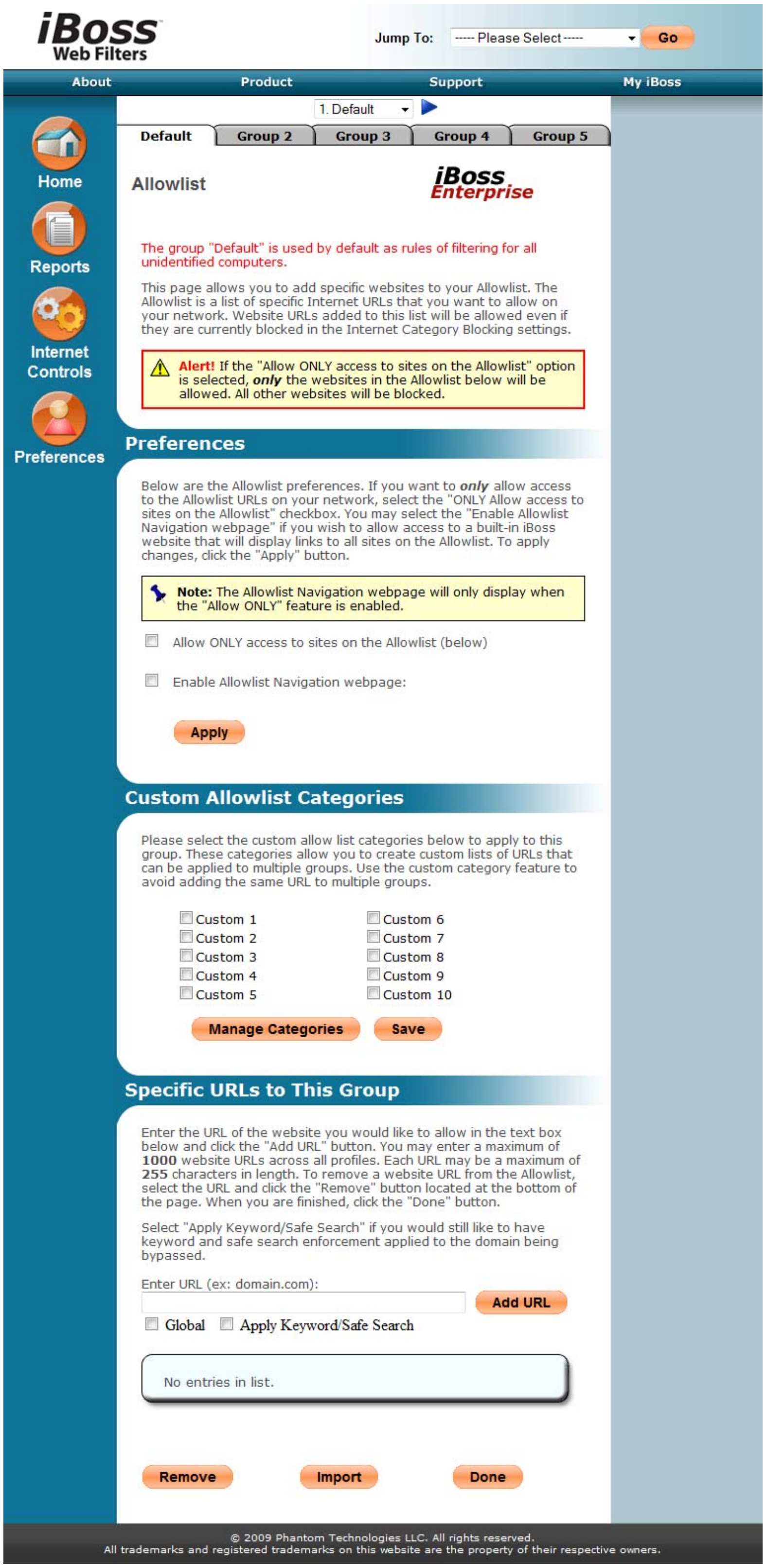
```
domain.com
google.com
yahoo.com
```

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 38 - Blocklist Import

You may import a list of domains to import. Please paste URLs one per line with a maximum of 255 characters per domain/IP/URL. Once you are done, click the Import Now button.

4.2.1 Allow Specific Websites



Allowlist

The group "Default" is used by default as rules of filtering for all unidentified computers.

This page allows you to add specific websites to your Allowlist. The Allowlist is a list of specific Internet URLs that you want to allow on your network. Website URLs added to this list will be allowed even if they are currently blocked in the Internet Category Blocking settings.

⚠ **Alert!** If the "Allow ONLY access to sites on the Allowlist" option is selected, ***only*** the websites in the Allowlist below will be allowed. All other websites will be blocked.

Preferences

Below are the Allowlist preferences. If you want to ***only*** allow access to the Allowlist URLs on your network, select the "ONLY Allow access to sites on the Allowlist" checkbox. You may select the "Enable Allowlist Navigation webpage" if you wish to allow access to a built-in iBoss website that will display links to all sites on the Allowlist. To apply changes, click the "Apply" button.

Note: The Allowlist Navigation webpage will only display when the "Allow ONLY" feature is enabled.

☐ Allow ONLY access to sites on the Allowlist (below)

☐ Enable Allowlist Navigation webpage:

Custom Allowlist Categories

Please select the custom allow list categories below to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

☐ Custom 1
☐ Custom 2
☐ Custom 3
☐ Custom 4
☐ Custom 5
☐ Custom 6
☐ Custom 7
☐ Custom 8
☐ Custom 9
☐ Custom 10

Specific URLs to This Group

Enter the URL of the website you would like to allow in the text box below and click the "Add URL" button. You may enter a maximum of **1000** website URLs across all profiles. Each URL may be a maximum of **255** characters in length. To remove a website URL from the Allowlist, select the URL and click the "Remove" button located at the bottom of the page. When you are finished, click the "Done" button.

Select "Apply Keyword/Safe Search" if you would still like to have keyword and safe search enforcement applied to the domain being bypassed.

Enter URL (ex: domain.com):

☐ Global ☐ Apply Keyword/Safe Search

No entries in list.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 39 - Allow Specific Websites

This page allows you to add specific websites to your Allowlist. The Allowlist is a list of specific Internet URLs that you want to allow on your network. Website URLs added to this list will be allowed even if they are currently blocked in the Internet Category Blocking settings.

Alert! If the "Allow **ONLY access to sites on the Allowlist**" option is selected, only the websites in the Allowlist below will be allowed. All other websites will be blocked.

If you want to only allow access to the Allowlist URLs on your network, select the "**ONLY Allow access to sites on the Allowlist**" checkbox. You may select the "**Enable Allowlist Navigation webpage**" if you wish to allow access to a built-in iBoss website that will display links to all sites on the Allowlist. To apply changes, click the "**Apply**" button.

Note: The Allowlist Navigation webpage will only display when the "**Allow ONLY**" feature is enabled.

Allow ONLY access to sites on the Allowlist – Checking this option will only allow sites in list.
Enable Allowlist Navigation webpage - This will give you a page that has a list of the allowed sites to be able to give to your users.

Once you have changed any of these settings, click the “**Apply**” button.

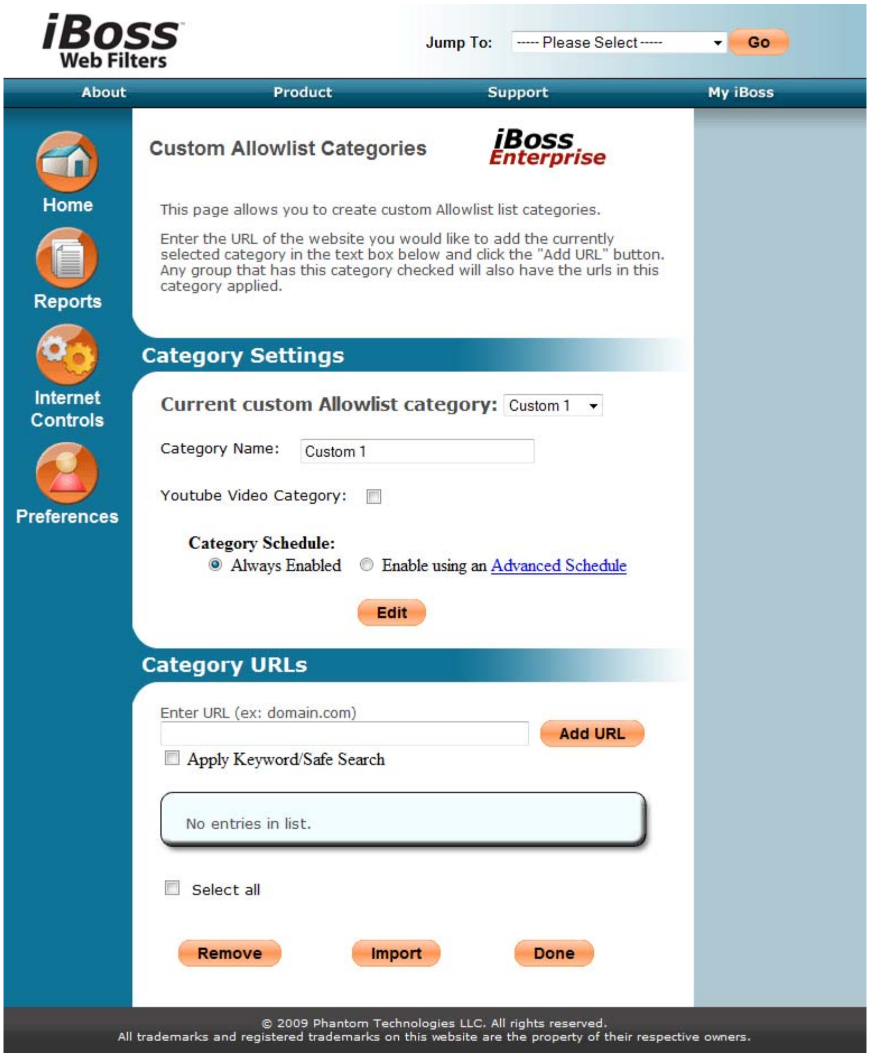
Enter the URL of the website you would like to allow in the text box below and click the "**Add URL**" button. You may enter a maximum of 1000 website URLs across all profiles. Each URL may be a maximum of 255 characters in length. To remove a website URL from the Allowlist, select the URL and click the "**Remove**" button located at the bottom of the page. When you are finished, click the "**Done**" button.

Select "**Apply Keyword / Safe Search**" if you would still like to have keyword and safe search enforcement applied to the domain being bypassed.

Enter URL (ex: domain.com) – field to enter the domain or URL to allow.
Global – Option to allow across all filtering groups
Apply Keyword / Safe Search – Allows the domain or URL if it contains this keyword added. This is not recommended as it may allow false positives.

Once you have entered in a URL or domain, click the “**Add URL**” button.

4.2.1.1 Custom Allowlist Categories



Custom Allowlist Categories

This page allows you to create custom Allowlist list categories.

Enter the URL of the website you would like to add the currently selected category in the text box below and click the "Add URL" button. Any group that has this category checked will also have the urls in this category applied.

Category Settings

Current custom Allowlist category: Custom 1

Category Name: Custom 1

Youtube Video Category: □

Category Schedule:
● Always Enabled ○ Enable using an Advanced Schedule

Category URLs

Enter URL (ex: domain.com)

□ Apply Keyword/Safe Search

No entries in list.

□ Select all

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 40 - Custom Allowlist Categories

Select the custom allow list categories to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

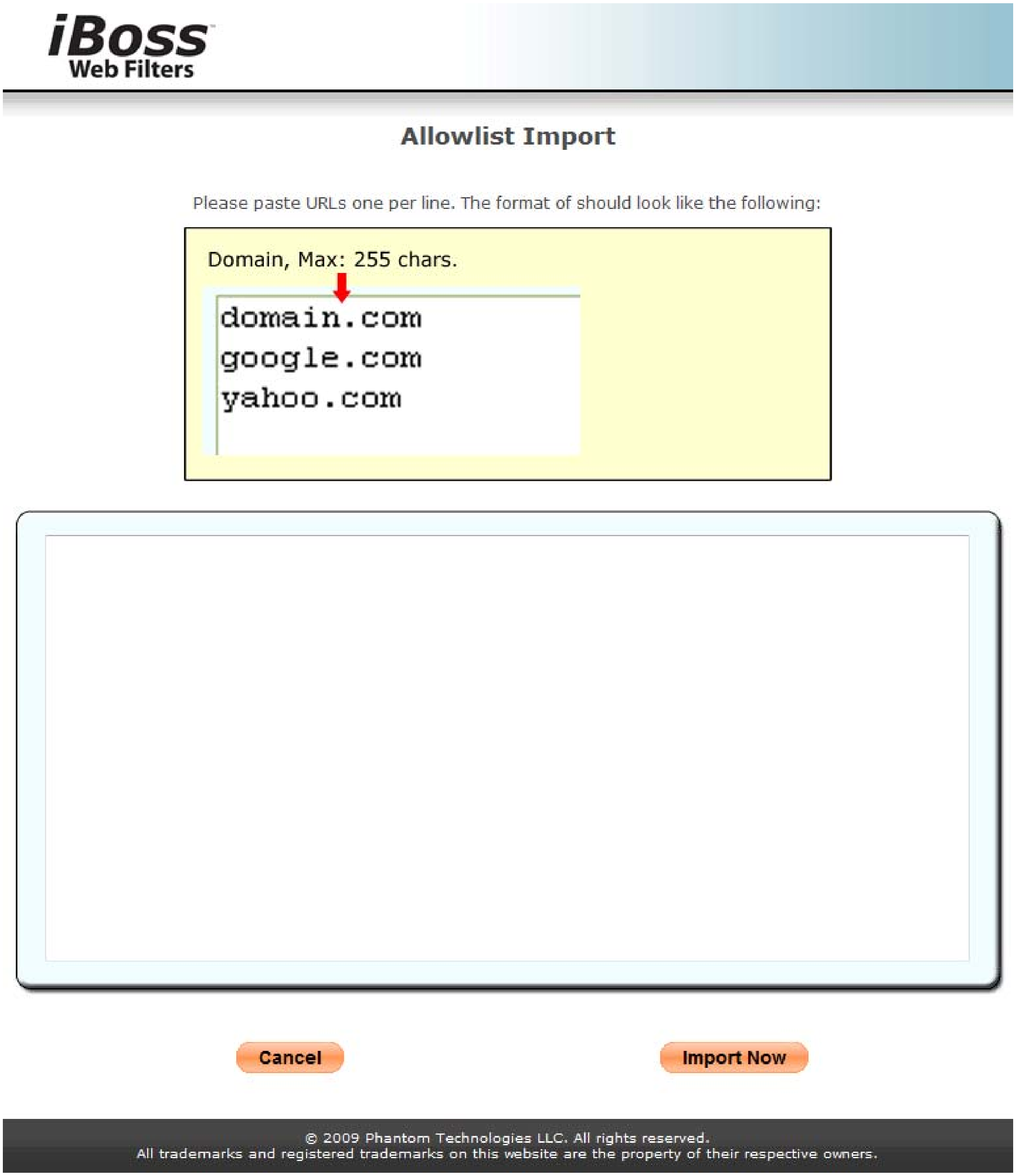
This feature allows you to create custom Allowlist list categories.

Enter the URL of the website you would like to add the currently selected category in the text box below and click the "**Add URL**" button. Any group that has this category checked will also have the URLs in this category applied.

Youtube Video Category – This option allows you to allow specific YouTube videos while blocking having the Audio/Video category still block the YouTube site.

Apply Keyword/Safe Search - Allows the domain or URL if it contains this keyword added. This is not recommended as it may allow false positives.

4.2.1.2 Allowlist Import



Allowlist Import

Please paste URLs one per line. The format of should look like the following:

Domain, Max: 255 chars.

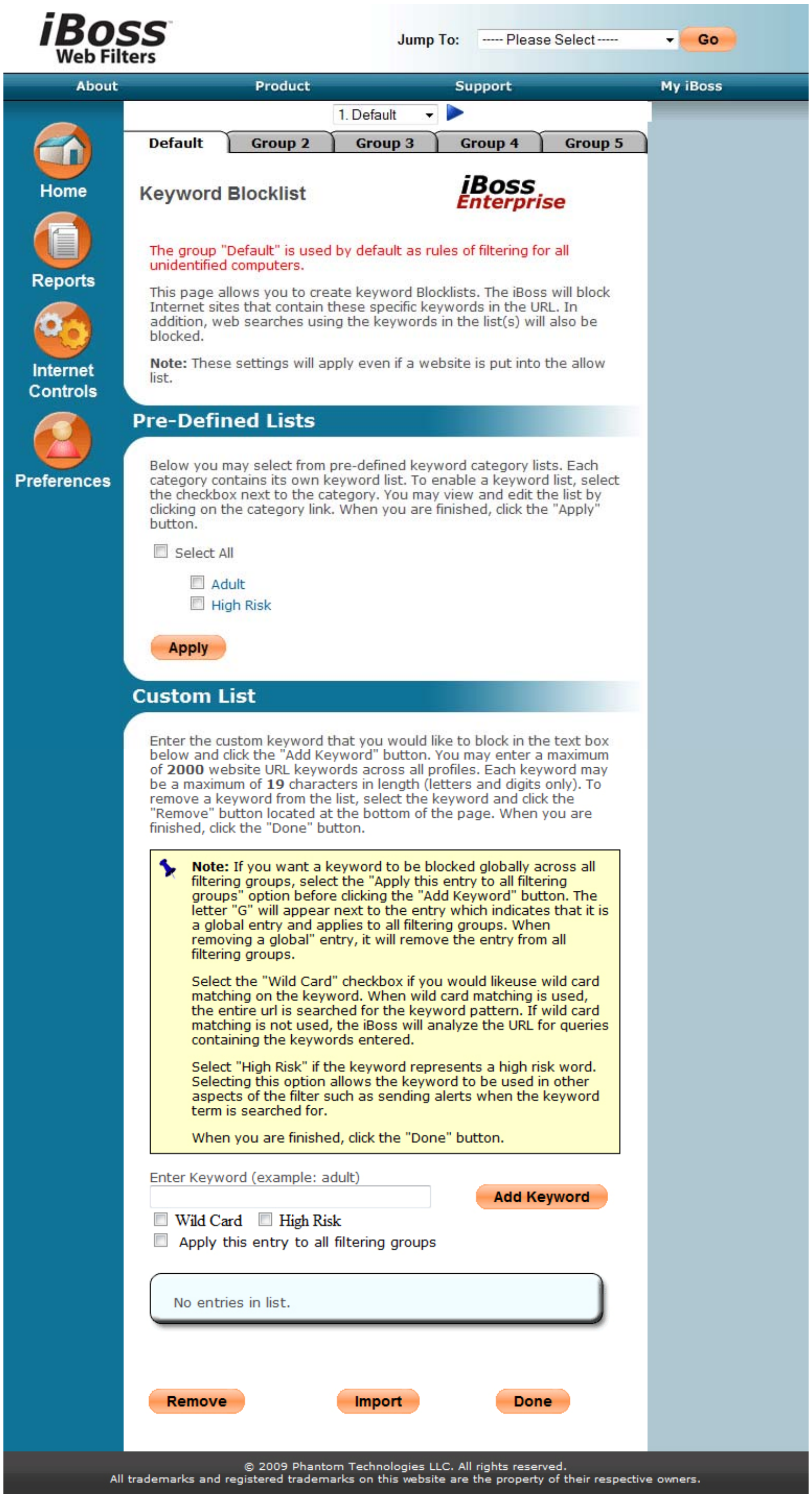
```
domain.com
google.com
yahoo.com
```

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 41 - Allowlist Import

You may import a list of domains to import. Please paste URLs one per line with a maximum of 255 characters per domain/IP/URL. Once you are done, click the Import Now button.

4.2.2 Block Specific Keywords



Keyword Blocklist

The group "Default" is used by default as rules of filtering for all unidentified computers.

This page allows you to create keyword Blocklists. The iBoss will block Internet sites that contain these specific keywords in the URL. In addition, web searches using the keywords in the list(s) will also be blocked.

Note: These settings will apply even if a website is put into the allow list.

Pre-Defined Lists

Below you may select from pre-defined keyword category lists. Each category contains its own keyword list. To enable a keyword list, select the checkbox next to the category. You may view and edit the list by clicking on the category link. When you are finished, click the "Apply" button.

☐ Select All

☐ Adult
☐ High Risk

Custom List

Enter the custom keyword that you would like to block in the text box below and click the "Add Keyword" button. You may enter a maximum of **2000** website URL keywords across all profiles. Each keyword may be a maximum of **19** characters in length (letters and digits only). To remove a keyword from the list, select the keyword and click the "Remove" button located at the bottom of the page. When you are finished, click the "Done" button.

Note: If you want a keyword to be blocked globally across all filtering groups, select the "Apply this entry to all filtering groups" option before clicking the "Add Keyword" button. The letter "G" will appear next to the entry which indicates that it is a global entry and applies to all filtering groups. When removing a global" entry, it will remove the entry from all filtering groups.

Select the "Wild Card" checkbox if you would likeuse wild card matching on the keyword. When wild card matching is used, the entire url is searched for the keyword pattern. If wild card matching is not used, the iBoss will analyze the URL for queries containing the keywords entered.

Select "High Risk" if the keyword represents a high risk word. Selecting this option allows the keyword to be used in other aspects of the filter such as sending alerts when the keyword term is searched for.

When you are finished, click the "Done" button.

Enter Keyword (example: adult)

☐ Wild Card ☐ High Risk
☐ Apply this entry to all filtering groups

No entries in list.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 42 - Block Specific Keywords

This feature allows you to create keyword Blocklists. The iBoss will block Internet sites that contain these specific keywords in the URL. In addition, web searches using the keywords in the list(s) will also be blocked.

Pre-Defined Lists

You may select from pre-defined keyword category lists. Each category contains its own keyword list. To enable a keyword list, select the checkbox next to the category. You may view and edit the list by clicking on the category link. When you are finished, click the "**Apply**" button. To see the pre-defined list, you may click on the category name to see the pre-defined list and uncheck words if you wish.

Custom List

Enter the custom keyword that you would like to block in the text box below and click the "**Add Keyword**" button. You may enter a maximum of 2000 website URL keywords across all profiles. Each keyword may be a maximum of 19 characters in length (letters and digits only). To remove a keyword from the list, select the keyword and click the "**Remove**" button located at the bottom of the page. When you are finished, click the "**Done**" button.

Note: If you want a keyword to be blocked globally across all filtering groups, select the "**Apply this entry to all filtering groups**" option before clicking the "**Add Keyword**" button. The letter "**G**" will appear next to the entry which indicates that it is a global entry and applies to all filtering groups. When removing a global" entry, it will remove the entry from all filtering groups.

Select the "**Wild Card**" checkbox if you would like to use wild card matching on the keyword. When wild card matching is used, the entire URL is searched for the keyword pattern. If wild card matching is not used, the iBoss will analyze the URL for queries containing the keywords entered.

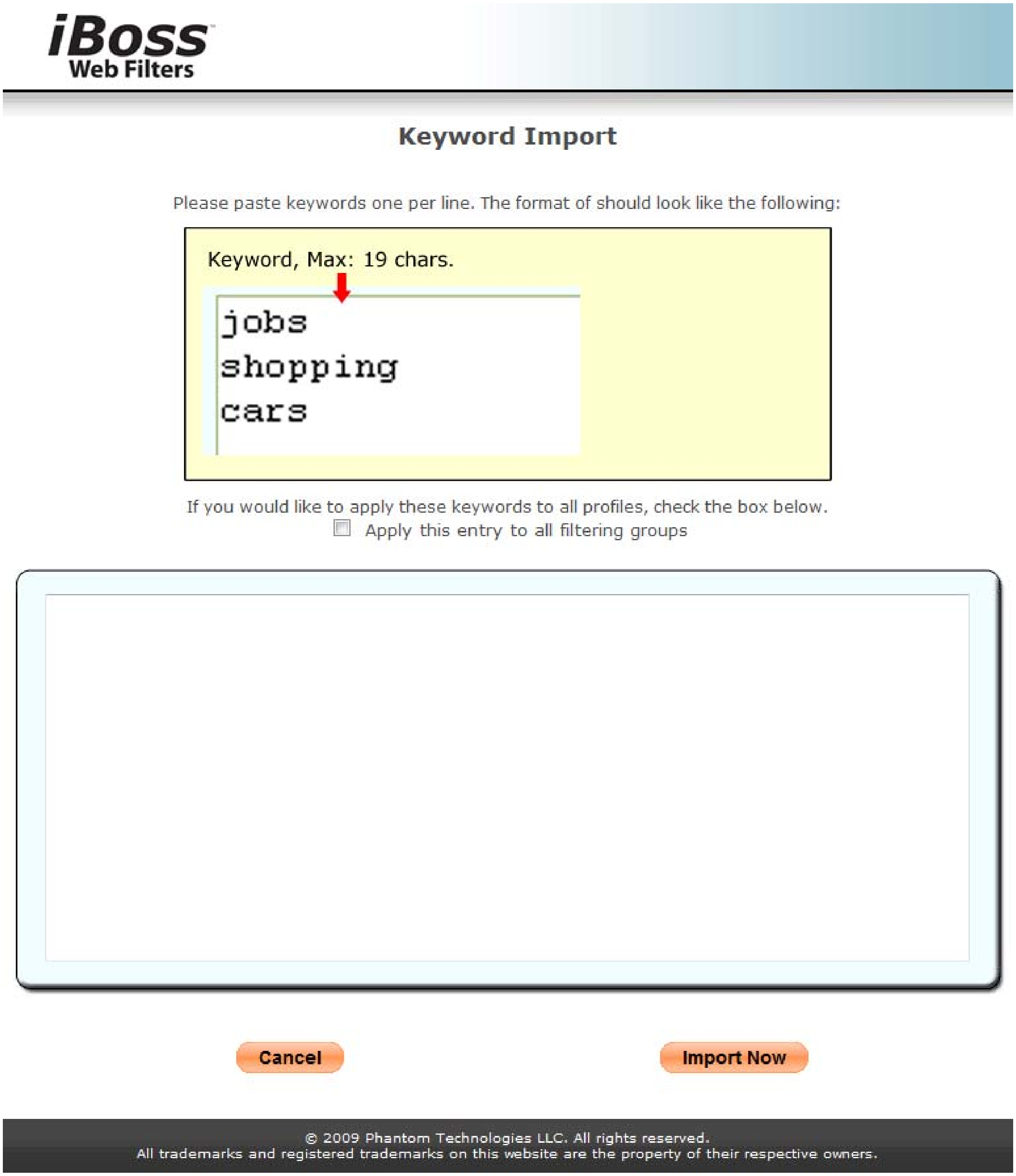
Select "**High Risk**" if the keyword represents a high risk word. Selecting this option allows the keyword to be used in other aspects of the filter such as sending alerts when the keyword term is searched for.

When you are finished, click the "**Done**" button.

Enter Keyword (example: adult) – This is the field to add the keyword you would like blocked. Once finished, click the “**Add Keyword**” button.
Wild Card – This is the wild card for any part of the URL to block the keyword.
High Risk – This option alerts the administrator when this keyword is searched for.
Apply this entry to all filtering groups – This option applies this block to all filtering groups.

You can import a list of keywords to block by clicking “**Import**”. You may remove keywords by checking the keyword and clicking the “**Remove**” button. Once finished, click the “**Done**” button.

4.2.2.1 Keyword Import



Keyword Import

Please paste keywords one per line. The format of should look like the following:

```
Keyword, Max: 19 chars.
jobs
shopping
cars
```

If you would like to apply these keywords to all profiles, check the box below.

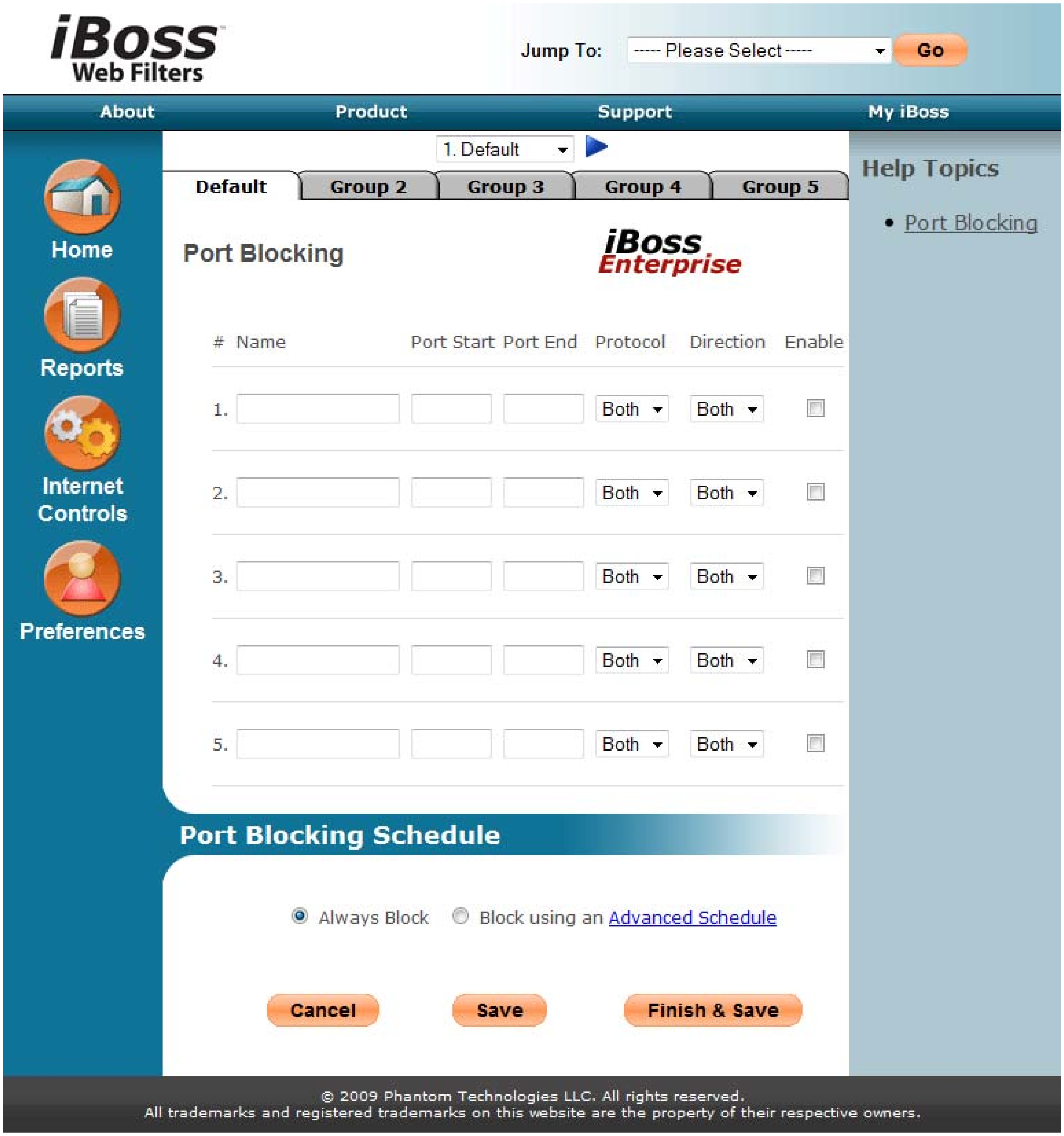
□ Apply this entry to all filtering groups

iBoss Web Filters
Cancel
Import Now
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 43 - Keyword Import

You may import a list of keywords to import. Please paste keywords one per line with a maximum of 19 characters per keyword. You may select Apply to all filtering groups. Once you are done, click the Import Now button.

4.2.3 Block Specific Ports


iBoss Web Filters
Jump To: ----- Please Select ----- Go
About
Product
Support
My iBoss
Home
Reports
Internet Controls
Preferences
1. Default
Default
Group 2
Group 3
Group 4
Group 5
iBoss Enterprise
Help Topics
Port Blocking
Cancel
Save
Finish & Save
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Port Blocking

#	Name	Port Start	Port End	Protocol	Direction	Enable
1.				Both	Both	□
2.				Both	Both	□
3.				Both	Both	□
4.				Both	Both	□
5.				Both	Both	□

Port Blocking Schedule

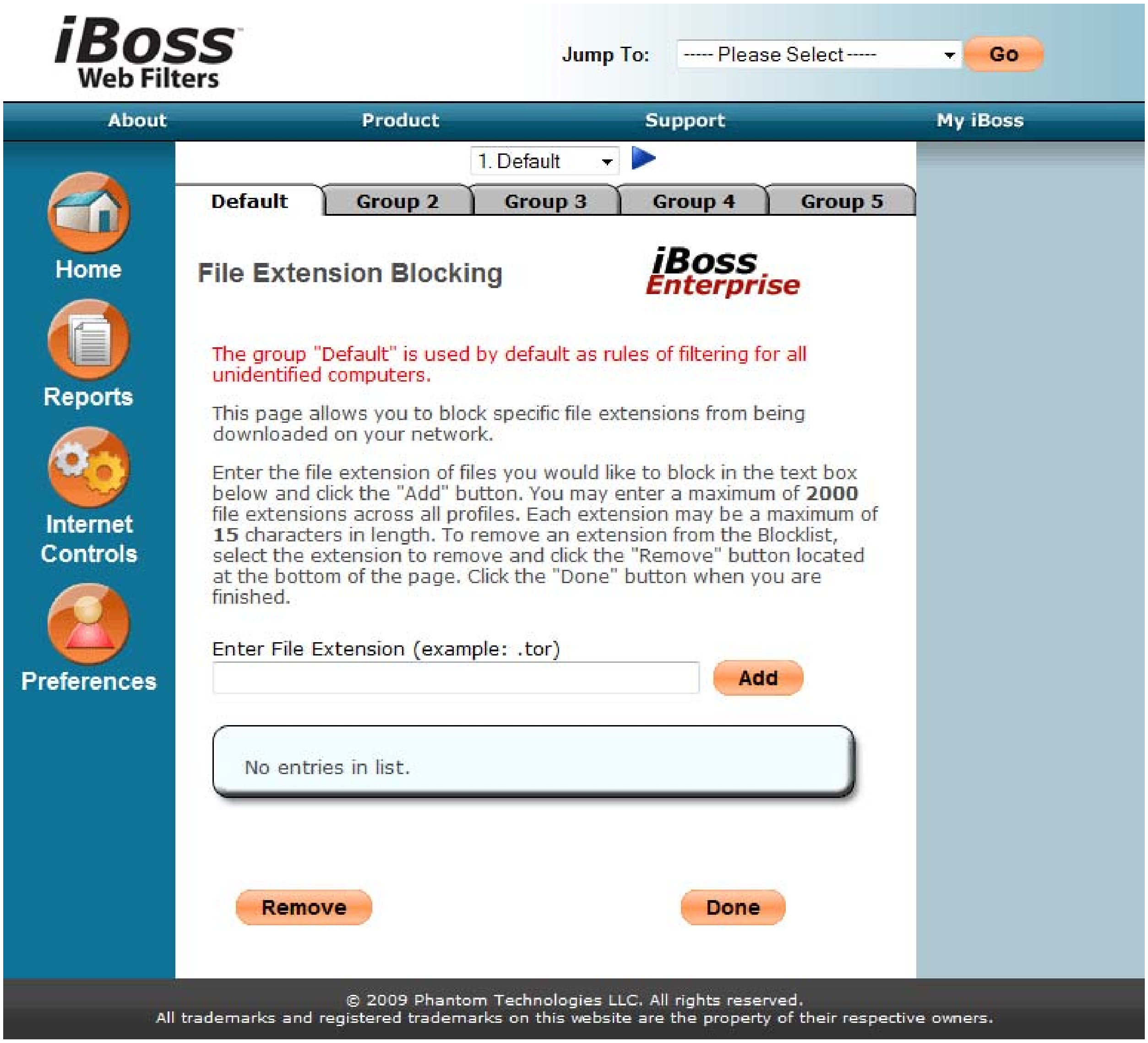
● Always Block ○ Block using an Advanced Schedule

Figure 44 - Port Blocking

Port blocking allows Internet traffic on specified ports or ranges of ports to be blocked from accessing the Internet. Traffic using the specified ports will be blocked completely. This allows you to enter the name, port start, port end, protocol, and direction. Once you enter in the information click Enable and save.

Port Blocking Schedule – You may choose to block these ports all the time or Block on an Advanced Schedule.

4.2.4 Block Specific File Extensions



File Extension Blocking

The group "Default" is used by default as rules of filtering for all unidentified computers.

This page allows you to block specific file extensions from being downloaded on your network.

Enter the file extension of files you would like to block in the text box below and click the "Add" button. You may enter a maximum of **2000** file extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the Blocklist, select the extension to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Enter File Extension (example: .tor)

No entries in list.

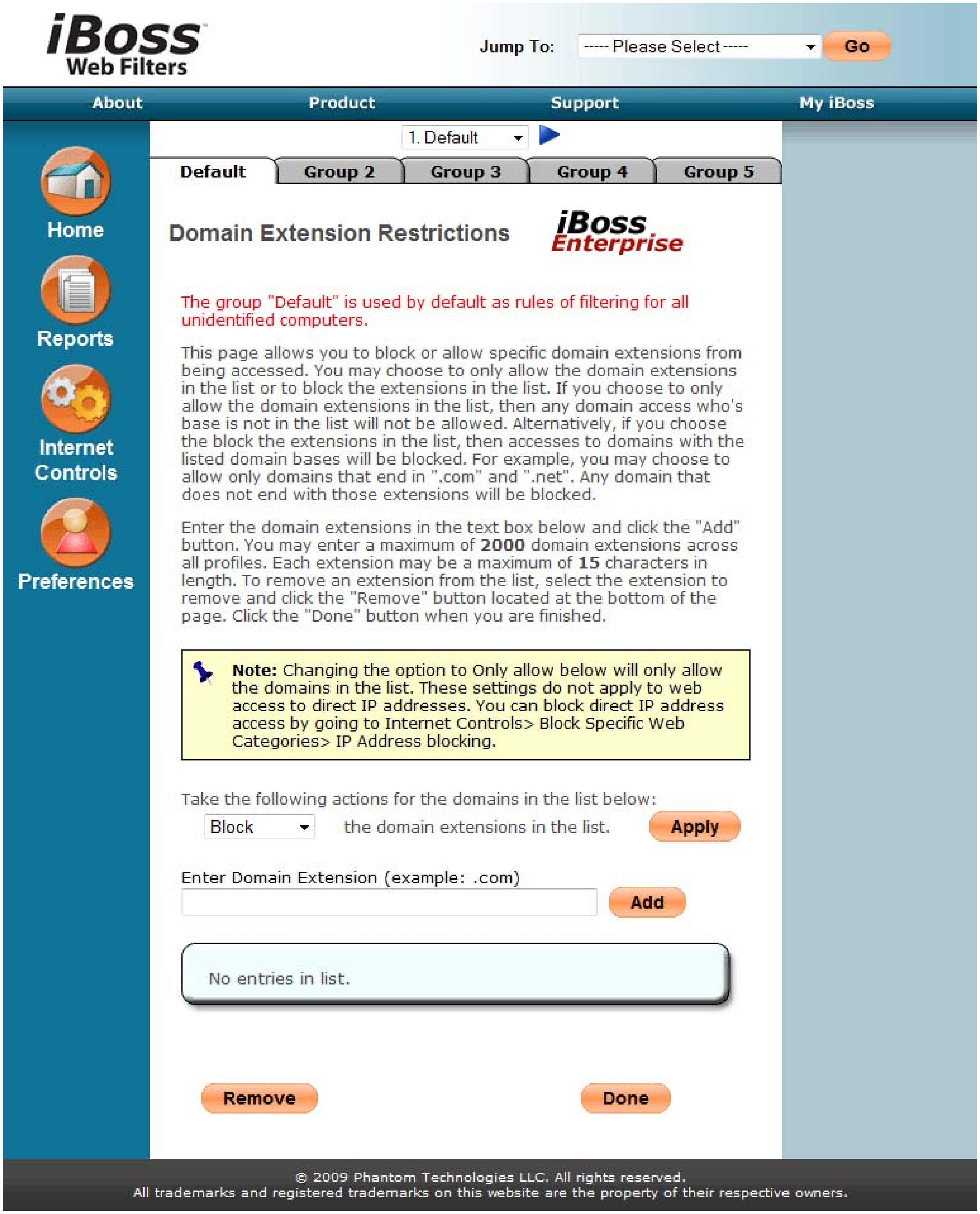
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 45 - Block Specific File Extensions

This page allows you to block specific file extensions from being downloaded on your network.

Enter the file extension of files you would like to block in the text box below and click the "**Add**" button. You may enter a maximum of **2000** file extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the Blocklist, select the extension to remove and click the "**Remove**" button located at the bottom of the page. Click the "**Done**" button when you are finished.

4.2.5 Restrict Domain Extensions



Domain Extension Restrictions

The group "Default" is used by default as rules of filtering for all unidentified computers.

This page allows you to block or allow specific domain extensions from being accessed. You may choose to only allow the domain extensions in the list or to block the extensions in the list. If you choose to only allow the domain extensions in the list, then any domain access who's base is not in the list will not be allowed. Alternatively, if you choose the block the extensions in the list, then accesses to domains with the listed domain bases will be blocked. For example, you may choose to allow only domains that end in ".com" and ".net". Any domain that does not end with those extensions will be blocked.

Enter the domain extensions in the text box below and click the "Add" button. You may enter a maximum of **2000** domain extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the list, select the extension to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note: Changing the option to Only allow below will only allow the domains in the list. These settings do not apply to web access to direct IP addresses. You can block direct IP address access by going to Internet Controls> Block Specific Web Categories> IP Address blocking.

Take the following actions for the domains in the list below:

Block the domain extensions in the list.

Enter Domain Extension (example: .com)

No entries in list.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

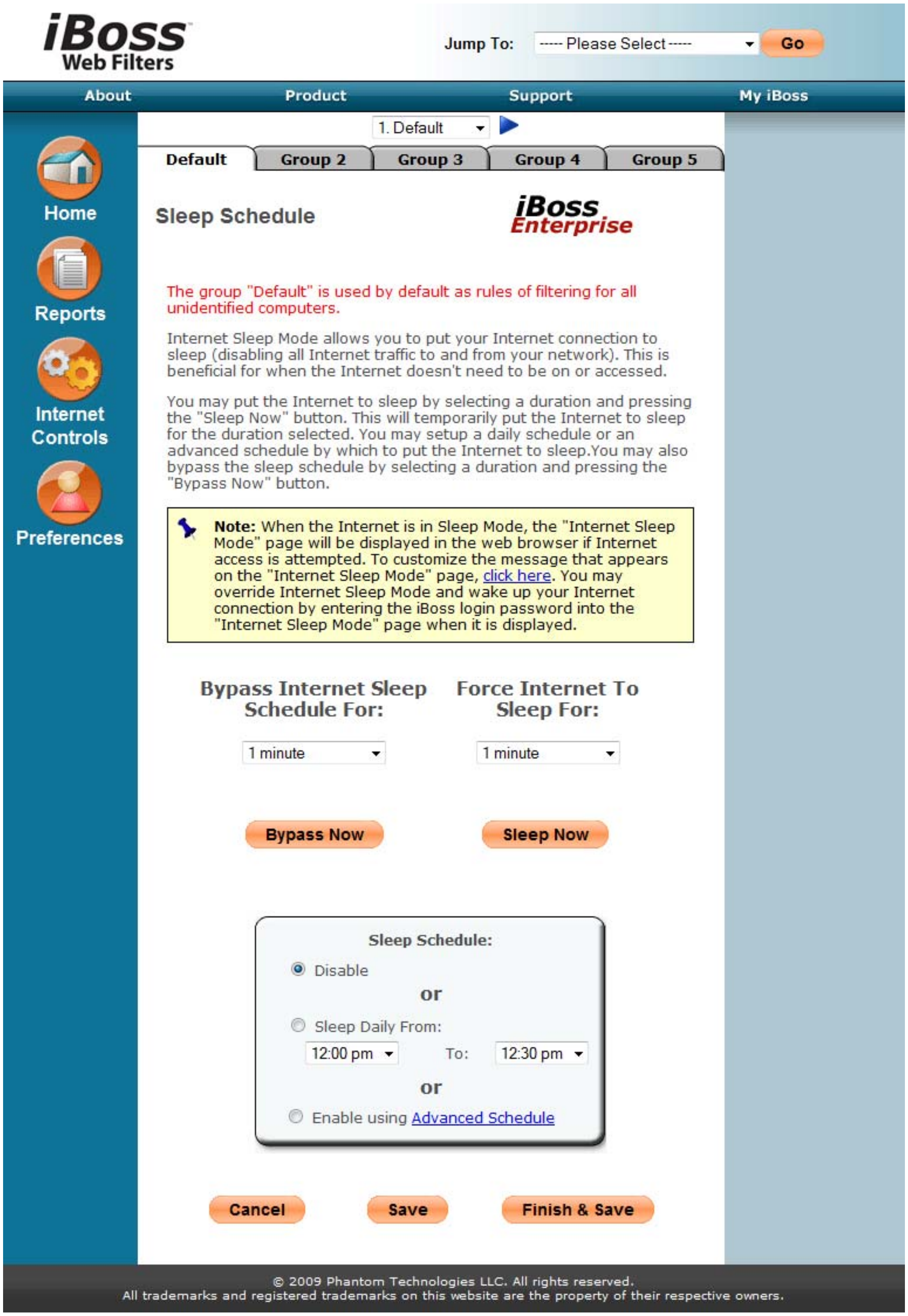
Figure 46 - Restrict Domain Extensions

This page allows you to block or allow specific domain extensions from being accessed. You may choose to only allow the domain extensions in the list or to block the extensions in the list. If you choose to only allow the domain extensions in the list, then any domain access who's base is not in the list will not be allowed. Alternatively, if you choose the block the extensions in the list, then accesses to domains with the listed domain bases will be blocked. For example, you may choose to allow only domains that end in ".com" and ".net". Any domain that does not end with those extensions will be blocked.

Enter the domain extensions in the text box below and click the "**Add**" button. You may enter a maximum of **2000** domain extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the list, select the extension to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note: Changing the option to Only allow below will only allow the domains in the list. These settings do not apply to web access to direct IP addresses. You can block direct IP address access by going to Internet Controls> Block Specific Web Categories> IP Address blocking.

4.2.6 Configure Sleep Schedule



Sleep Schedule

The group "Default" is used by default as rules of filtering for all unidentified computers.

Internet Sleep Mode allows you to put your Internet connection to sleep (disabling all Internet traffic to and from your network). This is beneficial for when the Internet doesn't need to be on or accessed.

You may put the Internet to sleep by selecting a duration and pressing the "Sleep Now" button. This will temporarily put the Internet to sleep for the duration selected. You may setup a daily schedule or an advanced schedule by which to put the Internet to sleep.You may also bypass the sleep schedule by selecting a duration and pressing the "Bypass Now" button.

Note: When the Internet is in Sleep Mode, the "Internet Sleep Mode" page will be displayed in the web browser if Internet access is attempted. To customize the message that appears on the "Internet Sleep Mode" page, click here. You may override Internet Sleep Mode and wake up your Internet connection by entering the iBoss login password into the "Internet Sleep Mode" page when it is displayed.

Bypass Internet Sleep Schedule For: 1 minute

Force Internet To Sleep For: 1 minute

Sleep Schedule:

● Disable

or

○ Sleep Daily From: 12:00 pm To: 12:30 pm

or

○ Enable using Advanced Schedule

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 47 - Configure Sleep Schedule

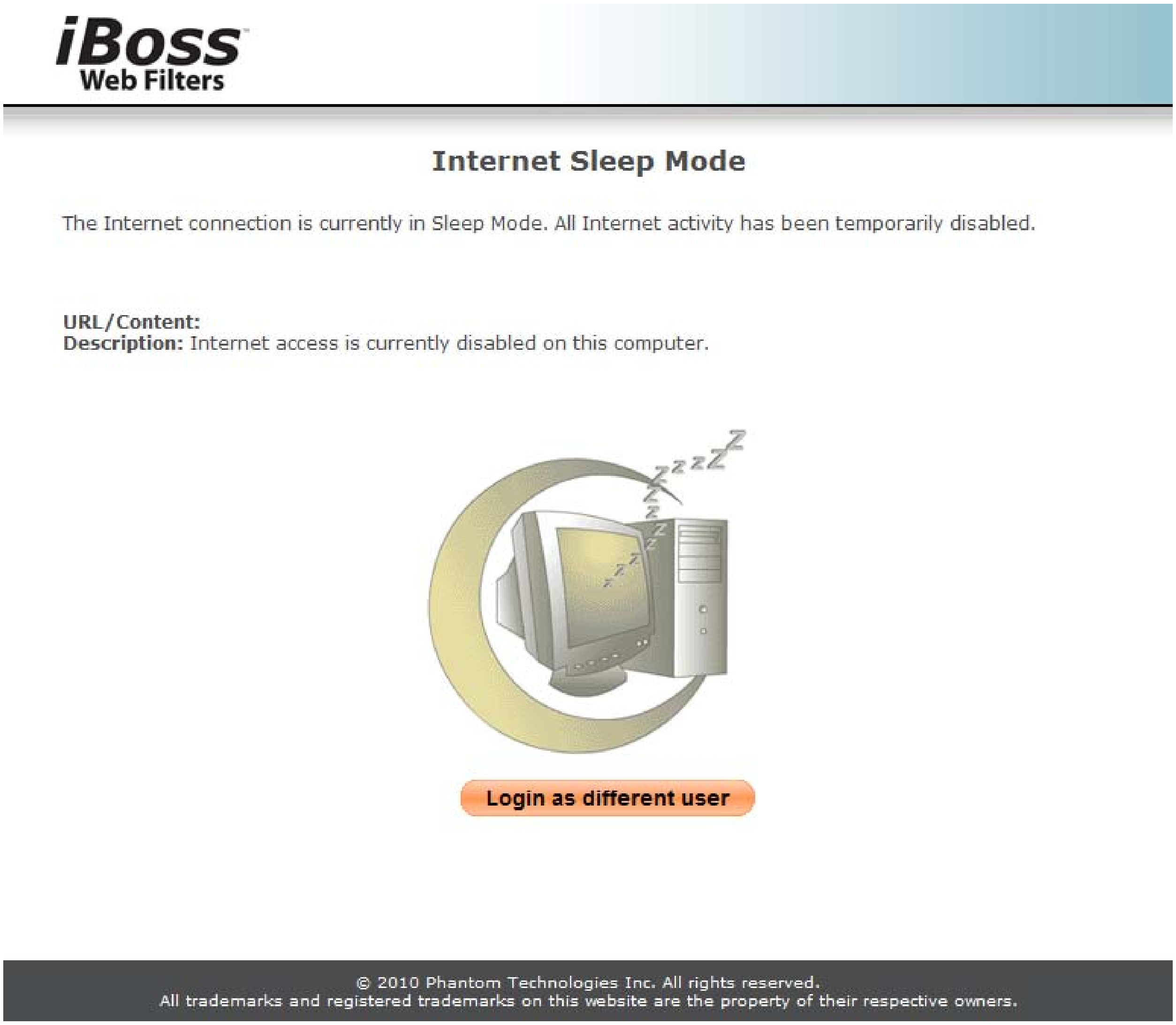
Internet Sleep Mode allows you to put your Internet connection to sleep (disabling all Internet traffic to and from your network). This is beneficial for when the Internet doesn't need to be on or accessed.

You may manually force the Internet to sleep by selecting a time period under the “**Force Internet To Sleep For:**” section and pressing the "**Sleep Now**" button. You may also bypass the sleep schedule by selecting a time period under the “**Bypass Internet Sleep Schedule For:**” section and pressing the “**Bypass Now**” button.

When manually forcing the Internet to sleep or bypassing the sleep schedule, a countdown timer will show that will allow you to cancel the forced sleep or cancel the bypass.
You may setup a daily schedule or an Advanced Schedule by which to put the Internet to sleep under the “**Sleep Schedule**” section.

When the Internet is in Sleep Mode, the "**Internet Sleep Mode**" page will be displayed in the web browser if Internet access is attempted. To customize the message that appears on the "**Internet Sleep Mode**" page, go the custom block page messages under preferences. You may override Internet Sleep Mode and wake up your Internet connection by entering the iBoss login password into the "**Internet Sleep Mode**" page if it is displayed.

4.2.6.1 Sleep Mode Page



Internet Sleep Mode

The Internet connection is currently in Sleep Mode. All Internet activity has been temporarily disabled.

URL/Content:
Description: Internet access is currently disabled on this computer.

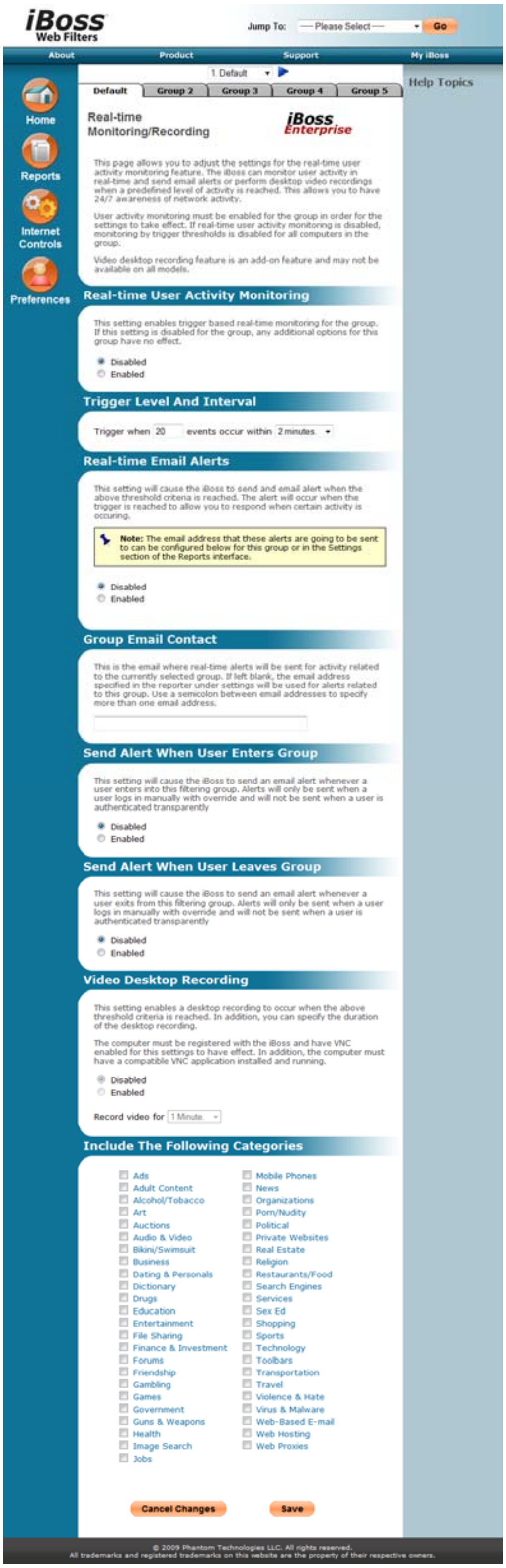
© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 48 - Internet Sleep Mode Page

When a page is blocked from violation of the iBoss sleep mode schedule, this page will show up in the web browser to the user. You may manually login and turn off Internet Sleep Mode by typing in the password and pressing Login. The Sleep Mode will continue at the next scheduled time.

If a custom message is set, this will show up above the sleeping computer.

4.2.7 Real-Time Monitoring/Recording



Real-time Monitoring/Recording

This page allows you to adjust the settings for the real-time user activity monitoring feature. The iBoss can monitor user activity in real-time and send email alerts or perform desktop video recordings when a predefined level of activity is reached. This allows you to have 24/7 awareness of network activity.

User activity monitoring must be enabled for the group in order for the settings to take effect. If real-time user activity monitoring is disabled, monitoring by trigger thresholds is disabled for all computers in the group.

Video desktop recording feature is an add-on feature and may not be available on all models.

Real-time User Activity Monitoring

This setting enables trigger based real-time monitoring for the group. If this setting is disabled for the group, any additional options for this group have no effect.

● Disabled
○ Enabled

Trigger Level And Interval

Trigger when 20 events occur within 2 minutes.

Real-time Email Alerts

This setting will cause the iBoss to send and email alert when the above threshold criteria is reached. The alert will occur when the trigger is reached to allow you to respond when certain activity is occuring.

Note: The email address that these alerts are going to be sent to can be configured below for this group or in the Settings section of the Reports interface.

● Disabled
○ Enabled

Group Email Contact

This is the email where real-time alerts will be sent for activity related to the currently selected group. If left blank, the email address specified in the reporter under settings will be used for alerts related to this group. Use a semicolon between email addresses to specify more than one email address.

Send Alert When User Enters Group

This setting will cause the iBoss to send an email alert whenever a user enters into this filtering group. Alerts will only be sent when a user logs in manually with override and will not be sent when a user is authenticated transparently

● Disabled
○ Enabled

Send Alert When User Leaves Group

This setting will cause the iBoss to send an email alert whenever a user exits from this filtering group. Alerts will only be sent when a user logs in manually with override and will not be sent when a user is authenticated transparently

● Disabled
○ Enabled

Video Desktop Recording

This setting enables a desktop recording to occur when the above threshold criteria is reached. In addition, you can specify the duration of the desktop recording.

The computer must be registered with the iBoss and have VNC enabled for this settings to have effect. In addition, the computer must have a compatible VNC application installed and running.

● Disabled
○ Enabled

Record video for 1 Minute.

Include The Following Categories

□ Ads
□ Adult Content
□ Alcohol/Tobacco
□ Art
□ Auctions
□ Audio & Video
□ Bikini/Swimsuit
□ Business
□ Dating & Personals
□ Dictionary
□ Drugs
□ Education
□ Entertainment
□ File Sharing
□ Finance & Investment
□ Forums
□ Friendship
□ Gambling
□ Games
□ Government
□ Guns & Weapons
□ Health
□ Image Search
□ Jobs
□ Mobile Phones
□ News
□ Organizations
□ Porn/Nudity
□ Political
□ Private Websites
□ Real Estate
□ Religion
□ Restaurants/Food
□ Search Engines
□ Services
□ Sex Ed
□ Shopping
□ Sports
□ Technology
□ Toolbars
□ Transportation
□ Travel
□ Violence & Hate
□ Virus & Malware
□ Web-Based E-mail
□ Web Hosting
□ Web Proxies

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 49 - Real-time Monitoring/Recording

* The VNC recording feature is not included by default. It is a feature add-on upgrade.

This feature allows you to adjust the settings for the real-time user activity monitoring feature. The iBoss can monitor user activity in real-time and send email alerts or perform desktop video recordings when a predefined level of activity is reached. This allows you to have 24/7 awareness of network activity.

User activity monitoring must be enabled for the group in order for the settings to take effect. If real-time user activity monitoring is disabled, monitoring by trigger thresholds is disabled for all computers in the group.

Video desktop recording feature is an add-on feature and may not be available on all models.

Real-time User Activity Monitoring – This setting enables trigger based real-time monitoring for the group. If this setting is disabled for the group, any additional options for this group have no effect.

Trigger Level And Interval - Trigger when specified number of events occur within a chosen time period.

Real-time Email Alerts - This setting will cause the iBoss to send and email alert when the above threshold criteria is reached. The alert will occur when the trigger is reached to allow you to respond when certain activity is occurring.

Note: The email address that these alerts are going to be sent to can be configured below for this group or in the Settings section of the Reports interface.

Group Email Contact - This is the email where real-time alerts will be sent for activity related to the currently selected group. If left blank, the email address specified in the reporter under settings will be used for alerts related to this group. Use a semicolon between email addresses to specify more than one email address.

Send Alert When User Enters Group - This setting will cause the iBoss to send an email alert whenever a user enters into this filtering group. Alerts will only be sent when a user logs in manually with override and will not be sent when a user is authenticated transparently

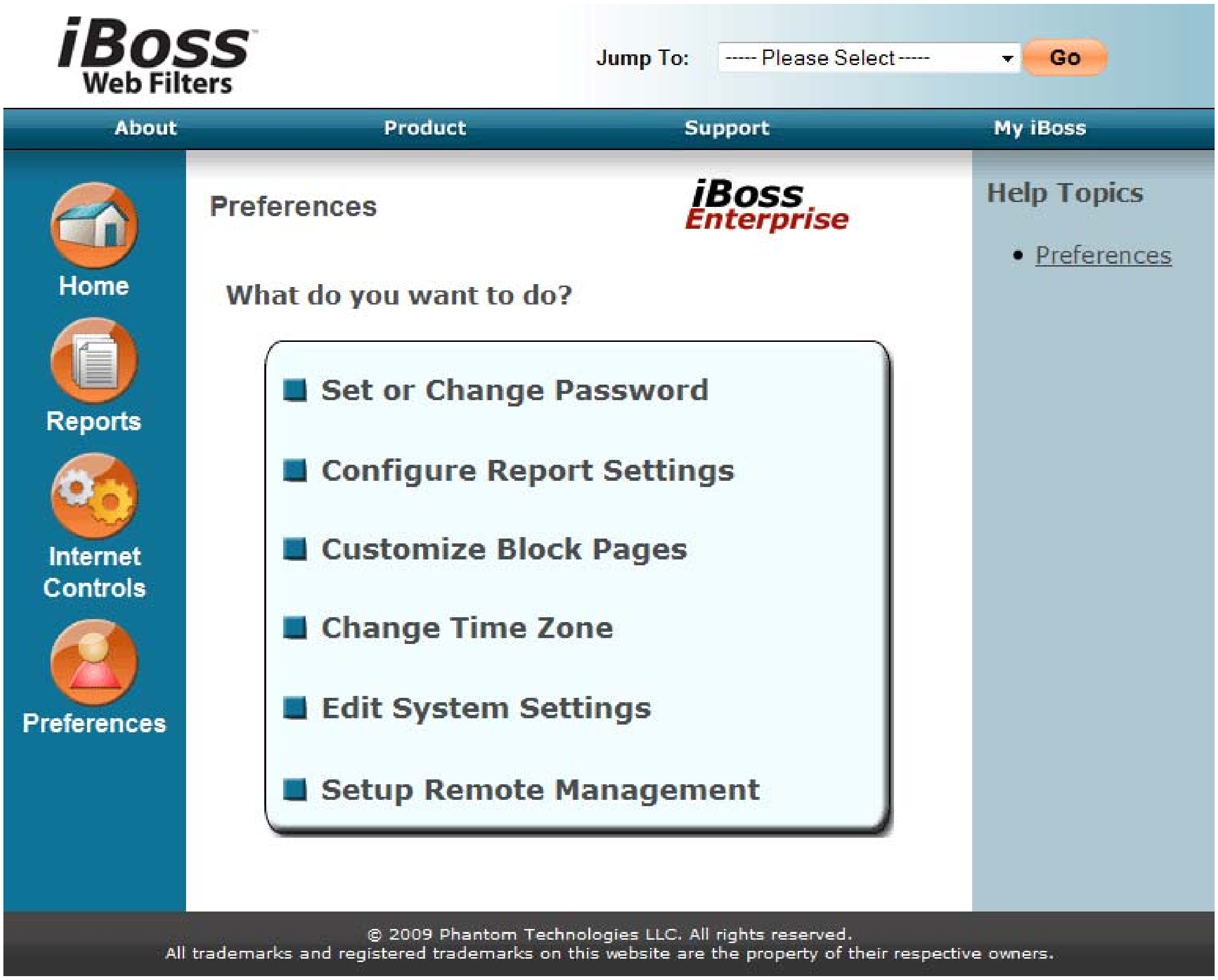
Send Alert When User Leaves Group - This setting will cause the iBoss to send an email alert whenever a user exits from this filtering group. Alerts will only be sent when a user logs in manually with override and will not be sent when a user is authenticated transparently

Video Desktop Recording - This setting enables a desktop recording to occur when the above threshold criteria is reached. In addition, you can specify the duration of the desktop recording.

The computer must be registered with the iBoss and have VNC enabled for this settings to have effect. In addition, the computer must have a compatible VNC application installed and running. This is where you set the option on how long to record the video for.

Include The Following Categories – This is the categories you choose to include in the trigger thresholds.

4.3 Edit My Preferences



Preferences

What do you want to do?

- Set or Change Password
- Configure Report Settings
- Customize Block Pages
- Change Time Zone
- Edit System Settings
- Setup Remote Management

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 50 - Edit My Preferences

The " **Preferences**" menu allows you to choose options for configuring the current preferences of the iBoss. These are the options to choose from: Set or Change Password, Configure Report Settings, Customize Block Pages, Change My Time Zone, Edit System Settings, and Setup Remote Management.

Set or Change Password - This option allows you to set or change the admin password used for logging into your iBoss device.

Setup Report Settings - This option allows you to setup report settings for report manager.

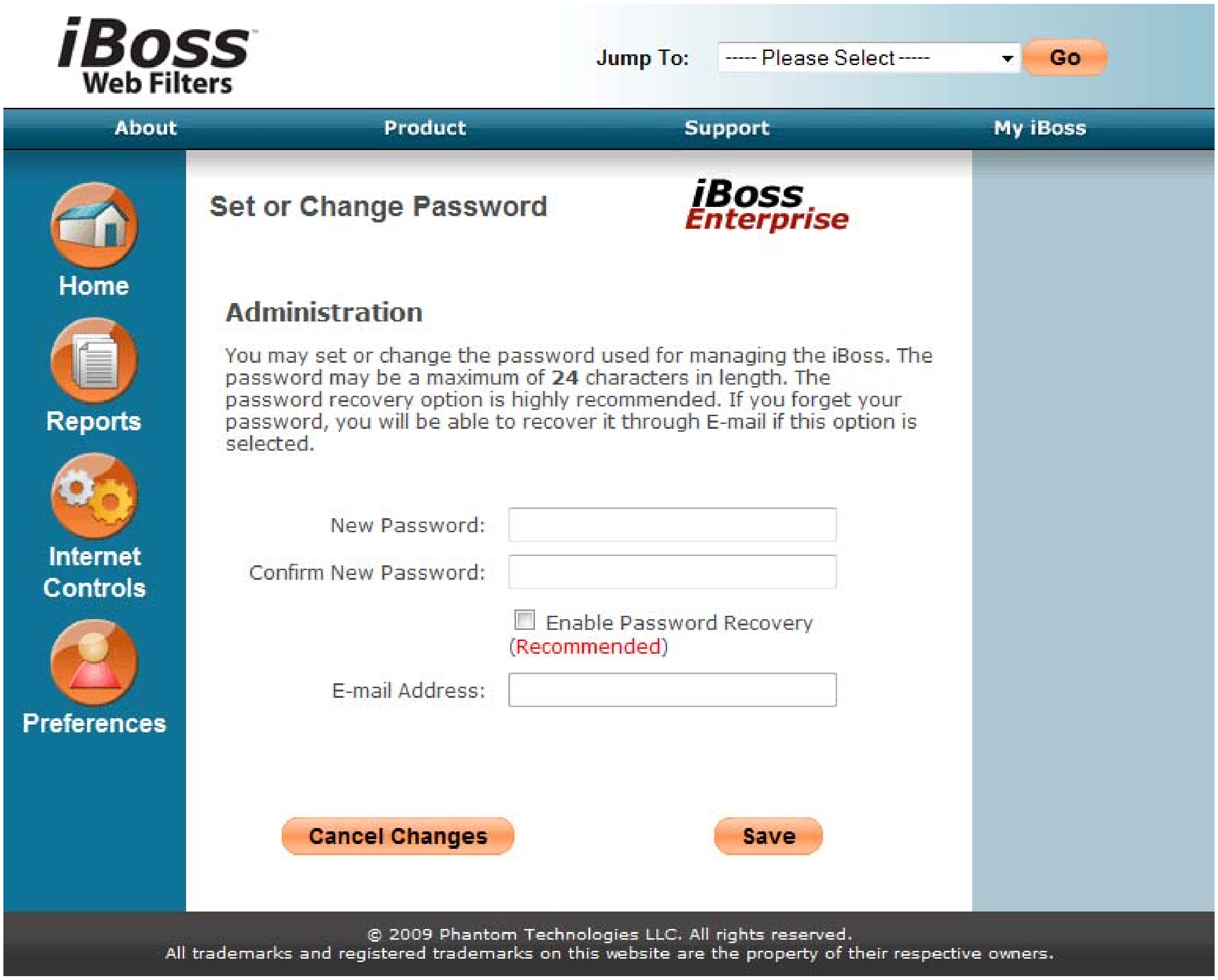
Customize Block Pages - This option allows you to customize the blocked pages.

Change Time Zone - This option allows you to change your current time zone. This option is important for your logs and schedules to work accurately.

Edit System Settings - This option allows you to change system settings.

Setup Remote Management - This option allows you to setup Remote Management.

4.3.1 Set or Change Password



Set or Change Password

Administration

You may set or change the password used for managing the iBoss. The password may be a maximum of **24** characters in length. The password recovery option is highly recommended. If you forget your password, you will be able to recover it through E-mail if this option is selected.

New Password:

Confirm New Password:

□ Enable Password Recovery (Recommended)

E-mail Address:

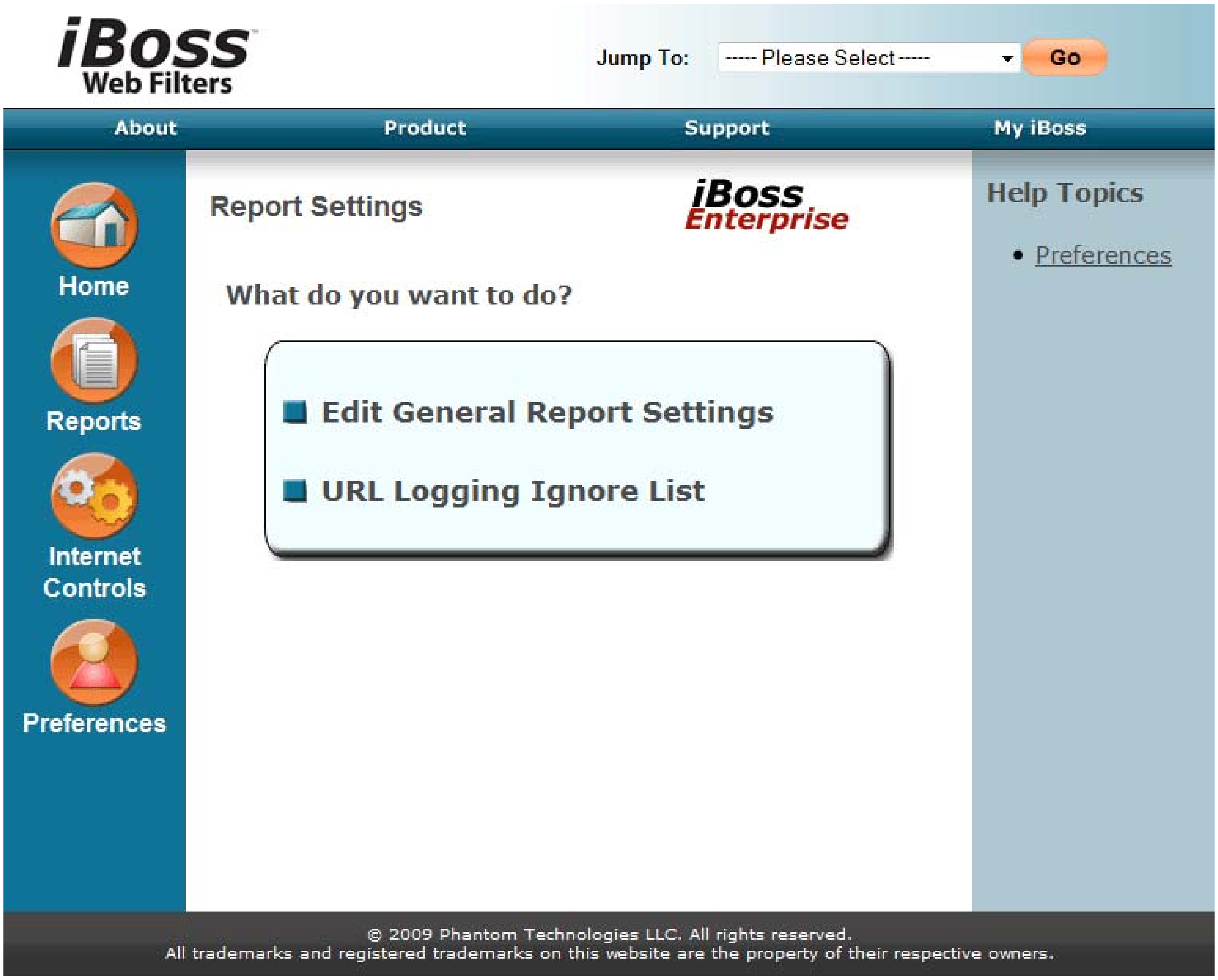
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 51 - Set or Change My Password

You may set or change the password used for managing the iBoss. The password may be a maximum of 24 characters in length. The password recovery option is if your password becomes lost, you will be able to recover it through e-mail if this option is selected.

Note: Be very careful with this password. It is used for configuration for your iBoss and for override functions.

4.3.2 Configure Report Settings


iBoss Web Filters
Jump To:
----- Please Select -----
Go
About
Product
Support
My iBoss
Home
Reports
Internet Controls
Preferences
iBoss Enterprise
Help Topics
Preferences
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Report Settings

What do you want to do?

- Edit General Report Settings
- URL Logging Ignore List

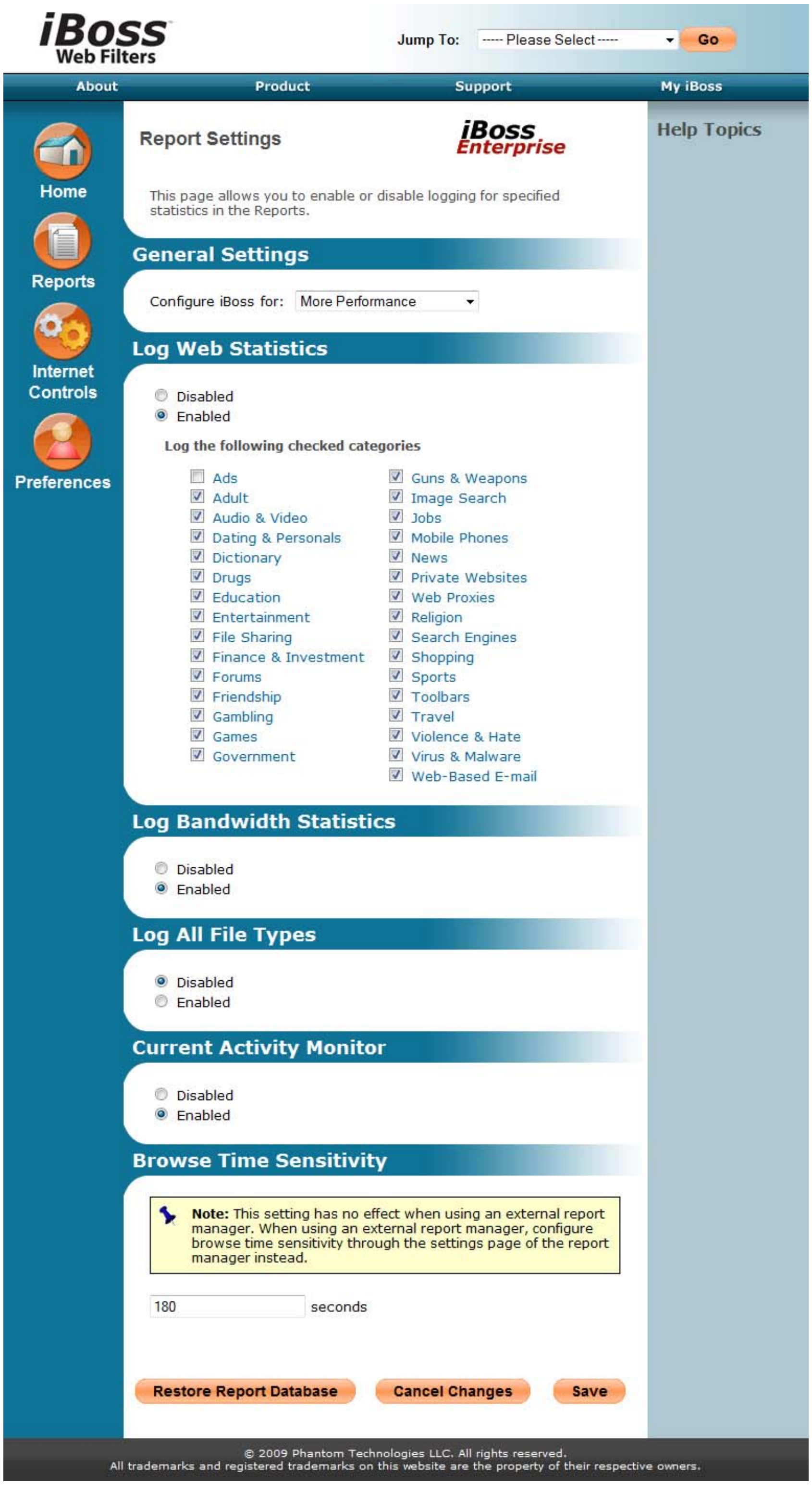
Figure 52 - Configure Report Settings

The "**Report Settings**" menu allows you to choose options for configuring the report manager of the iBoss. There are *three options to choose from: Edit General Report Settings, URL Logging Ignore List, *and Video Recording Settings (Feature Addition Upgrade).

Edit General Report Settings - This option allows you to enable or disable logging for specified statistics in the Reports.

URL Logging Ignore List - This option allows you to add domains which you do not wish to log to the iBoss Reports database.

4.3.2.1 Edit General Report Settings



Report Settings

This page allows you to enable or disable logging for specified statistics in the Reports.

General Settings

Configure iBoss for: More Performance

Log Web Statistics

○ Disabled
● Enabled

Log the following checked categories

□ Ads
☑ Adult
☑ Audio & Video
☑ Dating & Personals
☑ Dictionary
☑ Drugs
☑ Education
☑ Entertainment
☑ File Sharing
☑ Finance & Investment
☑ Forums
☑ Friendship
☑ Gambling
☑ Games
☑ Government
☑ Guns & Weapons
☑ Image Search
☑ Jobs
☑ Mobile Phones
☑ News
☑ Private Websites
☑ Web Proxies
☑ Religion
☑ Search Engines
☑ Shopping
☑ Sports
☑ Toolbars
☑ Travel
☑ Violence & Hate
☑ Virus & Malware
☑ Web-Based E-mail

Log Bandwidth Statistics

○ Disabled
● Enabled

Log All File Types

● Disabled
○ Enabled

Current Activity Monitor

○ Disabled
● Enabled

Browse Time Sensitivity

Note: This setting has no effect when using an external report manager. When using an external report manager, configure browse time sensitivity through the settings page of the report manager instead.

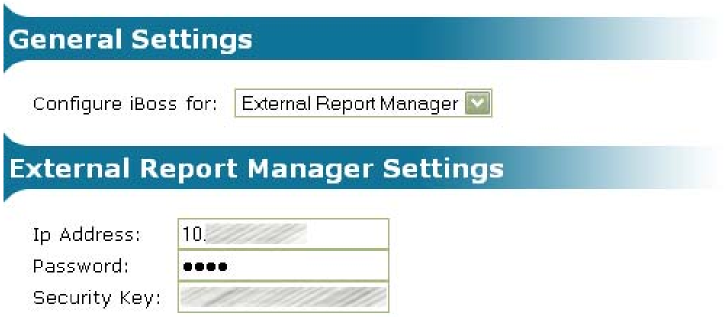
180 seconds

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 53 - Edit General Report Settings

These report settings are for the Report Manager.

Performance Settings – You may choose between More Logging, More Performance, and External Report Manager. This will set the logging settings for you. Some of the settings may disappear depending on which setting you select. It is recommended to use More Performance if you do not have an External Report Manager. If you have an External Report Manager, please choose External Report manager and refer to the following:



General Settings

Configure iBoss for: External Report Manager

External Report Manager Settings

Ip Address: 10.[redacted]
Password: ●●●●
Security Key: [redacted]

Figure 54 - External Report Manager Settings

* This feature is only available with the Enterprise Reporter Appliance.

External Report Manager Settings (only when External Report Manager is selected; must have an external report manager for this to work) – This option will show if you select External Report Manager selected as your performance settings. This setting should only be selected if you have the External Enterprise Reporter. This allows you to set the IP address for the External Report Manager, the Report Manager Database Password, and the Security Key. Please refer to the External Report Manager section for information on where to get these settings from.

Log Web Statistics (only when More logging is selected) – This allows you to enable or disable logging for web statistics. You may choose from the different categories to log.

Log Port Statistics (only when More logging is selected) – This allows you to enable or disable port statistics.

Log IP Address Access Statistics (only when More logging is selected) – This allows you to enable or disable IP Address statistics.

Log Bandwidth Category Statistics (only when More logging is selected) – This allows you to enable or disable bandwidth category statistics.

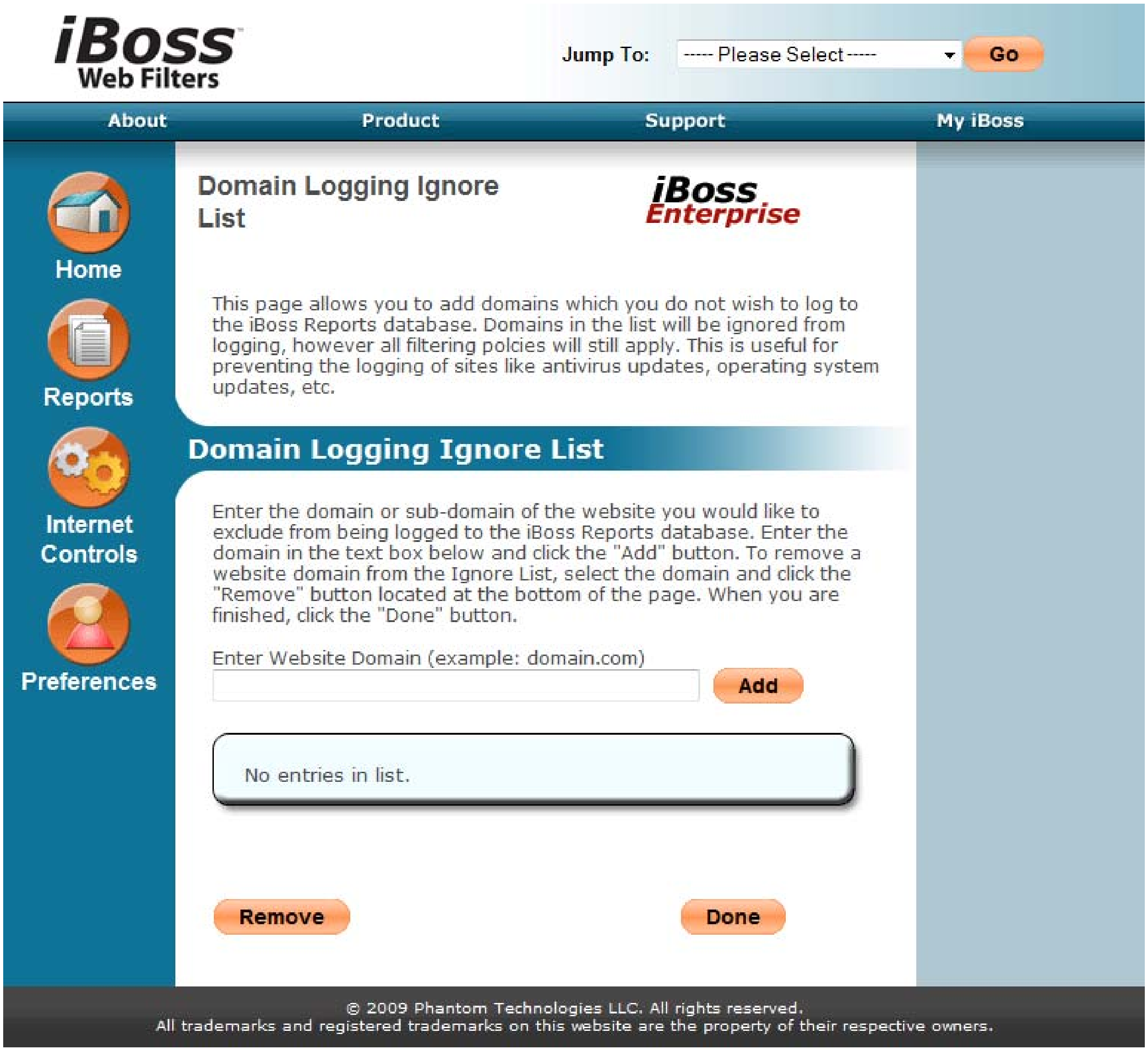
Log Application Statistics (only when More logging is selected) – This allows you to enable or disable application statistics.

Current Activity Monitory (only when More logging is selected) – This allows you to enable or disable the current activity monitor.

IP Address Name Resolution (only when More logging is selected) – This allows you to enable or disable the IP Address Name Resolution.

Bandwidth Logging - This allows you to enable or disable bandwidth logging.

4.3.2.2 URL Logging Ignore List



Domain Logging Ignore List

This page allows you to add domains which you do not wish to log to the iBoss Reports database. Domains in the list will be ignored from logging, however all filtering polcies will still apply. This is useful for preventing the logging of sites like antivirus updates, operating system updates, etc.

Domain Logging Ignore List

Enter the domain or sub-domain of the website you would like to exclude from being logged to the iBoss Reports database. Enter the domain in the text box below and click the "Add" button. To remove a website domain from the Ignore List, select the domain and click the "Remove" button located at the bottom of the page. When you are finished, click the "Done" button.

Enter Website Domain (example: domain.com)

No entries in list.

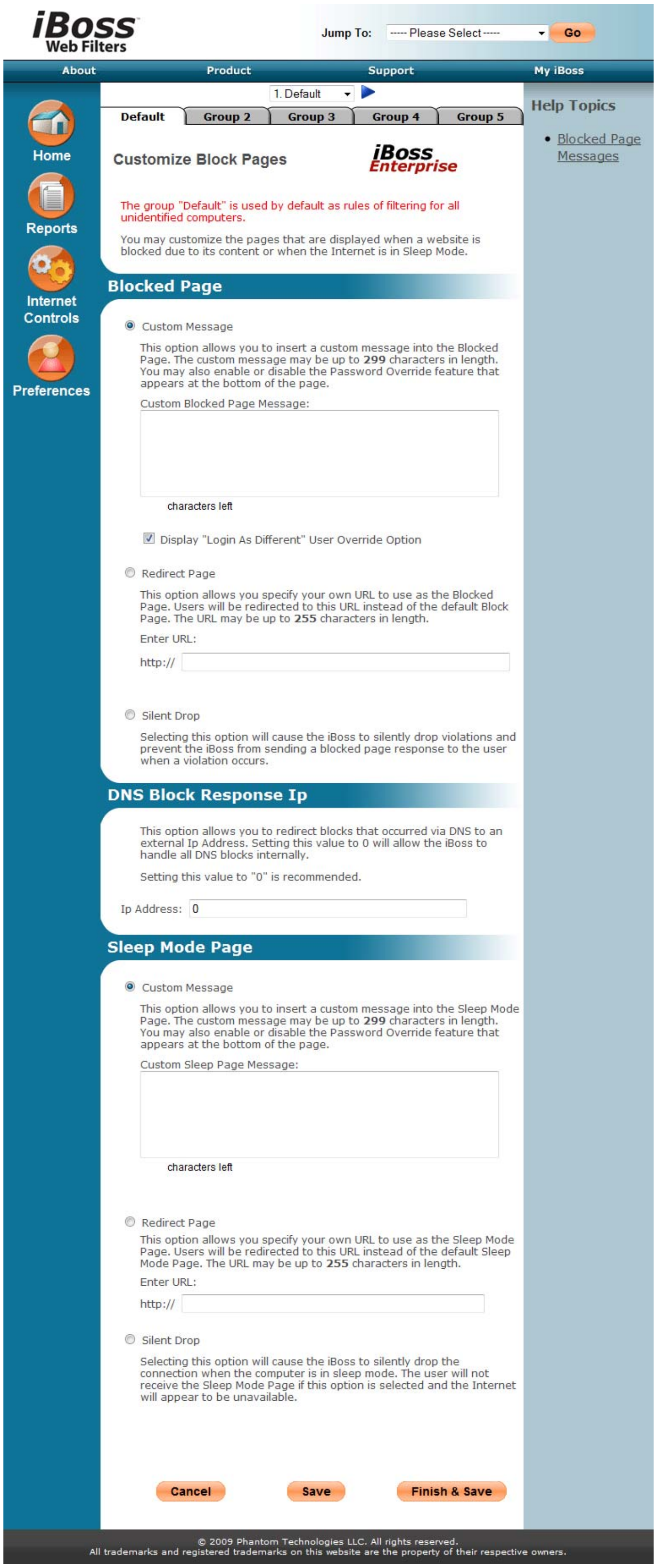
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 55 - URL Logging Ignore List

This page allows you to add domains which you do not wish to log to the iBoss Reports database. Domains in the list will be ignored from logging, however all filtering policies will still apply. This is useful for preventing the logging of sites like antivirus updates, operating system updates, etc.

Enter the domain or sub-domain of the website you would like to exclude from being logged to the iBoss Reports database. Enter the domain in the text box below and click the "**Add**" button. To remove a website domain from the Ignore List, select the domain and click the "**Remove**" button located at the bottom of the page. When you are finished, click the "**Done**" button.

4.3.3 Customize Block Pages



Customize Block Pages

The group "Default" is used by default as rules of filtering for all unidentified computers.

You may customize the pages that are displayed when a website is blocked due to its content or when the Internet is in Sleep Mode.

Blocked Page

● Custom Message

This option allows you to insert a custom message into the Blocked Page. The custom message may be up to **299** characters in length. You may also enable or disable the Password Override feature that appears at the bottom of the page.

Custom Blocked Page Message:

characters left

☑ Display "Login As Different" User Override Option

○ Redirect Page

This option allows you specify your own URL to use as the Blocked Page. Users will be redirected to this URL instead of the default Block Page. The URL may be up to **255** characters in length.

Enter URL:

http://

○ Silent Drop

Selecting this option will cause the iBoss to silently drop violations and prevent the iBoss from sending a blocked page response to the user when a violation occurs.

DNS Block Response Ip

This option allows you to redirect blocks that occurred via DNS to an external Ip Address. Setting this value to 0 will allow the iBoss to handle all DNS blocks internally.

Setting this value to "0" is recommended.

Ip Address: 0

Sleep Mode Page

● Custom Message

This option allows you to insert a custom message into the Sleep Mode Page. The custom message may be up to **299** characters in length. You may also enable or disable the Password Override feature that appears at the bottom of the page.

Custom Sleep Page Message:

characters left

○ Redirect Page

This option allows you specify your own URL to use as the Sleep Mode Page. Users will be redirected to this URL instead of the default Sleep Mode Page. The URL may be up to **255** characters in length.

Enter URL:

http://

○ Silent Drop

Selecting this option will cause the iBoss to silently drop the connection when the computer is in sleep mode. The user will not receive the Sleep Mode Page if this option is selected and the Internet will appear to be unavailable.

Figure 56 - Customize Block Pages

You may customize the pages that are displayed when a website is blocked due to its content or when the Internet is in Sleep Mode.

Blocked Page Custom Message - This option allows you to insert a custom message into the Blocked Page. The custom message may be up to 299 characters in length. You may also enable or disable the Password Override feature that appears at the bottom of the page.

Blocked Page Redirect Page - This option allows you specify your own URL to use as the Blocked Page. Users will be redirected to this URL instead of the default Block Page. The URL may be up to 255 characters in length.

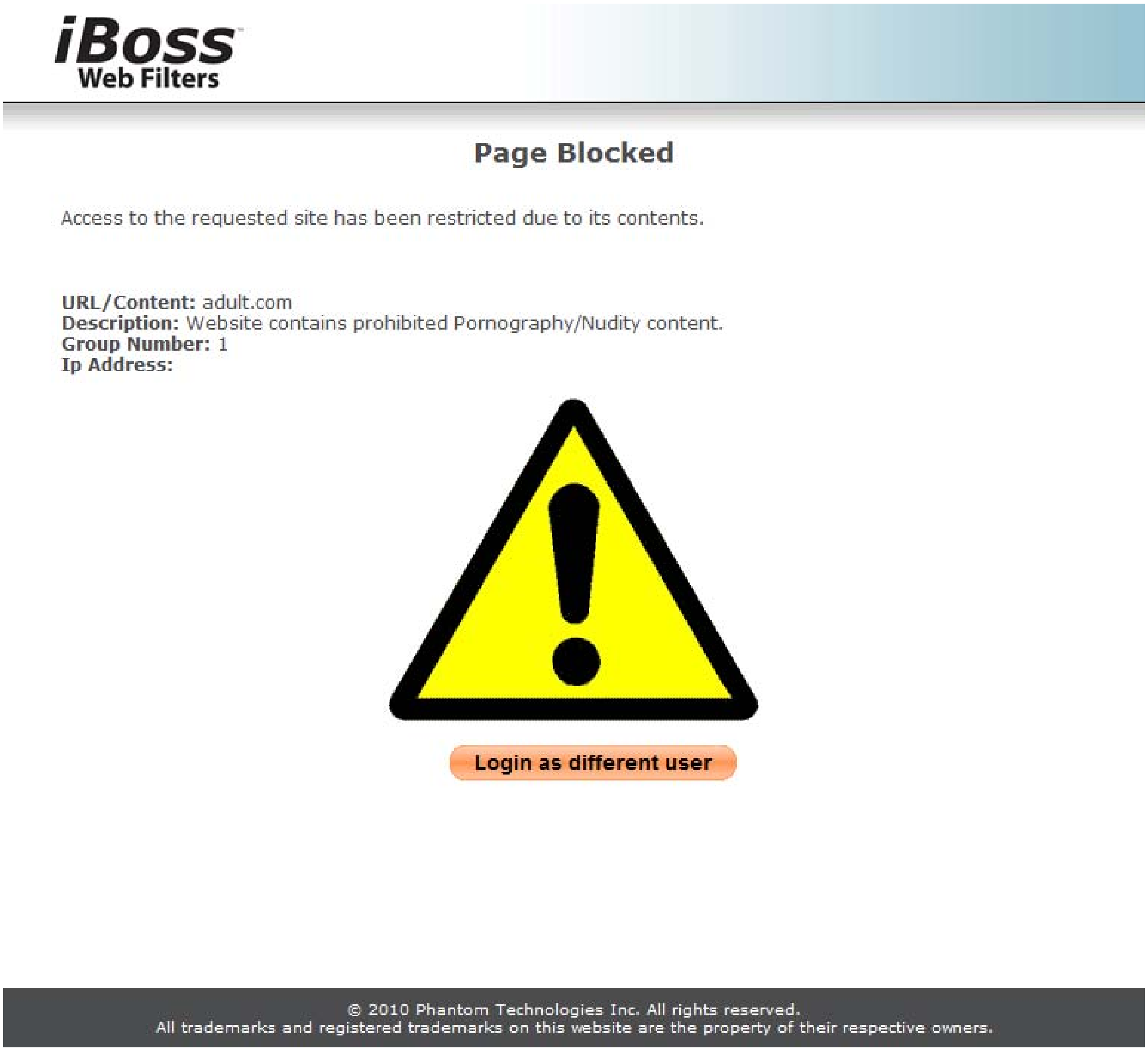
Blocked Page Silent Drop - Selecting this option will cause the iBoss to silently drop violations and prevent the iBoss from sending a blocked page response to the user when a violation occurs.

Sleep Mode Custom Message - This option allows you to insert a custom message into the Sleep Mode Page. The custom message may be up to 299 characters in length. You may also enable or disable the Password Override feature that appears at the bottom of the page.

Sleep Mode Redirect Page - This option allows you specify your own URL to use as the Sleep Mode Page. Users will be redirected to this URL instead of the default Sleep Mode Page. The URL may be up to 255 characters in length.

Sleep Mode Silent Drop - Selecting this option will cause the iBoss to silently drop the connection when the computer is in sleep mode. The user will not receive the Sleep Mode Page if this option is selected and the Internet will appear to be unavailable.

4.3.3.1 Blocked Page



Page Blocked

Access to the requested site has been restricted due to its contents.

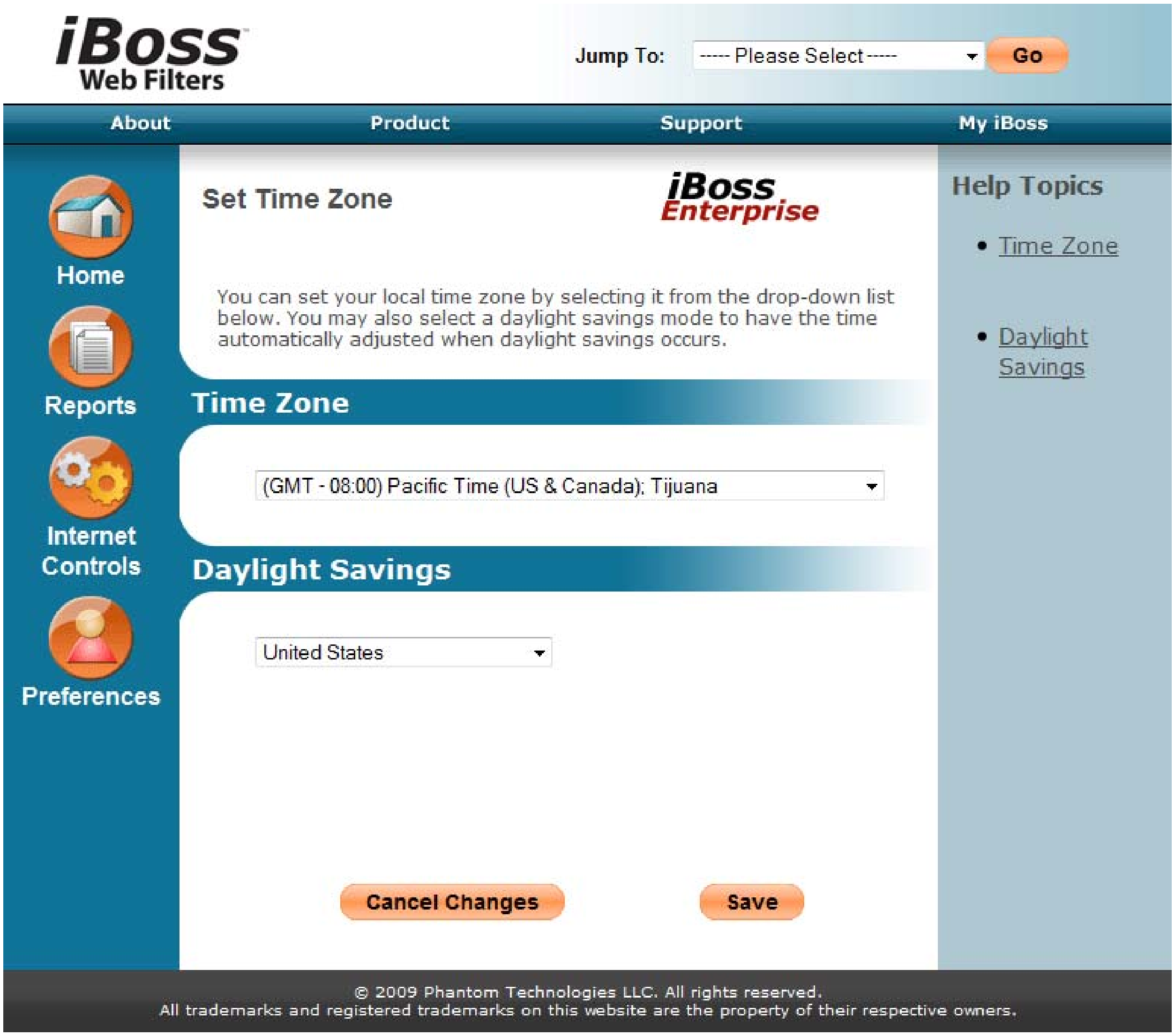
URL/Content: adult.com
Description: Website contains prohibited Pornography/Nudity content.
Group Number: 1
Ip Address:

© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 57 - iBoss Blocked Page

When a page is blocked from violation of the iBoss settings, this page will show up in the web browser to the user. You may manually login and add sites to the allowlist if you feel that you have received the blocked page in error by typing in the password and pressing Login. If a custom message is set, this will show up above the exclamation point.

4.3.4 Change Time Zone



Set Time Zone

You can set your local time zone by selecting it from the drop-down list below. You may also select a daylight savings mode to have the time automatically adjusted when daylight savings occurs.

Time Zone

(GMT - 08:00) Pacific Time (US & Canada); Tijuana

Daylight Savings

United States

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

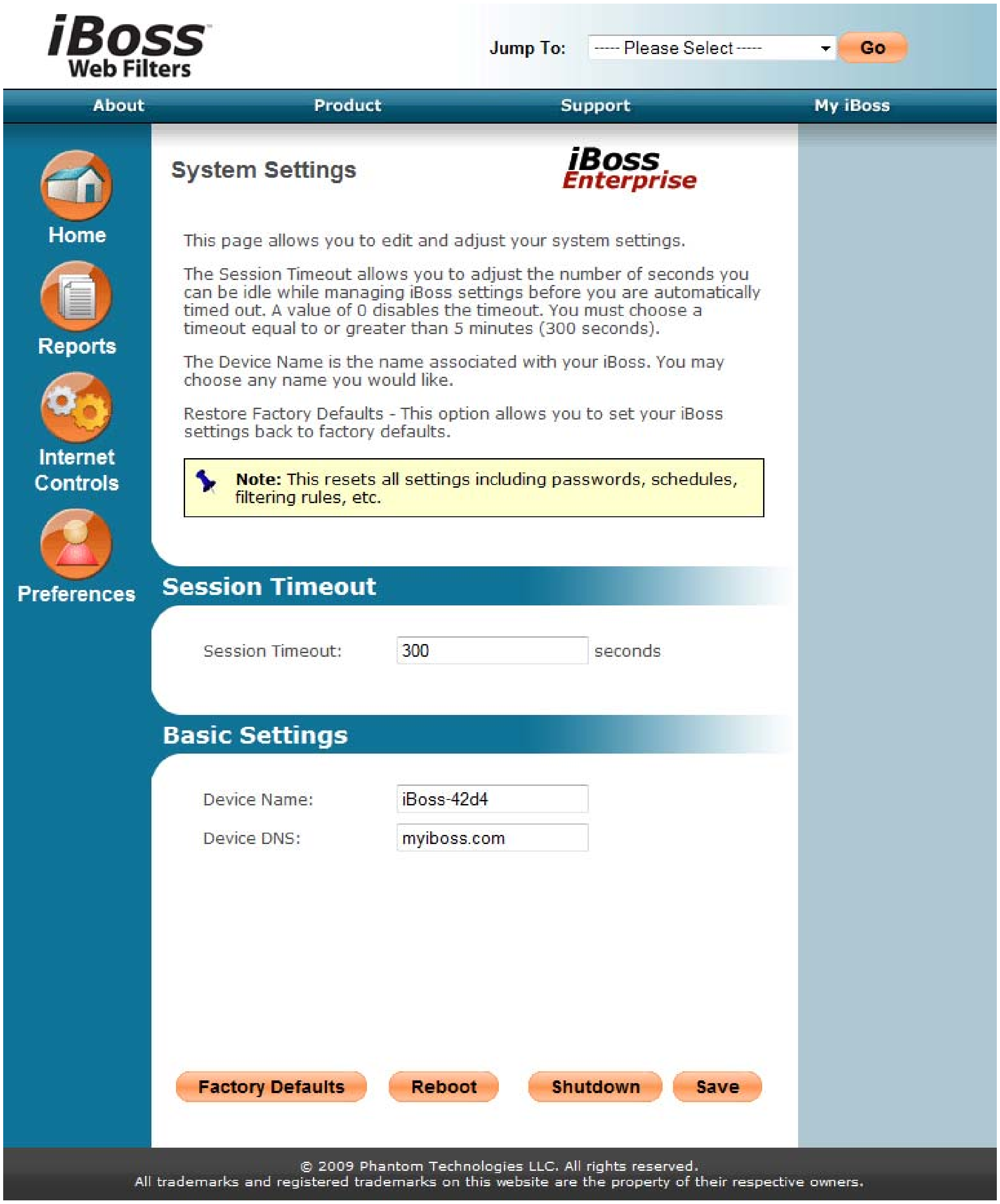
Figure 58 - Set Time Zone

The "Time Zone" page allows you to edit your current time zone settings and enable daylight savings.

Time Zone - This option allows you to set your local time zone. This is important for the logging and scheduling to work accurately.

Daylight Savings - This option allows you to setup daylight savings time for your local time zone setting.

4.3.5 Edit System Settings



System Settings

This page allows you to edit and adjust your system settings.

The Session Timeout allows you to adjust the number of seconds you can be idle while managing iBoss settings before you are automatically timed out. A value of 0 disables the timeout. You must choose a timeout equal to or greater than 5 minutes (300 seconds).

The Device Name is the name associated with your iBoss. You may choose any name you would like.

Restore Factory Defaults - This option allows you to set your iBoss settings back to factory defaults.

Note: This resets all settings including passwords, schedules, filtering rules, etc.

Session Timeout

Session Timeout: 300 seconds

Basic Settings

Device Name: iBoss-42d4

Device DNS: myiboss.com

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

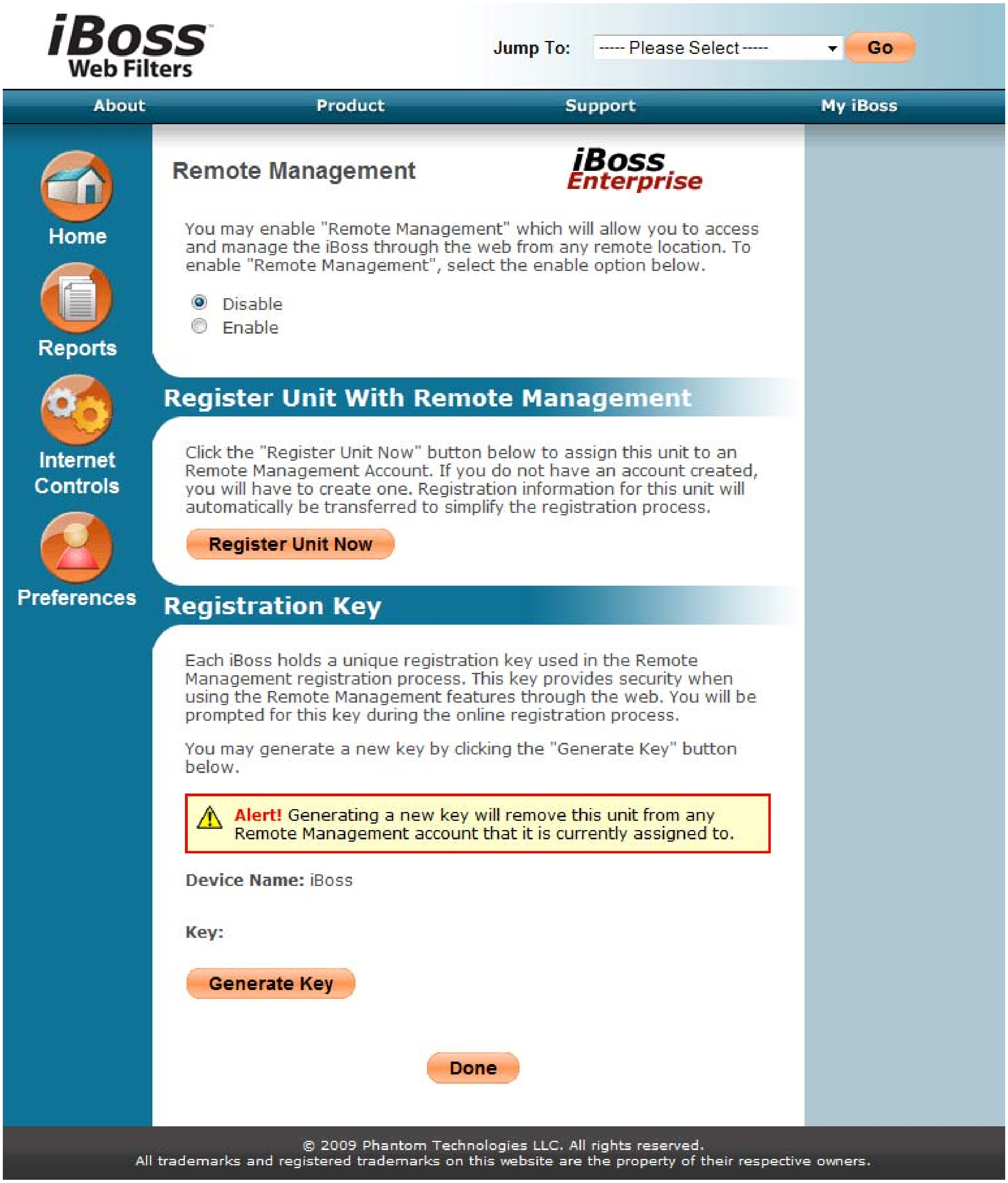
Figure 59 - Edit System Settings

The "Edit System Settings" page allows you to edit your device name of your iBoss.

Restore Factory Defaults - This option allows you to set your iBoss settings back to factory defaults.

You may also choose to Reboot & Shutdown the device from this page.

4.3.6 Setup Remote Management



Remote Management

You may enable "Remote Management" which will allow you to access and manage the iBoss through the web from any remote location. To enable "Remote Management", select the enable option below.

● Disable
○ Enable

Register Unit With Remote Management

Click the "Register Unit Now" button below to assign this unit to an Remote Management Account. If you do not have an account created, you will have to create one. Registration information for this unit will automatically be transferred to simplify the registration process.

Registration Key

Each iBoss holds a unique registration key used in the Remote Management registration process. This key provides security when using the Remote Management features through the web. You will be prompted for this key during the online registration process.

You may generate a new key by clicking the "Generate Key" button below.

⚠ **Alert!** Generating a new key will remove this unit from any Remote Management account that it is currently assigned to.

Device Name: iBoss

Key:

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 60 - Setup Remote Management

You may enable "**Remote Management**" which will allow you to access and manage the iBoss through the web from any remote location. To enable "**Remote Management**", select the enable.

Register Unit Now - Click the "**Register Unit Now**" button below to assign this unit to a Remote Management Account. If you do not have a Remote Management Account created, you will have to create one. Registration information for this unit will automatically be transferred to simplify the registration process.

Registration Key - Each iBoss holds a unique registration key used in the Remote Management registration process. This key provides security when using the Remote Management features through the web. You will be prompted for this key during the online registration process.

You may generate a new key by clicking the "**Generate Key**" button below.

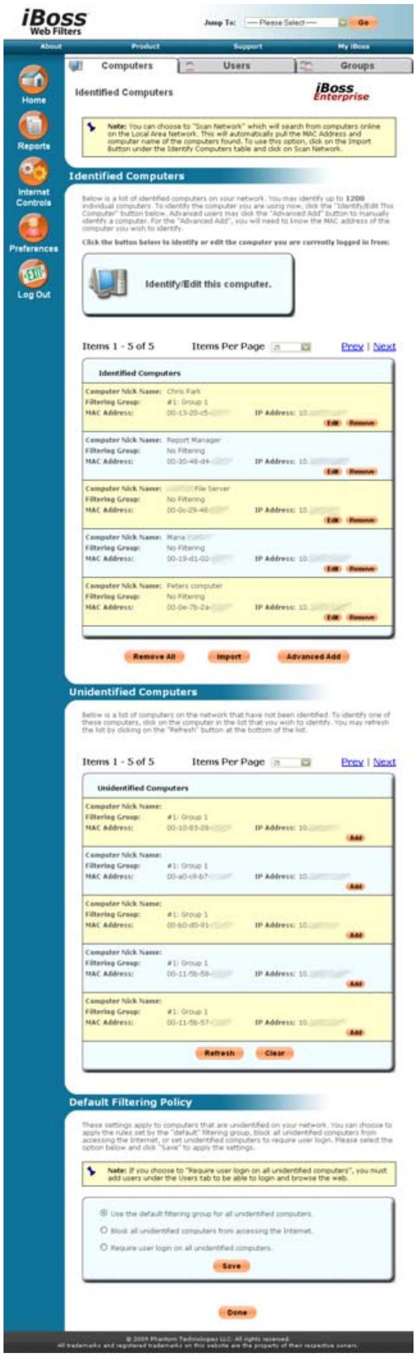
Important Note: Generating a new key will remove this unit from any Remote Management account that it is currently assigned to.

4.4 Identify Computers & Users

Figure 61 - Identify Computers & Users

The Identify Computers & Users has tabs at the top to switch from identified computers, added user accounts, and groups.

4.4.1 Identify Computers



Identified Computers

Note: You can choose to "Scan Network" which will search from computers online on the Local Area Network. This will automatically pull the MAC Address and computer name of the computers found. To use this option, click on the Import Button under the Identify Computers table and click on Scan Network.

Identified Computers

Below is a list of identified computers on your network. You may identify up to **1200** individual computers. To identify the computer you are using now, click the "Identify/Edit This Computer" button below. Advanced users may click the "Advanced Add" button to manually identify a computer. For the "Advanced Add", you will need to know the MAC address of the computer you wish to identify.

Click the button below to identify or edit the computer you are currently logged in from:

Identify/Edit this computer.

Items 1 - 5 of 5   Items Per Page 25   Prev | Next

Identified Computers

Computer Nick Name: Chris Fark
Filtering Group: #1: Group 1
MAC Address: 00-13-20-c5-[redacted]   **IP Address:** 10.[redacted]
Edit   Remove

Computer Nick Name: Report Manager
Filtering Group: No Filtering
MAC Address: 00-30-48-d4-[redacted]   **IP Address:** 10.[redacted]
Edit   Remove

Computer Nick Name: [redacted] File Server
Filtering Group: No Filtering
MAC Address: 00-0c-29-48-[redacted]   **IP Address:** 10.[redacted]
Edit   Remove

Computer Nick Name: Maria [redacted]
Filtering Group: No Filtering
MAC Address: 00-19-d1-02-[redacted]   **IP Address:** 10.[redacted]
Edit   Remove

Computer Nick Name: Peters computer
Filtering Group: No Filtering
MAC Address: 00-0e-7b-2a-[redacted]   **IP Address:** 10.[redacted]
Edit   Remove

Remove All   Import   Advanced Add

Unidentified Computers

Below is a list of computers on the network that have not been identified. To identify one of these computers, click on the computer in the list that you wish to identify. You may refresh the list by clicking on the "Refresh" button at the bottom of the list.

Items 1 - 5 of 5   Items Per Page 25   Prev | Next

Unidentified Computers

Computer Nick Name:
Filtering Group: #1: Group 1
MAC Address: 00-10-83-29-[redacted]   **IP Address:** 10.[redacted]
Add

Computer Nick Name:
Filtering Group: #1: Group 1
MAC Address: 00-a0-c9-b7-[redacted]   **IP Address:** 10.[redacted]
Add

Computer Nick Name:
Filtering Group: #1: Group 1
MAC Address: 00-60-d0-91-[redacted]   **IP Address:** 10.[redacted]
Add

Computer Nick Name:
Filtering Group: #1: Group 1
MAC Address: 00-11-5b-58-[redacted]   **IP Address:** 10.[redacted]
Add

Computer Nick Name:
Filtering Group: #1: Group 1
MAC Address: 00-11-5b-57-[redacted]   **IP Address:** 10.[redacted]
Add

Refresh   Clear

Default Filtering Policy

These settings apply to computers that are unidentified on your network. You can choose to apply the rules set by the "default" filtering group, block all unidentified computers from accessing the Internet, or set unidentified computers to require user login. Please select the option below and click "Save" to apply the settings.

Note: If you choose to "Require user login on all unidentified computers", you must add users under the Users tab to be able to login and browse the web.

● Use the default filtering group for all unidentified computers.
○ Block all unidentified computers from accessing the Internet.
○ Require user login on all unidentified computers.

Save

Done

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 62 - Identify Computers

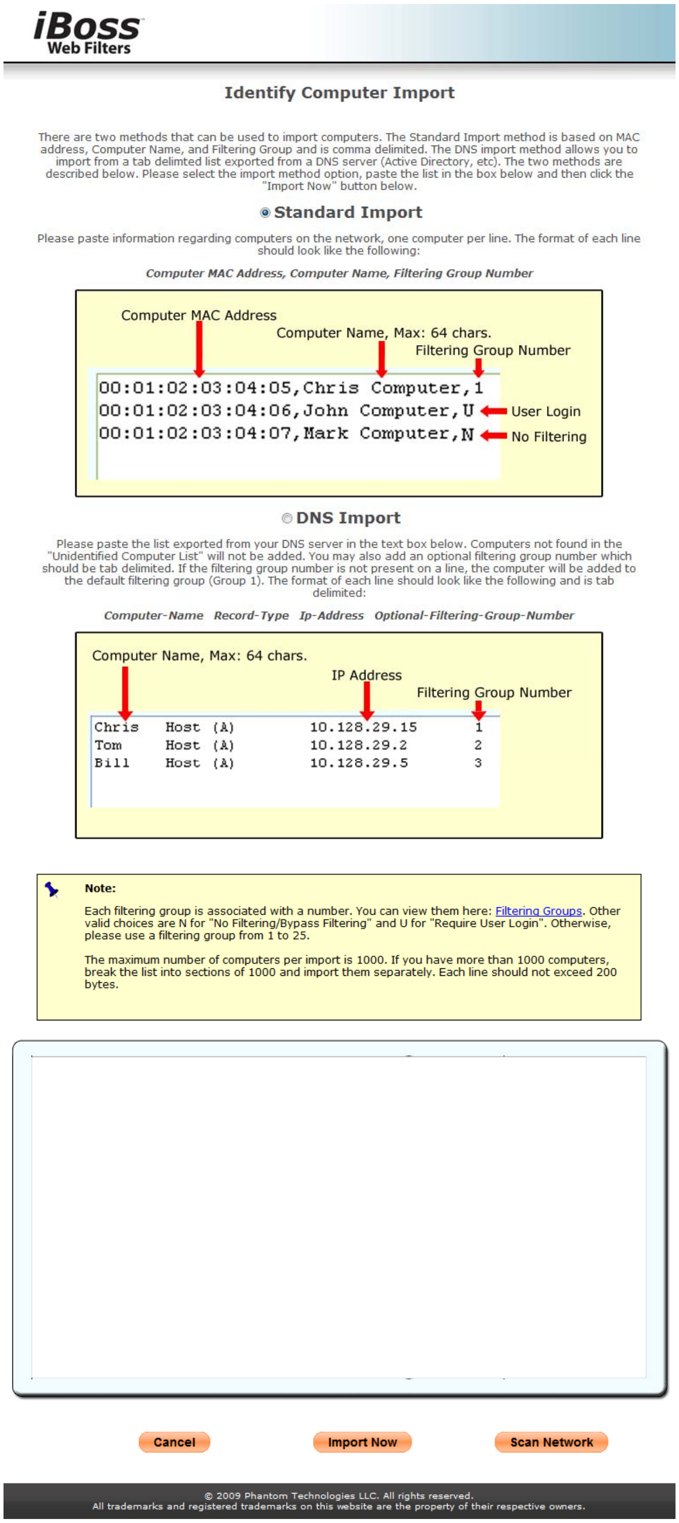
To identify the computer you are using now, click the "**Identify/Edit this computer**" button. Advanced users may click the "**Advanced Add**" button to manually identify a computer. For the "**Advanced Add**", you will need to know the MAC address or IP address of the computer you wish to identify. You may click on Import to import computers to the identified list. Please see the Computer Import section for more information.

Unidentified Computers - This is a list of computers on the network that have not been identified. To identify one of these computers, click Add on the computer in the list that you wish to identify. You may refresh the list by clicking on the "Refresh" button at the bottom of the list.

Default Filtering Policy - These settings apply to computers that are unidentified on your network. You can choose to apply the rules set by the "**default**" filtering group, block all unidentified computers from accessing the Internet, or set unidentified computers to require user login.

Note: If you choose to "**Require user login on all unidentified computers**", you must add users under the Users tab to be able to login and browse the web or have LDAP setup within the iBoss for user authentication.

4.4.1.1 Import Computers



Identify Computer Import

There are two methods that can be used to import computers. The Standard Import method is based on MAC address, Computer Name, and Filtering Group and is comma delimited. The DNS import method allows you to import from a tab delimted list exported from a DNS server (Active Directory, etc). The two methods are described below. Please select the import method option, paste the list in the box below and then click the "Import Now" button below.

● Standard Import

Please paste information regarding computers on the network, one computer per line. The format of each line should look like the following:

Computer MAC Address, Computer Name, Filtering Group Number

```
00:01:02:03:04:05,Chris Computer,1
00:01:02:03:04:06,John Computer,U
00:01:02:03:04:07,Mark Computer,N
```

○ DNS Import

Please paste the list exported from your DNS server in the text box below. Computers not found in the "Unidentified Computer List" will not be added. You may also add an optional filtering group number which should be tab delimited. If the filtering group number is not present on a line, the computer will be added to the default filtering group (Group 1). The format of each line should look like the following and is tab delimited:

Computer-Name Record-Type Ip-Address Optional-Filtering-Group-Number

```
Chris    Host  (A)          10.128.29.15        1
Tom      Host  (A)          10.128.29.2         2
Bill     Host  (A)          10.128.29.5         3
```

Note:

Each filtering group is associated with a number. You can view them here: Filtering Groups. Other valid choices are N for "No Filtering/Bypass Filtering" and U for "Require User Login". Otherwise, please use a filtering group from 1 to 25.

The maximum number of computers per import is 1000. If you have more than 1000 computers, break the list into sections of 1000 and import them separately. Each line should not exceed 200 bytes.

Figure 63 - Importing Computers

There are two methods that can be used to import computers. The Standard Import method is based on MAC address, Computer Name, and Filtering Group and is comma delimited. The DNS import method allows you to import from a tab delimited list exported from a DNS server (Active Directory, etc). The two methods are described below. Please select the import method option, paste the list in the box below and then click the "**Import Now**" button below.

Standard Import - Paste information regarding computers on the network, one computer per line. The format of each line should look like the following:

Computer MAC Address, Computer Name, Filtering Group Number

DNS Import - Paste the list exported from your DNS server in the text box below. Computers not found in the "Unidentified Computer List" will not be added. You may also add an optional filtering group number which should be tab delimited. If the filtering group number is not present on a line, the computer will be added to the default filtering group (Group 1). The format of each line should look like the following and is tab delimited:

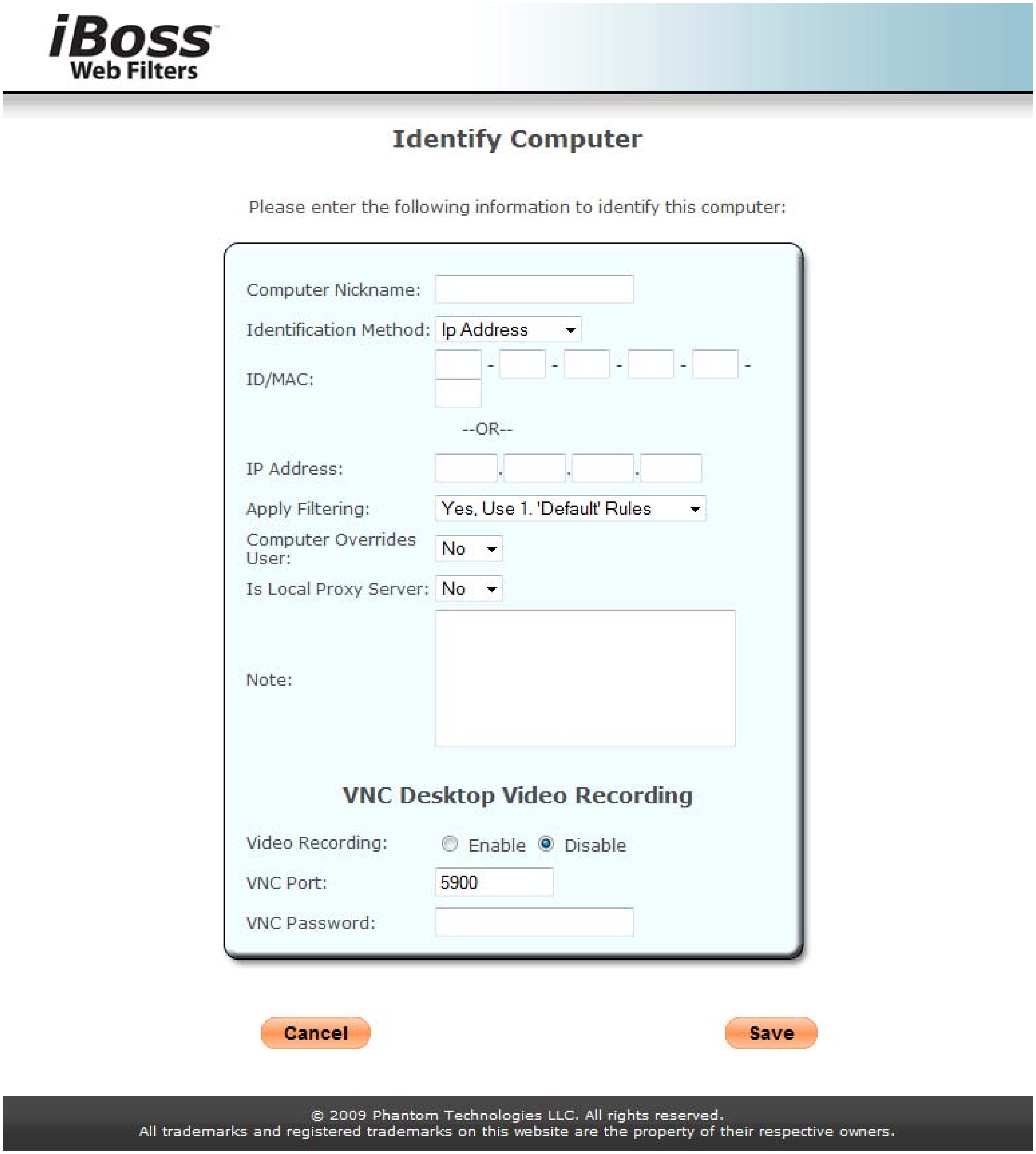
Computer-Name   Record-Type   Ip-Address   Optional-Filtering-Group-Number

Note: Each filtering group is associated with a number. You can view them here: Filtering Groups. Other valid choices are **N** for "**No Filtering/Bypass Filtering**" and **U** for "**Require User Login**". Otherwise, please use a filtering group from 1 to 25.

The maximum number of computers per import is 1000. If you have more than 1000 computers, break the list into sections of 1000 and import them separately. Each line should not exceed 200 bytes.

Scan Network – You can choose to "Scan Network" which will search from computers online on the Local Area Network. This will automatically pull the MAC Address and computer name of the computers found. This will cause the iBoss to be paused while this is processing. Once finished you will receive a Save dialogue which you can save. Open this file in a text editor to copy and paste computers found on the network.

4.4.1.2 Identifying a Computer



Identify Computer

Please enter the following information to identify this computer:

Computer Nickname:	
Identification Method:	Ip Address ▾
ID/MAC:	- - - - -
	--OR--
IP Address:	. . .
Apply Filtering:	Yes, Use 1. 'Default' Rules ▾
Computer Overrides User:	No ▾
Is Local Proxy Server:	No ▾
Note:	

VNC Desktop Video Recording

Video Recording:	○ Enable ● Disable
VNC Port:	5900
VNC Password:	

Figure 64 - Identifying a Computer

To identify a computer, you may enter a Computer Nickname for the computer. When clicking on the button "**Identify/Edit This Computer**", the ID/MAC address is automatically entered for you. If you have the subnet setup as IP mode, the IP address will be entered here. When clicking on "**Advanced Add**" you may enter in the ID/MAC address or IP address for the computer you are identifying.

You may either set the Apply Filtering to "**Yes, Use Default Rules**" with one of the filtering groups, "**No, Bypass Filtering Rules**" or “**Require user login for this computer**” for the computer you are identifying. When finished click the "Save" button. If you want to cancel your changes click the "Cancel" button.

*The "Yes, Use Default Rules" will show the assigned name of the filtering group.

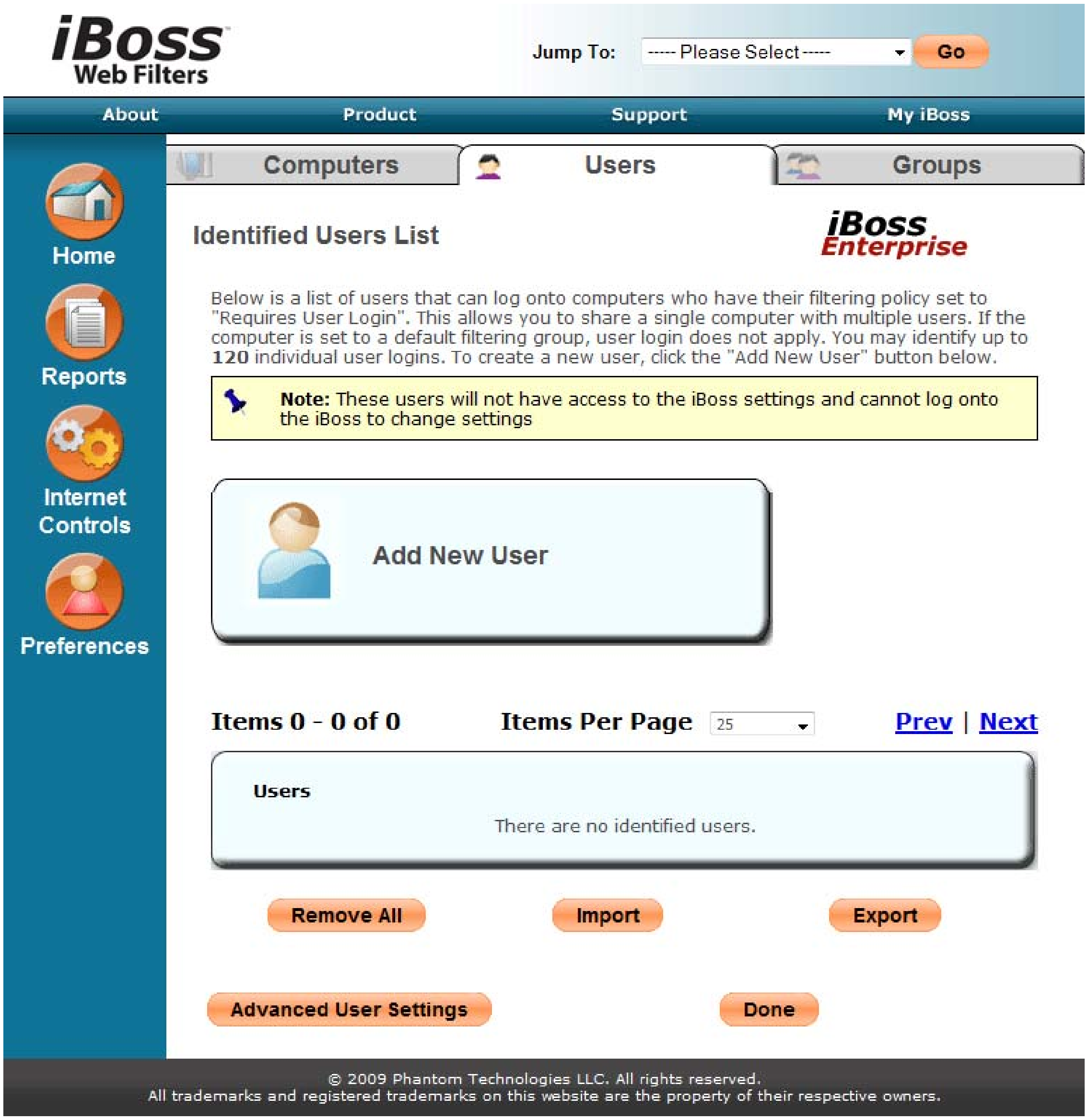
Computer Overrides User – This option allows you to always have the computer filtering policy in place and not allow users to override this option.

Is Local Proxy Server – This option is to identify if the computer you are identifying is a proxy server on your local network.

Note: Computers with filtering rules applied will be filtered by the iBoss. Computers with filtering rules bypassed will bypass the iBoss.

* There are more options if you have the DMCR feature added. This will allow you to put the Port, Password and IP address of the client VNC computer. Please refer to the DMCR section for more information.

4.4.2 Identify Users



Identified Users List

Below is a list of users that can log onto computers who have their filtering policy set to "Requires User Login". This allows you to share a single computer with multiple users. If the computer is set to a default filtering group, user login does not apply. You may identify up to 120 individual user logins. To create a new user, click the "Add New User" button below.

Note: These users will not have access to the iBoss settings and cannot log onto the iBoss to change settings

Items 0 - 0 of 0   Items Per Page 25   Prev | Next

Users

There are no identified users.

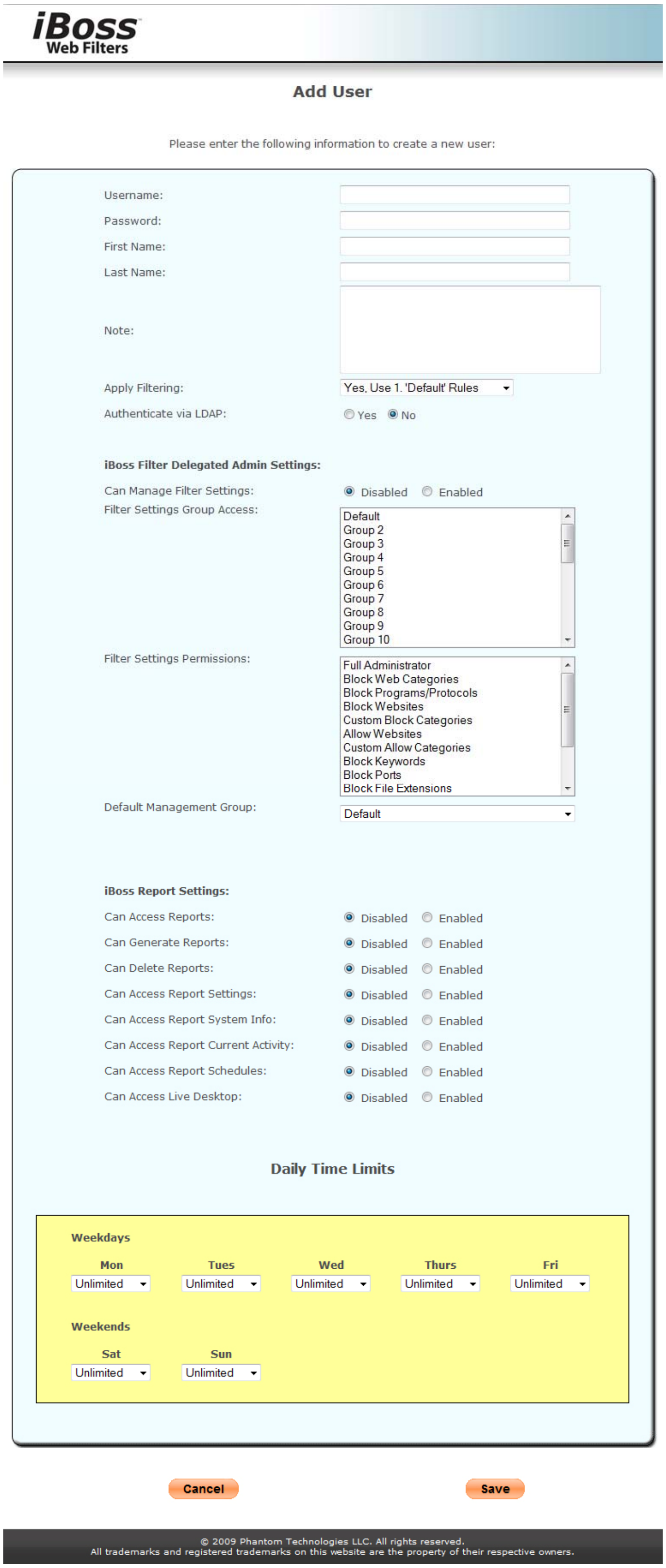
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 65 - Identify Users

This is a list of users that can log onto computers who have their filtering policy set to "Requires User Login". This allows you to share a single computer with multiple users. If the computer is set to a default filtering group, user login does not apply. You may identify up to 120 individual user logins. To create a new user, click the "**Add New User**" button below.

These users will not have access to the iBoss settings and cannot log onto the iBoss to change settings unless configured to allow access.

4.4.2.1 Adding a User



iBoss Web Filters

Add User

Please enter the following information to create a new user:

Username:	
Password:	
First Name:	
Last Name:	
Note:	
Apply Filtering:	Yes, Use 1. 'Default' Rules
Authenticate via LDAP:	○ Yes ● No

iBoss Filter Delegated Admin Settings:

Can Manage Filter Settings:	● Disabled ○ Enabled
Filter Settings Group Access:	Default Group 2 Group 3 Group 4 Group 5 Group 6 Group 7 Group 8 Group 9 Group 10
Filter Settings Permissions:	Full Administrator Block Web Categories Block Programs/Protocols Block Websites Custom Block Categories Allow Websites Custom Allow Categories Block Keywords Block Ports Block File Extensions
Default Management Group:	Default

iBoss Report Settings:

Can Access Reports:	● Disabled ○ Enabled
Can Generate Reports:	● Disabled ○ Enabled
Can Delete Reports:	● Disabled ○ Enabled
Can Access Report Settings:	● Disabled ○ Enabled
Can Access Report System Info:	● Disabled ○ Enabled
Can Access Report Current Activity:	● Disabled ○ Enabled
Can Access Report Schedules:	● Disabled ○ Enabled
Can Access Live Desktop:	● Disabled ○ Enabled

Daily Time Limits

Weekdays

Mon	Tues	Wed	Thurs	Fri
Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

Weekends

Sat	Sun
Unlimited	Unlimited

Figure 66 - Adding a User

To identify a user, you may enter a Username, Password, First Name, and Last Name. You may either set the Apply Filtering to "**Yes, Use Group 1* Rules**" using one of the filtering groups or "**No, Bypass Filtering Rules**" for the user you are identifying. You can authenticate the user via LDAP to use the users password within LDAP

Daily Time Limits - This will allow you to set daily time limits for each day of the week for a user. You can set a time between 15 minutes to 23 hours that a user can be logged in from throughout the day. This means that when a user has the allocated time throughout the day to use the time limit. When finished click the "**Save**" button. If you want to cancel your changes click the "**Cancel**" button.

4.4.2.2 Delegated Admins

When adding a user to the iBoss, you will also have options to give them access to filtering settings and report settings. The default name for the iBoss reports is Admin. This only applies to iBoss devices using a local report manager. For users with the External Report Manager, you will need to setup these users in the Report Manager settings. Please refer to the Report Manager section for more information.

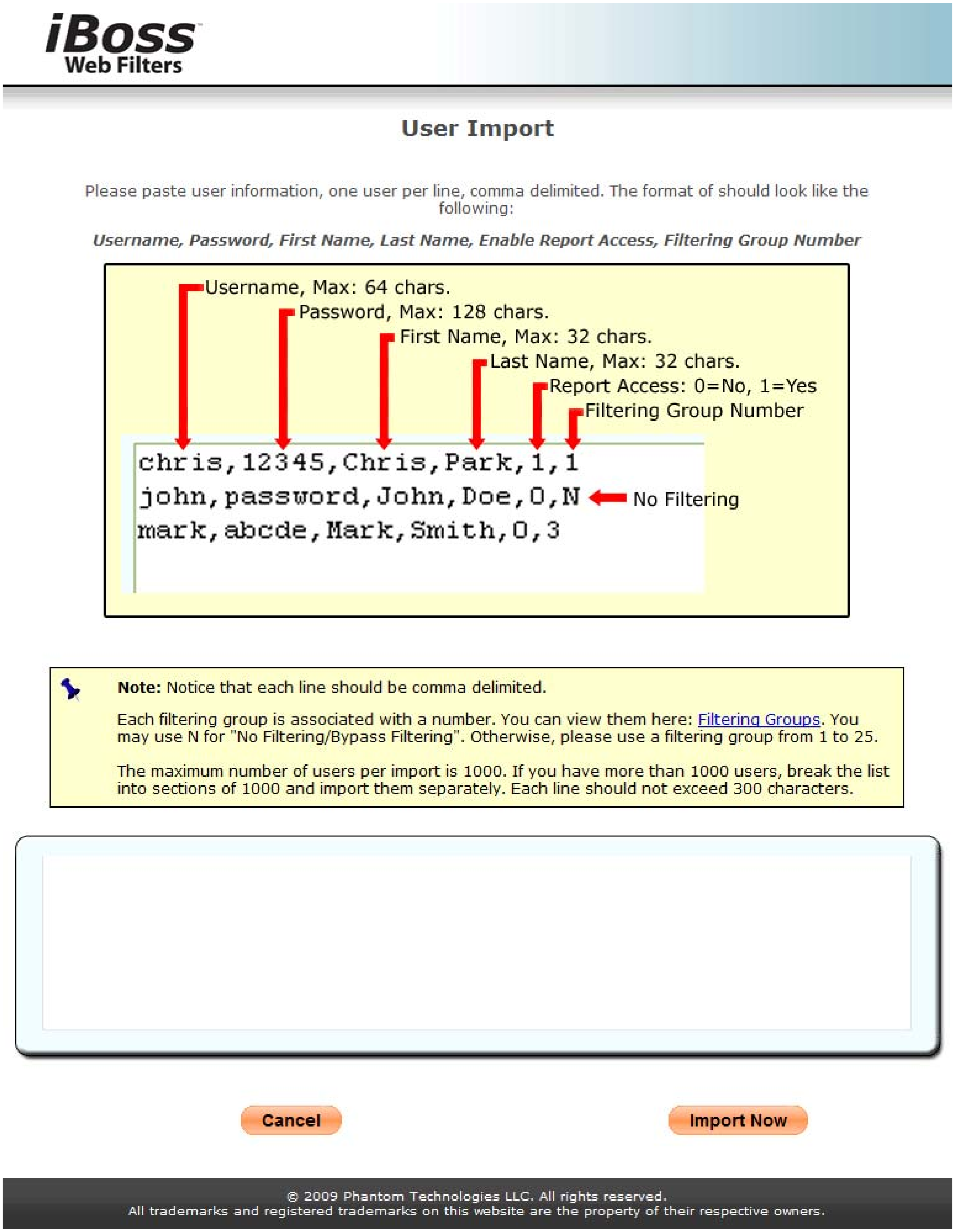
Filtering Settings Group Access – Use this option to select which groups the user will have rights to change settings for.

Filtering Settings Permissions – Use these options to select which options can be changed for the users

Default Management Group – This is the default management group that the user is administering.

iBoss Report Settings – Choose which options to allow the delegated admin to have access to in the iBoss reports.

4.4.2.3 Importing Users



User Import

Please paste user information, one user per line, comma delimited. The format of should look like the following:

Username, Password, First Name, Last Name, Enable Report Access, Filtering Group Number

Username, Max: 64 chars.
Password, Max: 128 chars.
First Name, Max: 32 chars.
Last Name, Max: 32 chars.
Report Access: 0=No, 1=Yes
Filtering Group Number

```
chris,12345,Chris,Park,1,1
john,password,John,Doe,0,N
mark,abcde,Mark,Smith,0,3
```

No Filtering

Note: Notice that each line should be comma delimited.

Each filtering group is associated with a number. You can view them here: Filtering Groups. You may use N for "No Filtering/Bypass Filtering". Otherwise, please use a filtering group from 1 to 25.

The maximum number of users per import is 1000. If you have more than 1000 users, break the list into sections of 1000 and import them separately. Each line should not exceed 300 characters.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 67 - Importing Users

Please paste user information, one user per line, comma delimited. The format of should look like the following:

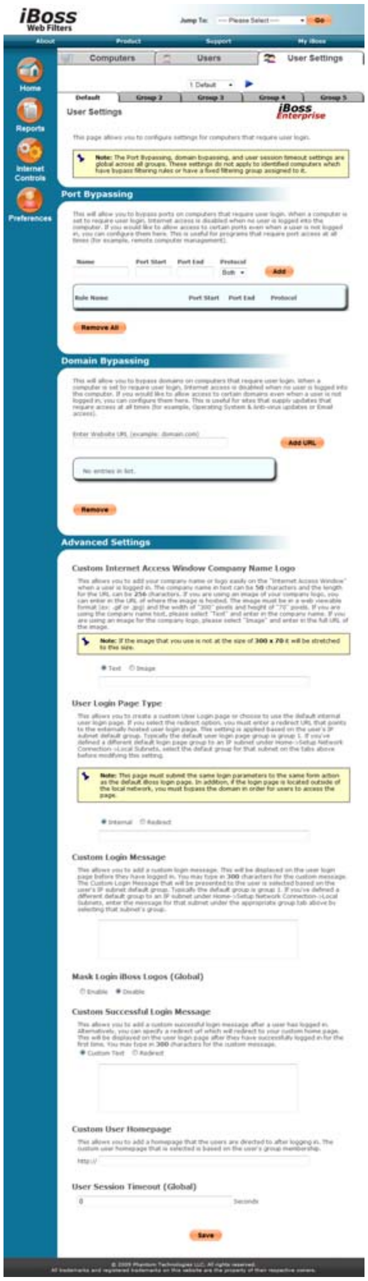
Username, Password, First Name, Last Name, Enable Report Access, Filtering Group Number

Note: Notice that each line should be comma delimited.
Each filtering group is associated with a number. You can view them here: Filtering Groups. You may use **N** for "**No Filtering/Bypass Filtering**". Otherwise, please use a filtering group.

The maximum number of users per import is 1000. If you have more than 1000 users, break the list into sections of 1000 and import them separately. Each line should not exceed 300 characters.

Once you have finished, click the “**Import Now**” button.

4.4.2.4 Advanced User Settings



User Settings

This page allows you to configure settings for computers that require user login.

Note: The Port Bypassing, domain bypassing, and user session timeout settings are global across all groups. These settings do not apply to identified computers which have bypass filtering rules or have a fixed filtering group assigned to it.

Port Bypassing

This will allow you to bypass ports on computers that require user login. When a computer is set to require user login, Internet access is disabled when no user is logged into the computer. If you would like to allow access to certain ports even when a user is not logged in, you can configure them here. This is useful for programs that require port access at all times (for example, remote computer management).

Name | Port Start | Port End | Protocol: Both | Add

Rule Name | Port Start | Port End | Protocol

Remove All

Domain Bypassing

This will allow you to bypass domains on computers that require user login. When a computer is set to require user login, Internet access is disabled when no user is logged into the computer. If you would like to allow access to certain domains even when a user is not logged in, you can configure them here. This is useful for sites that supply updates that require access at all times (for example, Operating System & Anti-virus updates or Email access).

Enter Website URL (example: domain.com) | Add URL

No entries in list.

Remove

Advanced Settings

Custom Internet Access Window Company Name Logo

This allows you to add your company name or logo easily on the "Internet Access Window" when a user is logged in. The company name in text can be **50** characters and the length for the URL can be **256** characters. If you are using an image of your company logo, you can enter in the URL of where the image is hosted. The image must be in a web viewable format (ex: .gif or .jpg) and the width of "300" pixels and height of "70" pixels. If you are using the company name text, please select "Text" and enter in the company name. If you are using an image for the company logo, please select "Image" and enter in the full URL of the image.

Note: If the image that you use is not at the size of **300 x 70** it will be stretched to this size.

● Text ○ Image

User Login Page Type

This allows you to create a custom User Login page or choose to use the default internal user login page. If you select the redirect option, you must enter a redirect URL that points to the externally hosted user login page. This setting is applied based on the user's IP subnet default group. Typically the default user login page group is group 1. If you've defined a different default login page group to an IP subnet under Home->Setup Network Connection->Local Subnets, select the default group for that subnet on the tabs above before modifying this setting.

Note: This page must submit the same login parameters to the same form action as the default iBoss login page. In addition, if the login page is located outside of the local network, you must bypass the domain in order for users to access the page.

● Internal ○ Redirect

Custom Login Message

This allows you to add a custom login message. This will be displayed on the user login page before they have logged in. You may type in **300** characters for the custom message. The Custom Login Message that will be presented to the user is selected based on the user's IP subnet default group. Typically the default group is group 1. If you've defined a different default group to an IP subnet under Home->Setup Network Connection->Local Subnets, enter the message for that subnet under the appropriate group tab above by selecting that subnet's group.

Mask Login iBoss Logos (Global)

○ Enable ● Disable

Custom Successful Login Message

This allows you to add a custom successful login message after a user has logged in. Alternatively, you can specify a redirect url which will redirect to your custom home page. This will be displayed on the user login page after they have successfully logged in for the first time. You may type in **300** characters for the custom message.

● Custom Text ○ Redirect

Custom User Homepage

This allows you to add a homepage that the users are directed to after logging in. The custom user homepage that is selected is based on the user's group membership.

http://

User Session Timeout (Global)

0 Seconds

Save

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 68 – Advanced User Settings

This page allows you to configure settings for computers that require user login.
Note: These settings are global across all computers that require user login and only apply to computers which require user login. These settings do not apply to identified computers which have bypass filtering rules or have a filtering group set for it.

Port Bypassing - This will allow you to bypass ports on computers that require user login. When a computer is set to require user login, Internet access is disabled when no user is logged into the computer. If you would like to allow access to certain ports even when a user is not logged in, you can configure them here. This is useful for programs that require port access at all times (for example, remote computer management).

Domain Bypassing - This will allow you to bypass domains on computers that require user login. When a computer is set to require user login, Internet access is disabled when no user is logged into the computer. If you would like to allow access to certain domains even when a user is not logged in, you can configure them here. This is useful for sites that supply updates that require access at all times (for example, Operating System & Anti-virus updates or Email access).

Custom Internet Access Window Company Name Logo - This allows you to add your company name or logo easily on the "Internet Access Window" when a user is logged in. The company name in text can be 50 characters and the length for the URL can be 256 characters. If you are using an image of your company logo, you can enter in the URL of where the image is hosted. The image must be in a web viewable format (ex: .gif or .jpg) and the width of "300" pixels and height of "70" pixels. If you are using the company name text, please select "Text" and enter in the company name. If you are using an image for the company logo, please select "Image" and enter in the full URL of the image.

Note: If the image that you use is not at the size of 300 x 70 it will be stretched to this size

User Login Page - This allows you to create a custom User Login page or choose to use the default internal user login page. If you select the redirect option, you must enter a redirect URL that points to the externally hosted user login page. This setting is applied based on the user's IP subnet default group. Typically the default user login page group is group 1. If you've defined a different default login page group to an IP subnet under Home->Setup Network Connection->Local Subnets, select the defaut group for that subnet on the tabs above before modifying this setting. You may choose either Internal or Redirect.

Note: This page must submit the same login parameters to the same form action as the default iBoss login page. In addition, if the login page is located outside of the local network, you must bypass the domain in order for users to access the page.

Custom Login Message - This allows you to add a custom login message. This will be displayed on the user login page before they have logged in. You may type in 300 characters for the custom message.

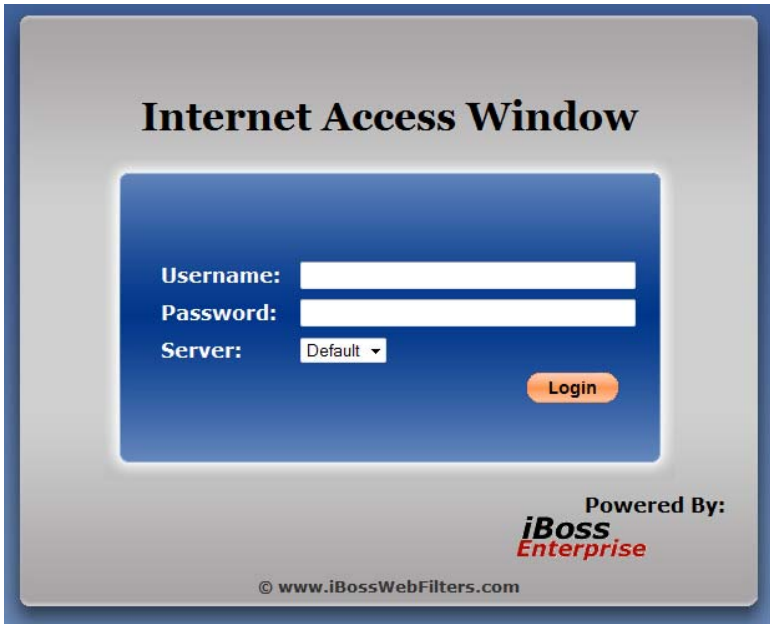
Mask Login iBoss Logos (Global) - This allows you to mask the iBoss logos on the login pages. This hides which filtering device you are using on your network.

Custom Successful Login Message - This allows you to add a custom successful login message after a user has logged in. This will be displayed on the user login page after they have successfully logged in for the first time. You may type in 300 characters for the custom message.

Custom User Homepage - This allows you to add a homepage that the users are directed to after logging in.

User Session Timeout – This allows you to change how long it will take before a user is automatically logged out if the iBoss does not hear from it being logged in. This is in seconds and if you are having issues with it logging out, you may set this to a higher number in seconds or set it to ‘0’ to disable the timeout.

4.4.2.5 User Internet Access Window



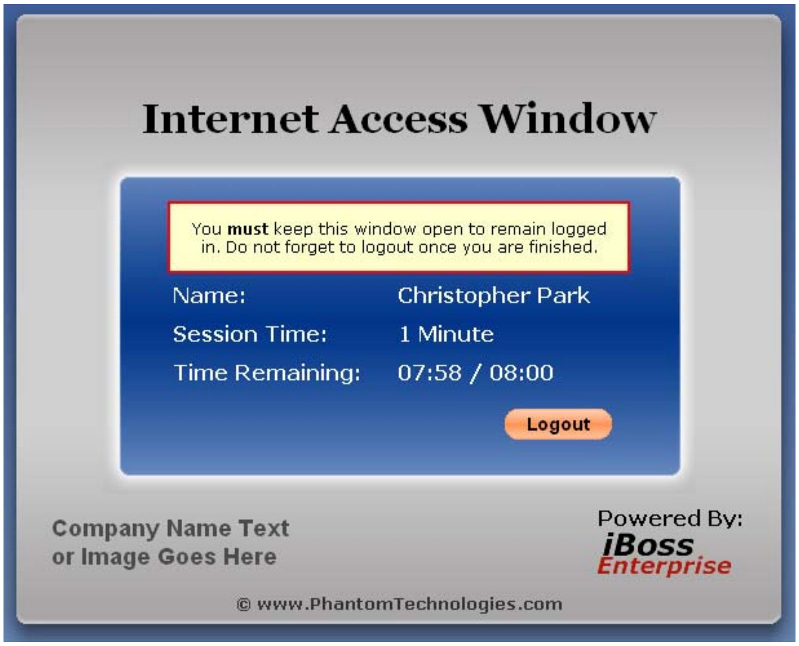
Internet Access Window

Username:

Password:

Server: Default

Figure 69 - Internet Access Window Login



Internet Access Window

You **must** keep this window open to remain logged in. Do not forget to logout once you are finished.

Name: Christopher Park

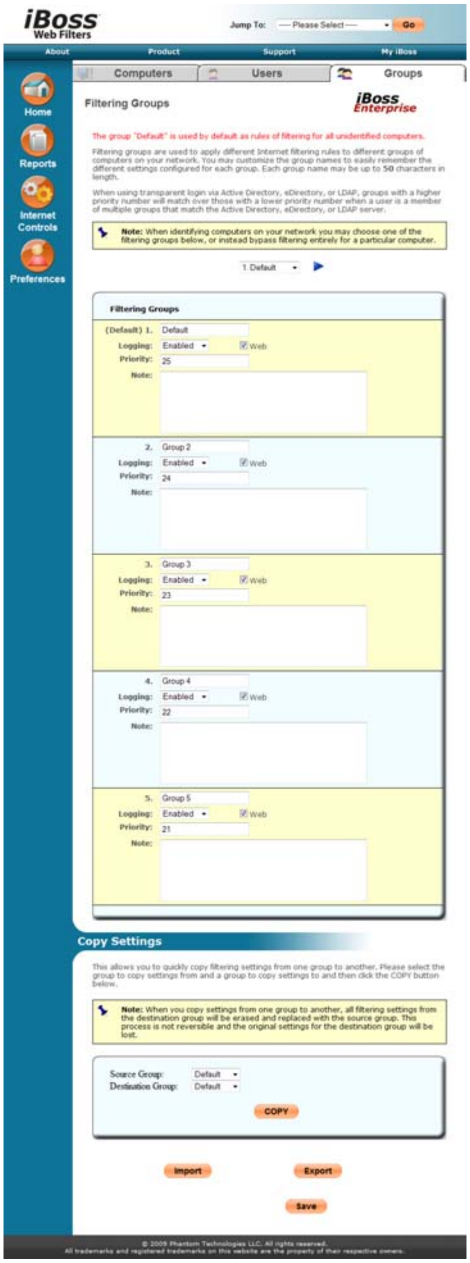
Session Time: 1 Minute

Time Remaining: 07:58 / 08:00

Figure 70 - Internet Access Window Session

The iBoss Internet Access Window is the session window for the user that is logged in. This window must be kept open to remain logged in. This window will show you the Name of the user logged in, how long they have been logged in (Session Time), Time Remaining/Daily time limit and which server they are logged into if you have multiple Domains. The iBoss user login feature also allows you to put your own Company Name in text or put a URL for a Company Logo Image. The user login feature allows you to put custom messages before a user logs in and after they log in. This allows you to post company policies and rules before using the Internet to protect your company from liability conflicts.

4.4.3 Filtering Groups



Filtering Groups

The group "Default" is used by default as rules of filtering for all unidentified computers.

Filtering groups are used to apply different Internet filtering rules to different groups of computers on your network. You may customize the group names to easily remember the different settings configured for each group. Each group name may be up to 50 characters in length.

When using transparent login via Active Directory, eDirectory, or LDAP, groups with a higher priority number will match over those with a lower priority number when a user is a member of multiple groups that match the Active Directory, eDirectory, or LDAP server.

Note: When identifying computers on your network you may choose one of the filtering groups below, or instead bypass filtering entirely for a particular computer.

1. Default ▶

Filtering Groups

(Default) 1. Default
Logging: Enabled ☑ Web
Priority: 25
Note:

2. Group 2
Logging: Enabled ☑ Web
Priority: 24
Note:

3. Group 3
Logging: Enabled ☑ Web
Priority: 23
Note:

4. Group 4
Logging: Enabled ☑ Web
Priority: 22
Note:

5. Group 5
Logging: Enabled ☑ Web
Priority: 21
Note:

Copy Settings

This allows you to quickly copy filtering settings from one group to another. Please select the group to copy settings from and a group to copy settings to and then click the COPY button below.

Note: When you copy settings from one group to another, all filtering settings from the destination group will be erased and replaced with the source group. This process is not reversible and the original settings for the destination group will be lost.

Source Group: Default
Destination Group: Default

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 71 - Edit Filtering Groups

Filtering groups are used to apply different Internet filtering rules to different groups of computers on your network. You may customize the group names to easily remember the different settings configured for each group. Each group name may be up to 50 characters in length.

When using transparent login via Active Directory, eDirectory, or LDAP, groups with a higher priority number will match over those with a lower priority number when a user is a member of multiple groups that match the Active Directory, eDirectory, or LDAP server.

Note: When identifying computers on your network you may choose one of the filtering groups below, or instead bypass filtering entirely for a particular computer

Note: You may put a higher number in the Priority group so that it has higher priority than the other filtering groups if users fall under more than one filtering group.

Copy Settings – This allows you to quickly copy filtering settings from one group to another. Please select the group to copy settings from and a group to copy settings to and then click the COPY button below.

Note: When you copy settings from one group to another, all filtering settings from the destination group will be erased and replaced with the source group. This process is not reversible and the original settings for the destination group will be lost.

4.4.3.1 Filtering Group Tabs

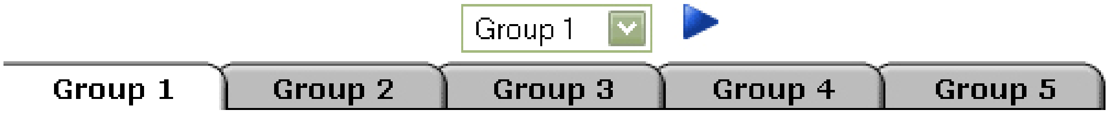
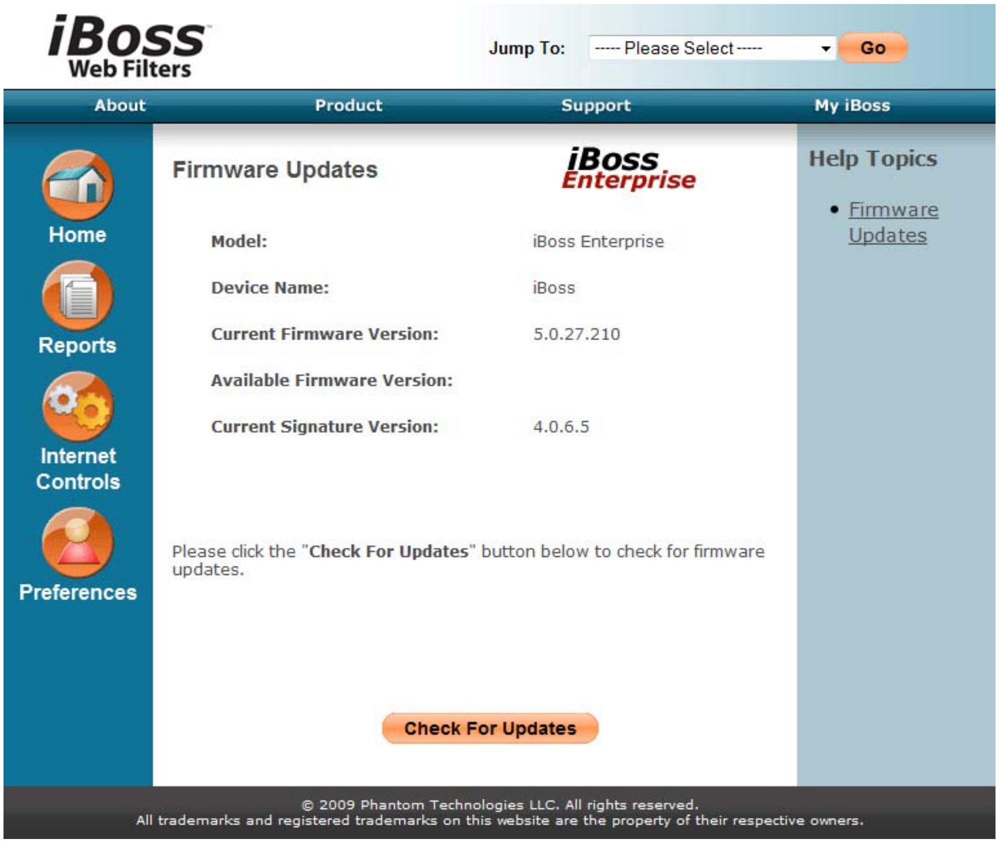


Figure 72 - Filtering Group Tabs

When configuring the rules for your iBoss, you will notice the Group tabs at the top of each configuration page. These pages allow you to set different filtering rules for the different filtering groups. The selected group will appear to have the tab in front of the other tabs. To switch configuration for different groups, select the group tab at the top of the page or from the drop down menu to quickly jump to a filtering group. You may use the arrows to go to the next or previous set of filtering groups.

4.5 Firmware Updates



Firmware Updates

Model:	iBoss Enterprise
Device Name:	iBoss
Current Firmware Version:	5.0.27.210
Available Firmware Version:	
Current Signature Version:	4.0.6.5

Please click the "**Check For Updates**" button below to check for firmware updates.

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 73 - Firmware Updates

Firmware updates may be available from time to time. These updates include feature enhancements. The updates are downloaded over the Internet directly into the device. Firmware updates include feature enhancements only and are not related to the iBoss Internet filtering functionality. The iBoss will always be up-to-date with the latest web category URLs and online application definitions used with filtering rules. You must have an active subscription and a live Internet connection in order to download firmware updates.

Model - Indicates the model of your iBoss device.
Device Name - Indicates the name given to the iBoss.
Current Firmware Version - Indicates the firmware version installed on your iBoss.
Available Firmware Version - Indicates the latest firmware version available for download. If this version number matches the number in the "Current Version" field, then your iBoss firmware is up to date.
Current Signature Version - Indicates the signature version installed on your iBoss
Download/Install - The "Download/Install" button will appear when new firmware is available. Click this button to begin downloading and installing the new firmware. The "**Install**" button will appear when new firmware has been downloaded and is ready to install. Click this button to begin installing the new firmware. Once this process begins, do not power down the iBoss until installation is complete. When the installation is complete, you will be redirected back to the iBoss home page.
Download Progress - Indicates the download progress of the firmware updates.

5 Enterprise Report Manager

The iBoss is equipped with an advanced report manager capable of tracking and generating statistics and a variety of aspects of network traffic. This includes web statistics such as web sites visited and top visited domains, as well as detailed port and IP Address accesses.

The report manager provides a deep drill down capability that can identify potential risks as well as help optimize the network. The high level of report detail also includes a variety of information that can be summarized for all users in a report or information specific to a particular user. This includes bandwidth usage and graphs showing accesses throughout the report period.

The report manager is separated into two major subsections. The first deals with report management, scheduling and generation, while the other involves the report viewing.

5.1 External Enterprise Reporter

The External Report Manager or Enterprise Reporter is an appliance that offloads the reporting onto a different server appliance. Some of the features discussed below are not in the external report manager.

5.1.1 Installing the External iBoss Enterprise Reporter on the network.

Please setup the network settings for the external iBoss Enterprise Reporter before placing it on the network. Please refer to the Network Settings section for the Enterprise Reporter for more information on how to set these settings.

Once the network settings have been configured, the iBoss Enterprise Reporter is ready to be installed on the network. The port you will be using is the “WAN” port located on the back of the iBoss Enterprise Reporter.

Place the iBoss Enterprise Reporter on the switch just as a computer would be. For example, add a network cable from your switch to the “WAN” port of the Enterprise Reporter. Do not put the device in line, like you would when setting up the iBoss filter.

After setting up the iBoss Enterprise Reporter on the network, do not forget to identify the Enterprise Reporter and Select “No, Bypass Filtering Rules”.

5.1.2 Setup Steps to Register iBoss to External Enterprise Reporter

This section is a quick guide for registering iBoss devices to an Enterprise Reporter.

1. Setup an IP address for the iBoss Device (please refer to the iBoss IP address section to set this)

2. Setup an IP address for the iBoss Enterprise Reporter (please refer to the iBoss Enterprise Reporter Network Settings section to set this)

3. Log into the report manager and click on Settings→ General → then change the Report Database Password. (please refer to the iBoss Enterprise Reporter Settings section for more information)

4. Click on Register iBoss Devices→ Add Device → Then set the iBoss name, iBoss IP address, and copy the Security key. (please refer to the iBoss Enterprise Reporter Settings section for more information)

5. Log into the iBoss device and click on Preferences → Configure Report Settings → Edit General Report Settings → change the 'Configure iBoss for' option to "External Report Manager". (please refer to the iBoss Report Settings section for more information)

6. Enter the IP address, database password, and security key of the iBoss Enterprise Reporter and click Save. (please refer to the iBoss Report Settings section for more information)

Note: Please be sure to identify the report manager within the iBoss interface to bypass any filtering rules.

5.2 Accessing the Report Manager

The report manager can be accessed by logging into the iBoss via myiboss.com and then clicking on the "Report" icon, or by using the following URL:

http://www.myiboss.com/reports

You can access the report manager only while on the same network as the iBoss. You can access the iBoss reports from any computer on the network that has access to the iBoss interface.

Note: The default IP address of the iBoss Enterprise Reporter is 192.168.1.20.

5.3 Logging into the Report Manager

The default username for the report manager is admin. The administrative password for the iBoss Report Manager is the same as the password that is used to configure the iBoss filtering rules.

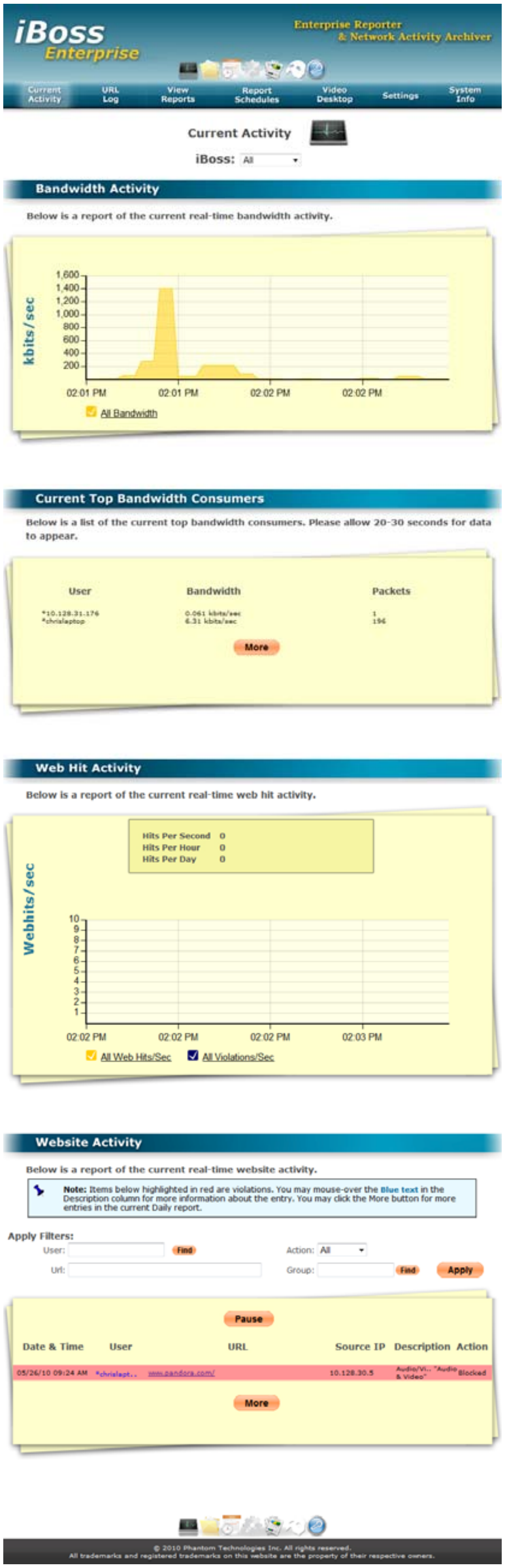
Note: The default username for the External iBoss Enterprise Reports is admin. There is no password by default. You will need to change this setting and also be able to add users within the Enterprise Reporter settings.

You can create additional users that can access the report manager by creating them within the iBoss configuration interface and giving that user privileges to access the Report Manager in the user Add/Edit screens. You can also configure specific privileges for the user to restrict the types of operations the user can perform within the report manager. This only applies when you are not using an external Enterprise Reporter.

Only users configured locally in the iBoss can be allowed access into the report manager. Users logging in through LDAP/Active directory will not have access to the report manager. This only applies when you are not using an external Enterprise Reporter.

5.4 Report Generation and Management

After logging into the report manager, the iBoss presents a page detailing the current activity. This page contains information regarding what is currently occurring on the network. There are several other sections within the report management section that include viewing and creating generated reports, viewing and creating report schedules, configuring report settings, and viewing system information.



Current Activity

iBoss: All

Bandwidth Activity

Below is a report of the current real-time bandwidth activity.

Current Top Bandwidth Consumers

Below is a list of the current top bandwidth consumers. Please allow 20-30 seconds for data to appear.

User	Bandwidth	Packets
*10.128.31.176 *chrislaptop	0.061 kbits/sec 6.31 kbits/sec	1 196

Web Hit Activity

Below is a report of the current real-time web hit activity.

Hits Per Second	0
Hits Per Hour	0
Hits Per Day	0

Website Activity

Below is a report of the current real-time website activity.

Note: Items below highlighted in red are violations. You may mouse-over the Blue text in the Description column for more information about the entry. You may click the More button for more entries in the current Daily report.

Apply Filters:

User:

Action: All

Url:

Group:

Date & Time	User	URL	Source IP	Description	Action
05/26/10 09:24 AM	*chrislapt..	www.pandora.com/	10.128.30.5	Audio/Vi.. "Audio & Video"	Blocked

© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

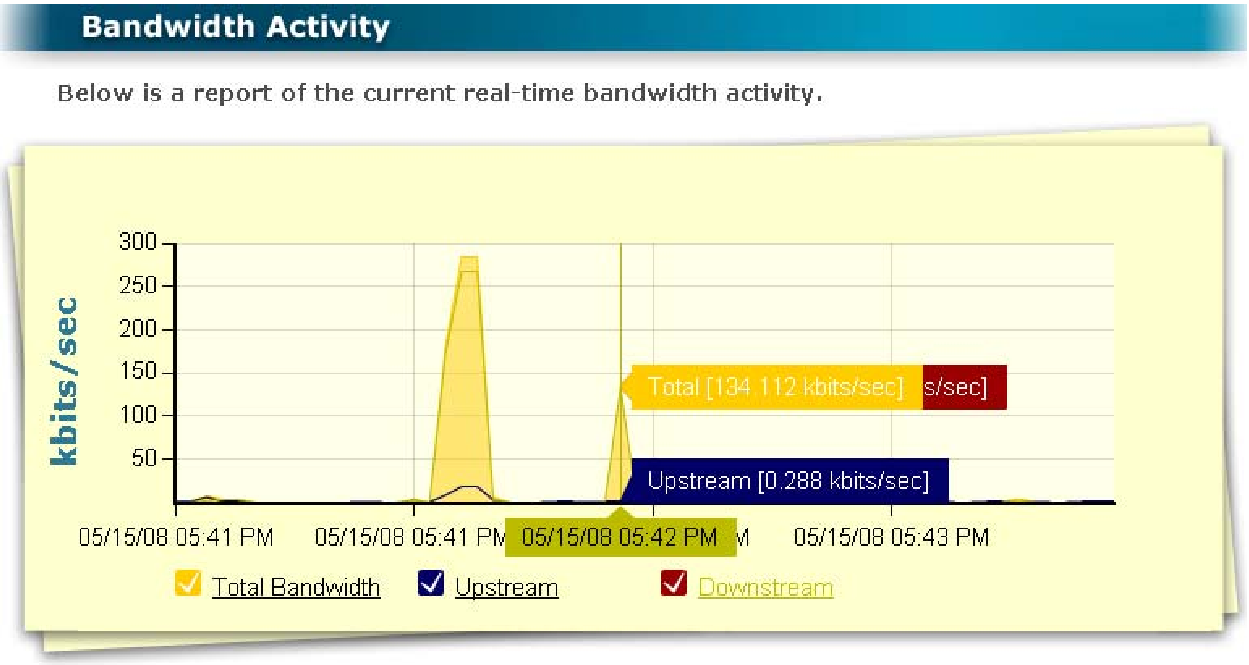
Figure 74 – Current Activity

5.4.1 Current Activity

The current activity section shows active real-time information about the network. This information is updated in real-time automatically.

5.4.1.1 Real-time Web Hit Activity Graph

The first section includes a real-time Web Hit Activity that includes Web Hits per second and Violation per second.



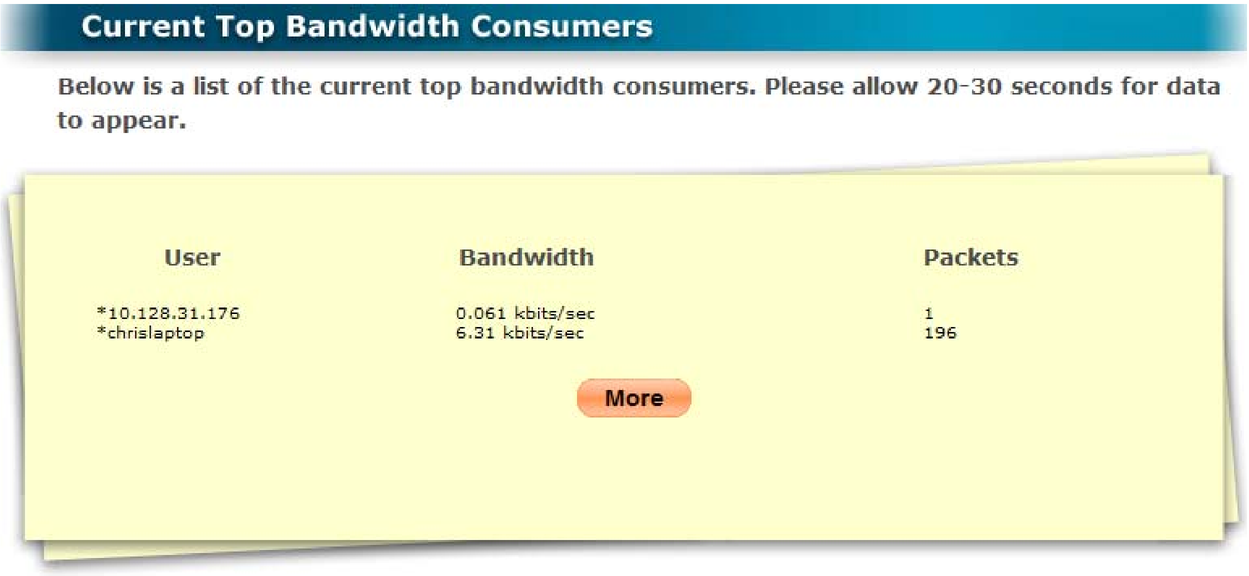
Bandwidth Activity

Below is a report of the current real-time bandwidth activity.

Figure 75 - Real-time MRTG Bandwidth Graph

5.4.1.2 Current Top Bandwidth Consumers

This section includes the top consumers of bandwidth updated in real-time. You can click on the “**More**” button for more details of users.



Current Top Bandwidth Consumers

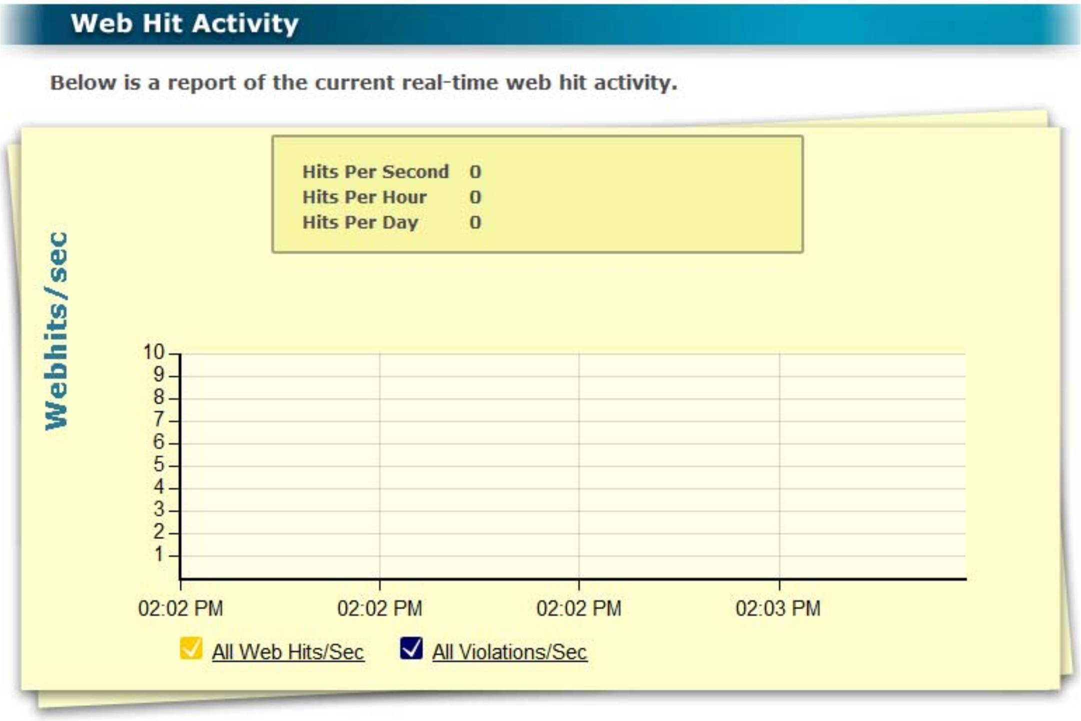
Below is a list of the current top bandwidth consumers. Please allow 20-30 seconds for data to appear.

User	Bandwidth	Packets
*10.128.31.176	0.061 kbits/sec	1
*chrislaptop	6.31 kbits/sec	196

Figure 76 - Current Top Bandwidth Consumers

5.4.1.3 Real-time Web Hit activity graph

This section shows total the current total webhits per second, as well as the total current violations per second. It will also show statistics at the top for the speed of hits per second, hour and day.



Web Hit Activity

Below is a report of the current real-time web hit activity.

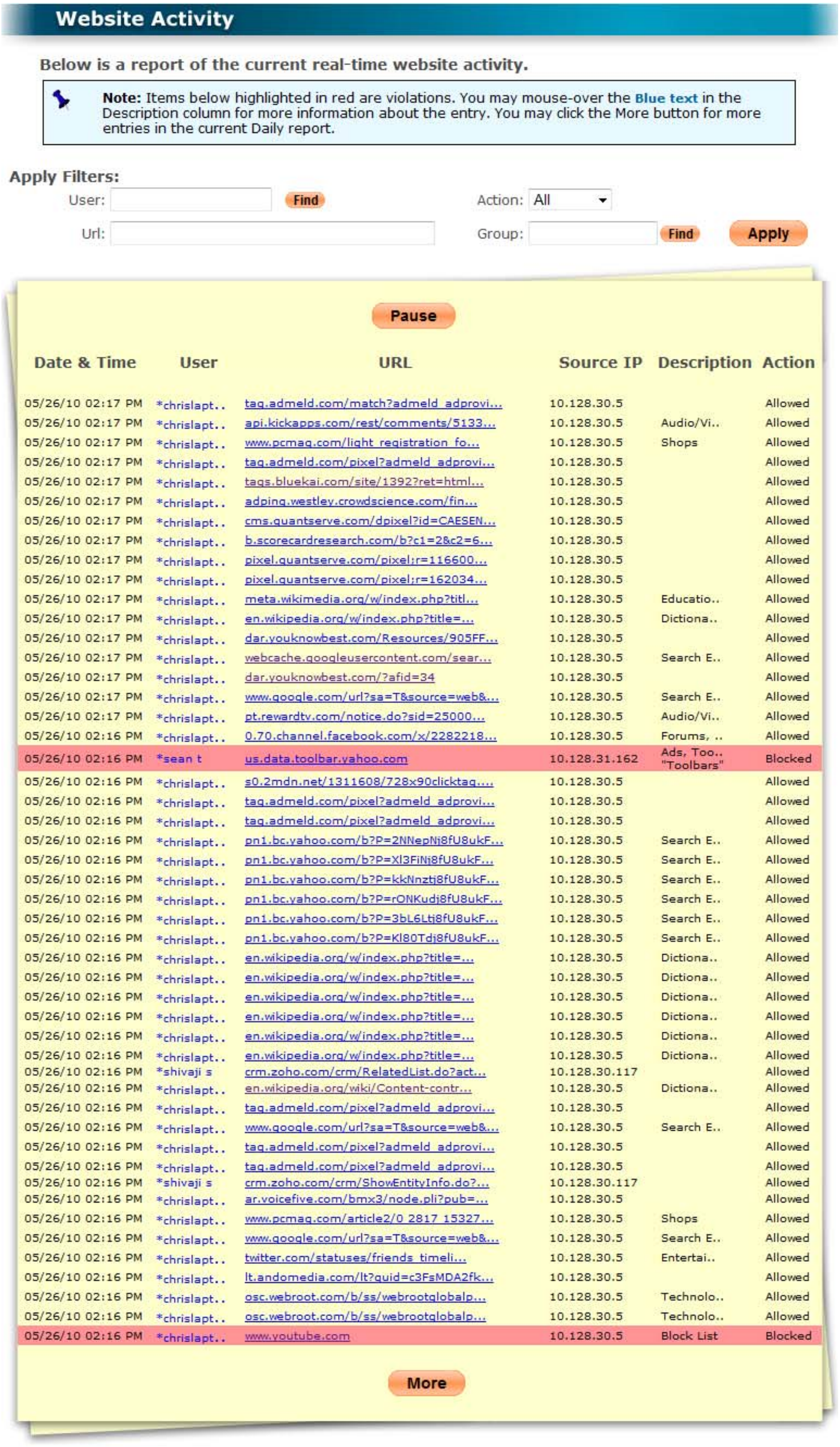
Hits Per Second	0
Hits Per Hour	0
Hits Per Day	0

Figure 77 - Real-time Webhit Activity

5.4.1.4 Real-time website activity

This section shows the current websites being visited. The URLs are updated in real-time as users on the network access website destinations. It will also provide details about the URL access including categories. The list will highlight URLs that were blocked by the iBoss. This list is updated in real-time without the need to refresh the page.

This section also has a filter to only show a specific User and/or Action (Allowed or Blocked). You may simply click the username in this list to automatically set the filter to a specific user. You may also click the Pause button to stop the list from scrolling.



Website Activity

Below is a report of the current real-time website activity.

Note: Items below highlighted in red are violations. You may mouse-over the **Blue text** in the Description column for more information about the entry. You may click the More button for more entries in the current Daily report.

Apply Filters:

User: Find

Action: All

Url:

Group: Find

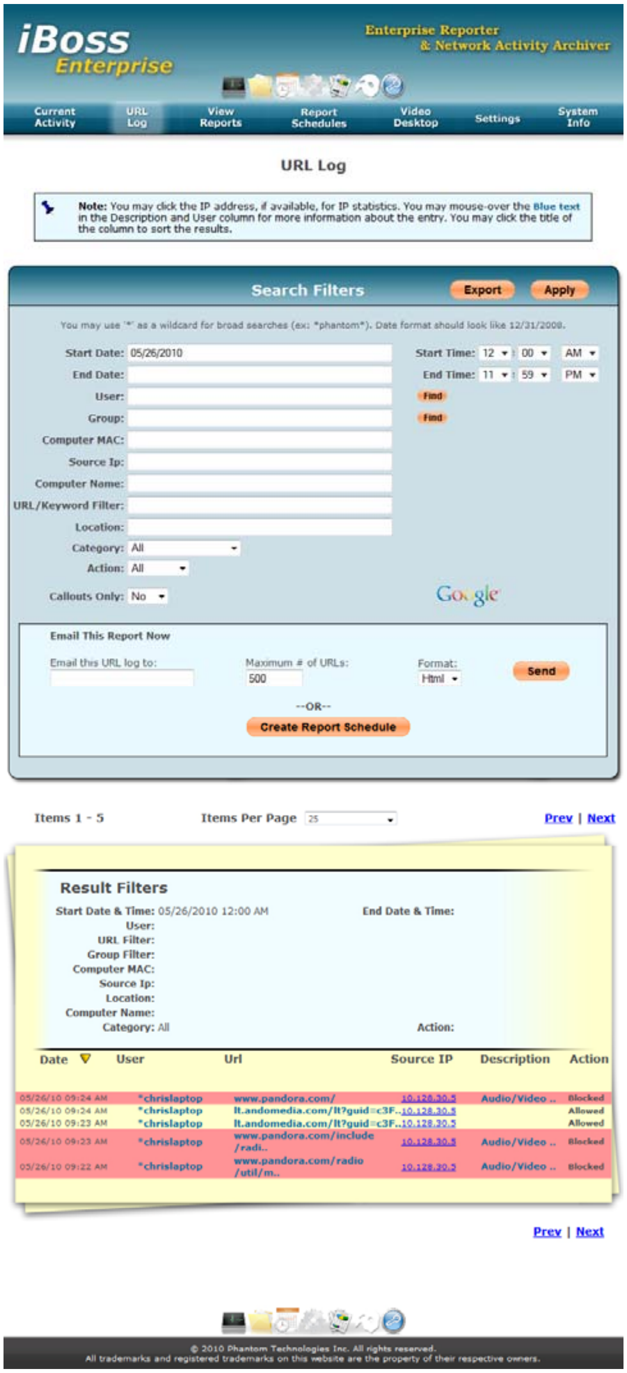
Apply

Date & Time	User	URL	Source IP	Description	Action
05/26/10 02:17 PM	*chrislapt..	tag.admeld.com/match?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	api.kickapps.com/rest/comments/5133...	10.128.30.5	Audio/Vi..	Allowed
05/26/10 02:17 PM	*chrislapt..	www.pcmag.com/light registration fo...	10.128.30.5	Shops	Allowed
05/26/10 02:17 PM	*chrislapt..	tag.admeld.com/pixel?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	tags.bluekai.com/site/1392?ret=html...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	adping.westley.crowdscience.com/fin...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	cms.quantserve.com/dpixel?id=CAESEN...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	b.scorecardresearch.com/b?c1=2&c2=6...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	pixel.quantserve.com/pixel;r=116600...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	pixel.quantserve.com/pixel;r=162034...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	meta.wikimedia.org/w/index.php?titl...	10.128.30.5	Educatio..	Allowed
05/26/10 02:17 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:17 PM	*chrislapt..	dar.youknowbest.com/Resources/905FF...	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	webcache.googleusercontent.com/sear...	10.128.30.5	Search E..	Allowed
05/26/10 02:17 PM	*chrislapt..	dar.youknowbest.com/?afid=34	10.128.30.5		Allowed
05/26/10 02:17 PM	*chrislapt..	www.google.com/url?sa=T&source=web&...	10.128.30.5	Search E..	Allowed
05/26/10 02:17 PM	*chrislapt..	pt.rewardtv.com/notice.do?sid=25000...	10.128.30.5	Audio/Vi..	Allowed
05/26/10 02:16 PM	*chrislapt..	0.70.channel.facebook.com/x/2282218...	10.128.30.5	Forums, ..	Allowed
05/26/10 02:16 PM	*sean t	us.data.toolbar.yahoo.com	10.128.31.162	Ads, Too.. "Toolbars"	Blocked
05/26/10 02:16 PM	*chrislapt..	s0.2mdn.net/1311608/728x90clicktag....	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	tag.admeld.com/pixel?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	tag.admeld.com/pixel?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	pn1.bc.yahoo.com/b?P=2NNepNj8fU8ukF...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	pn1.bc.yahoo.com/b?P=Xl3FiNj8fU8ukF...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	pn1.bc.yahoo.com/b?P=kkNnztj8fU8ukF...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	pn1.bc.yahoo.com/b?P=rONKudj8fU8ukF...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	pn1.bc.yahoo.com/b?P=3bL6Ltj8fU8ukF...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	pn1.bc.yahoo.com/b?P=Kl80Tdj8fU8ukF...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/w/index.php?title=...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*shivaji s	crm.zoho.com/crm/RelatedList.do?act...	10.128.30.117		Allowed
05/26/10 02:16 PM	*chrislapt..	en.wikipedia.org/wiki/Content-contr...	10.128.30.5	Dictiona..	Allowed
05/26/10 02:16 PM	*chrislapt..	tag.admeld.com/pixel?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	www.google.com/url?sa=T&source=web&...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	tag.admeld.com/pixel?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	tag.admeld.com/pixel?admeld adprovi...	10.128.30.5		Allowed
05/26/10 02:16 PM	*shivaji s	crm.zoho.com/crm/ShowEntityInfo.do?...	10.128.30.117		Allowed
05/26/10 02:16 PM	*chrislapt..	ar.voicefive.com/bmx3/node.pli?pub=...	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	www.pcmag.com/article2/0 2817 15327...	10.128.30.5	Shops	Allowed
05/26/10 02:16 PM	*chrislapt..	www.google.com/url?sa=T&source=web&...	10.128.30.5	Search E..	Allowed
05/26/10 02:16 PM	*chrislapt..	twitter.com/statuses/friends timeli...	10.128.30.5	Entertai..	Allowed
05/26/10 02:16 PM	*chrislapt..	lt.andomedia.com/lt?guid=c3FsMDA2fk...	10.128.30.5		Allowed
05/26/10 02:16 PM	*chrislapt..	osc.webroot.com/b/ss/webrootglobalp...	10.128.30.5	Technolo..	Allowed
05/26/10 02:16 PM	*chrislapt..	osc.webroot.com/b/ss/webrootglobalp...	10.128.30.5	Technolo..	Allowed
05/26/10 02:16 PM	*chrislapt..	www.youtube.com	10.128.30.5	Block List	Blocked

Figure 78 - Real-time URL Access Activity

5.4.2 URL Log Section

This section allows you to view the list of URLs. You may click the IP address, if available, for IP statistics. You may mouse over the Blue text in the description and User column for more information about the entry.



URL Log

Note: You may click the IP address, if available, for IP statistics. You may mouse-over the Blue text in the Description and User column for more information about the entry. You may click the title of the column to sort the results.

Search Filters

You may use '*' as a wildcard for broad searches (ex: *phantom*). Date format should look like 12/31/2008.

Start Date: 05/26/2010
Start Time: 12 : 00 AM
End Date:
End Time: 11 : 59 PM
User:
Group:
Computer MAC:
Source Ip:
Computer Name:
URL/Keyword Filter:
Location:
Category: All
Action: All
Callouts Only: No

Email This Report Now

Email this URL log to:
Maximum # of URLs: 500
Format: Html

--OR--

Items 1 - 5   Items Per Page 25   Prev | Next

Result Filters

Start Date & Time: 05/26/2010 12:00 AM
End Date & Time:
User:
URL Filter:
Group Filter:
Computer MAC:
Source Ip:
Location:
Computer Name:
Category: All
Action:

Date ▼	User	Url	Source IP	Description	Action
05/26/10 09:24 AM	*chrislaptop	www.pandora.com/	10.128.30.5	Audio/Video ..	Blocked
05/26/10 09:24 AM	*chrislaptop	lt.andomedia.com/lt?guid=c3F..	10.128.30.5		Allowed
05/26/10 09:23 AM	*chrislaptop	lt.andomedia.com/lt?guid=c3F..	10.128.30.5		Allowed
05/26/10 09:23 AM	*chrislaptop	www.pandora.com/include /radi..	10.128.30.5	Audio/Video ..	Blocked
05/26/10 09:22 AM	*chrislaptop	www.pandora.com/radio /util/m..	10.128.30.5	Audio/Video ..	Blocked

Prev | Next

© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

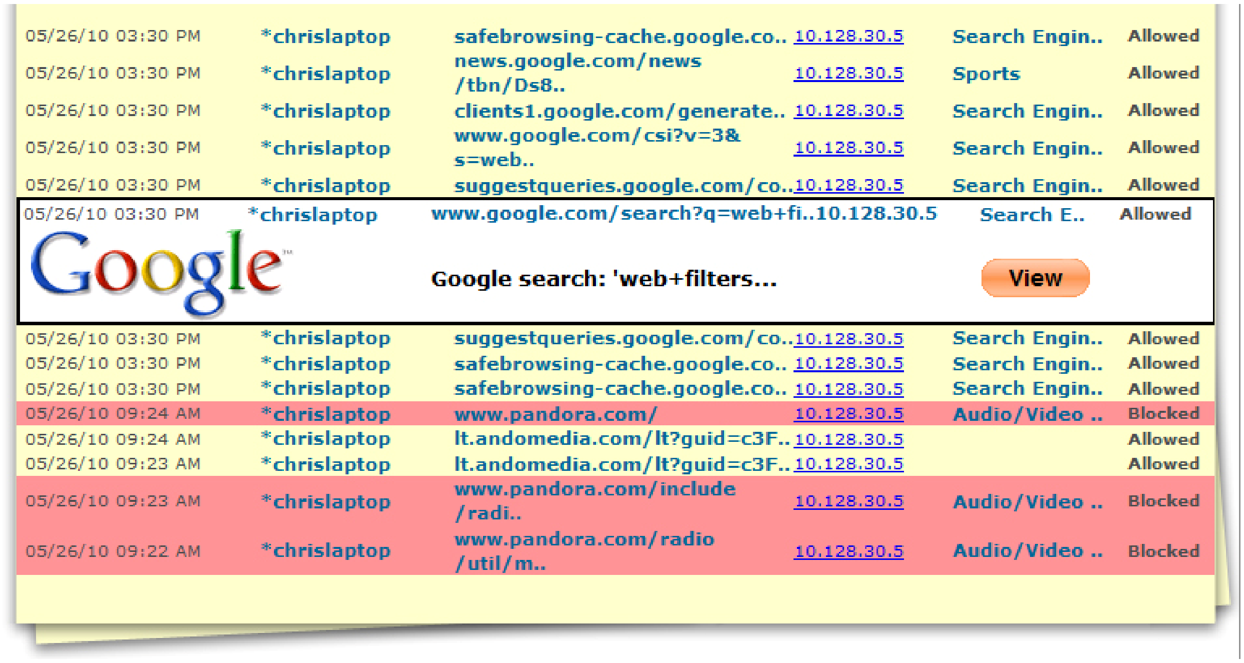
Figure 79 - URL Log

5.4.2.1 Search Filters

These filters allow hiding other URLs and only showing filters in which you'd like to see. This makes it easier to diagnose and look through the URLs. You can search for date ranges, users, groups, Mac addresses, source IP addresses, computer names, URL or keyword filter, location, category, action and callout. Once you have made these filters, click the "**Apply**" button above the search filters. You can export this You may also send this report directly from this page by entering email information under the section for Email This Report Now and clicking the "**Send**" button. You may also generate a report schedule by clicking on the "**Create Report Schedule**" button.

5.4.2.2 Site Callouts

These are callouts in which site logos are displayed and search terms are tagged. For example, sites like Google will show the logo of Google and the term that was used to search with.

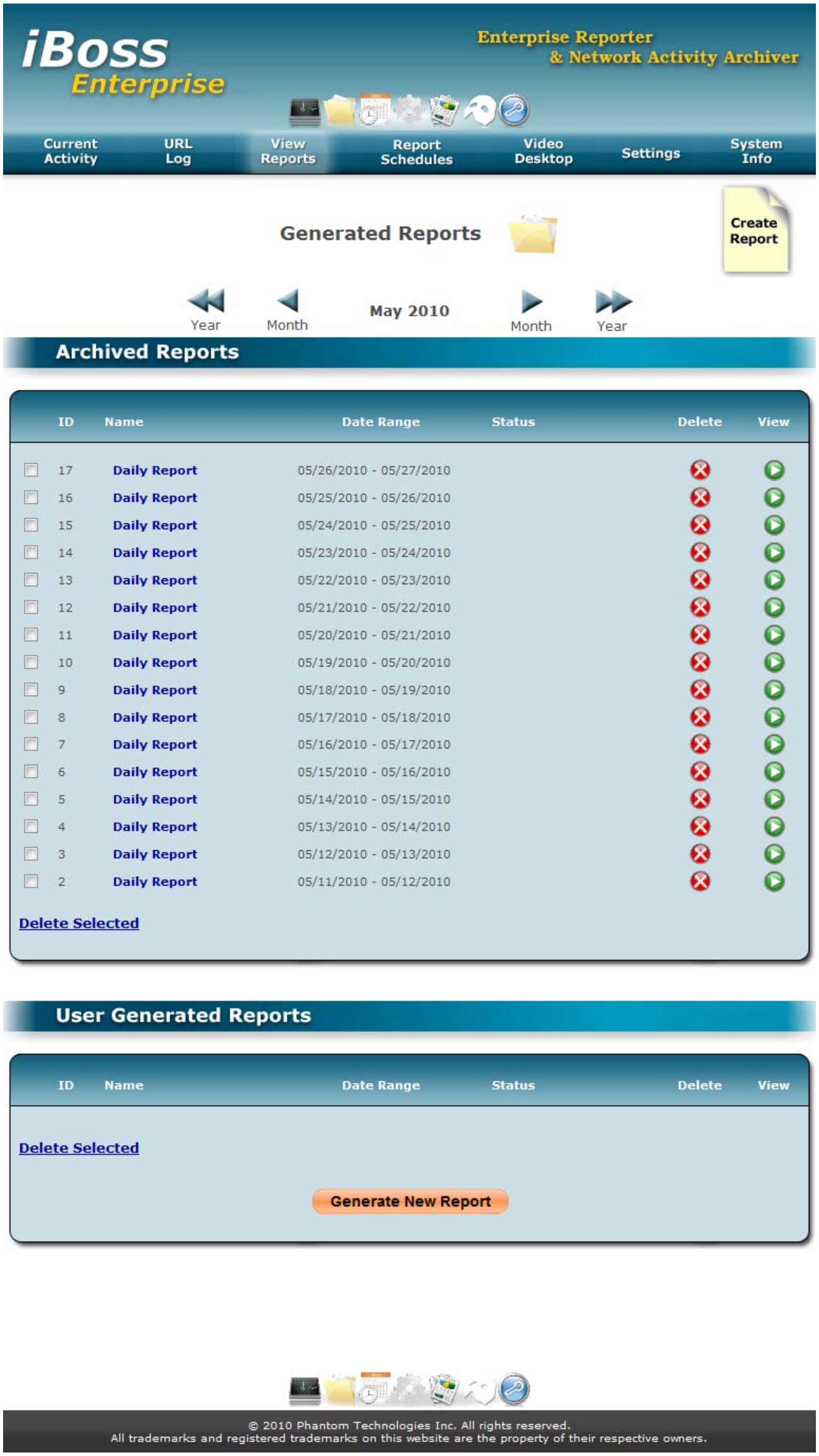


05/26/10 03:30 PM	*chrislaptop	safebrowsing-cache.google.co..	10.128.30.5	Search Engin..	Allowed
05/26/10 03:30 PM	*chrislaptop	news.google.com/news /tbn/Ds8..	10.128.30.5	Sports	Allowed
05/26/10 03:30 PM	*chrislaptop	clients1.google.com/generate..	10.128.30.5	Search Engin..	Allowed
05/26/10 03:30 PM	*chrislaptop	www.google.com/csi?v=3& s=web..	10.128.30.5	Search Engin..	Allowed
05/26/10 03:30 PM	*chrislaptop	suggestqueries.google.com/co..	10.128.30.5	Search Engin..	Allowed
05/26/10 03:30 PM	*chrislaptop	www.google.com/search?q=web+fi..	10.128.30.5	Search E..	Allowed
Google		Google search: 'web+filters...		View	
05/26/10 03:30 PM	*chrislaptop	suggestqueries.google.com/co..	10.128.30.5	Search Engin..	Allowed
05/26/10 03:30 PM	*chrislaptop	safebrowsing-cache.google.co..	10.128.30.5	Search Engin..	Allowed
05/26/10 03:30 PM	*chrislaptop	safebrowsing-cache.google.co..	10.128.30.5	Search Engin..	Allowed
05/26/10 09:24 AM	*chrislaptop	www.pandora.com/	10.128.30.5	Audio/Video ..	Blocked
05/26/10 09:24 AM	*chrislaptop	lt.andomedia.com/lt?guid=c3F..	10.128.30.5		Allowed
05/26/10 09:23 AM	*chrislaptop	lt.andomedia.com/lt?guid=c3F..	10.128.30.5		Allowed
05/26/10 09:23 AM	*chrislaptop	www.pandora.com/include /radi..	10.128.30.5	Audio/Video ..	Blocked
05/26/10 09:22 AM	*chrislaptop	www.pandora.com/radio /util/m..	10.128.30.5	Audio/Video ..	Blocked

Figure 80 - Site Callouts

5.4.3 View Reports Section

This section allows you to view the generated reports that exist within the report manager. You can generate and delete reports within this section. In addition, this is where you access individual reports for viewing. The generated reports page contains a breakdown of the auto-generated daily reports as well as the user generated reports



iBoss Enterprise
Enterprise Reporter & Network Activity Archiver
Current Activity
URL Log
View Reports
Report Schedules
Video Desktop
Settings
System Info
Create Report
Year
Month
Month
Year
Generate New Report
© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Generated Reports

May 2010

Archived Reports

	ID	Name	Date Range	Status	Delete	View
□	17	Daily Report	05/26/2010 - 05/27/2010		✖	▶
□	16	Daily Report	05/25/2010 - 05/26/2010		✖	▶
□	15	Daily Report	05/24/2010 - 05/25/2010		✖	▶
□	14	Daily Report	05/23/2010 - 05/24/2010		✖	▶
□	13	Daily Report	05/22/2010 - 05/23/2010		✖	▶
□	12	Daily Report	05/21/2010 - 05/22/2010		✖	▶
□	11	Daily Report	05/20/2010 - 05/21/2010		✖	▶
□	10	Daily Report	05/19/2010 - 05/20/2010		✖	▶
□	9	Daily Report	05/18/2010 - 05/19/2010		✖	▶
□	8	Daily Report	05/17/2010 - 05/18/2010		✖	▶
□	7	Daily Report	05/16/2010 - 05/17/2010		✖	▶
□	6	Daily Report	05/15/2010 - 05/16/2010		✖	▶
□	5	Daily Report	05/14/2010 - 05/15/2010		✖	▶
□	4	Daily Report	05/13/2010 - 05/14/2010		✖	▶
□	3	Daily Report	05/12/2010 - 05/13/2010		✖	▶
□	2	Daily Report	05/11/2010 - 05/12/2010		✖	▶

Delete Selected

User Generated Reports

ID	Name	Date Range	Status	Delete	View

Delete Selected

Figure 81 - Generated Reports Section

5.4.3.1 Report Types

Generated reports come in two basic types, auto-generated daily reports and user generated reports. Auto-generated daily reports are automatically created by the iBoss. There is one daily report generated per day that includes statistics for usage on that day. User generated reports are reports that are created by the user. These reports can contain custom date ranges, include particular groups, and include only certain statistics among other things.

5.4.3.2 Deleting Reports

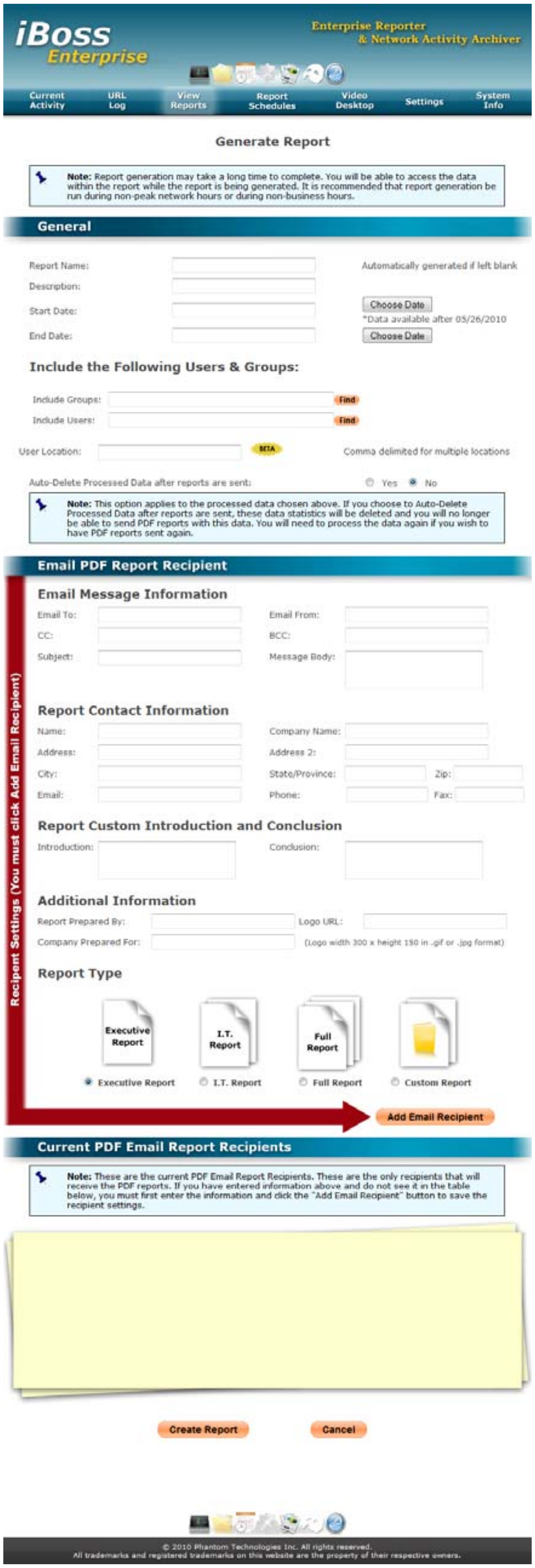
Reports are deleted as space becomes necessary, but you can select and delete any report on this page by clicking on the "Delete" button next to the report or selecting the checkboxes of the reports you wish to delete and clicking on the "Delete Selected" button. Please note that deleting reports may take a while to process as the iBoss will clean out all related data pertaining to the report.

5.4.3.3 Exporting PDF Reports

To export a report, click on the export button next to the report. This will generate a PDF Report which you can select which options to include in the report.

5.4.3.4 Generating a Report

To generate a report, click on the "Generate New Report" button toward the bottom of the list of generated reports. This will lead to a page that presents the options available when creating a report. There are many options available that can be configured when generating a report such as the included group users, the types of statistics you would like to include in the report, as well as the date range for the report.



Generate Report

Note: Report generation may take a long time to complete. You will be able to access the data within the report while the report is being generated. It is recommended that report generation be run during non-peak network hours or during non-business hours.

General

Report Name: Automatically generated if left blank

Description:

Start Date: Choose Date *Data available after 05/26/2010

End Date: Choose Date

Include the Following Users & Groups:

Include Groups:

Include Users:

User Location: Comma delimited for multiple locations

Auto-Delete Processed Data after reports are sent: ○ Yes ● No

Note: This option applies to the processed data chosen above. If you choose to Auto-Delete Processed Data after reports are sent, these data statistics will be deleted and you will no longer be able to send PDF reports with this data. You will need to process the data again if you wish to have PDF reports sent again.

Email PDF Report Recipient

Email Message Information

Email To: Email From:

CC: BCC:

Subject: Message Body:

Report Contact Information

Name: Company Name:

Address: Address 2:

City: State/Province: Zip:

Email: Phone: Fax:

Report Custom Introduction and Conclusion

Introduction: Conclusion:

Additional Information

Report Prepared By: Logo URL:

Company Prepared For: (Logo width 300 x height 150 in .gif or .jpg format)

Report Type

● Executive Report ○ I.T. Report ○ Full Report ○ Custom Report

Current PDF Email Report Recipients

Note: These are the current PDF Email Report Recipients. These are the only recipients that will receive the PDF reports. If you have entered information above and do not see it in the table below, you must first enter the information and click the "Add Email Recipient" button to save the recipient settings.

Figure 82 - Generate Report

5.4.3.4.1 *General Report Settings*

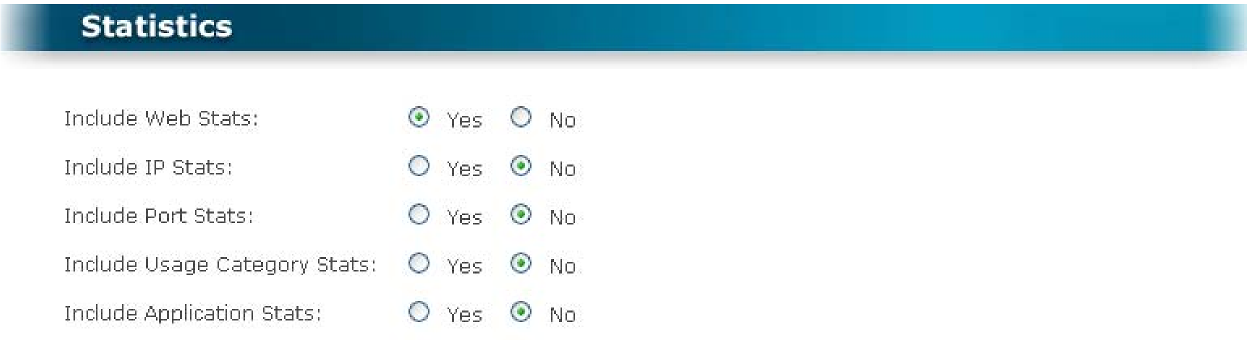
This section contains the general settings for the report to be generated. Below is a description of the options:

Report Name	This is the friendly name for the report.
Description	This allows you to enter a description for the report.
Start Date	This is the date from which to start including data for this report. All report statistics within this report will be based on this start date.
End Date	This is the end date which you wish to stop including data for the report. The end date is not included in the statistics for this report. All data up to this end date is included. The end date must be after the start date.

5.4.3.4.2 *Statistics*

This section allows you to control what type of statistics you would like to include in the report.

Note: Selecting More Performance or External Report Manager from within the iBoss Report Settings will only report Web and Bandwidth Statistics.



Statistics

Include Web Stats: ● Yes ○ No

Include IP Stats: ○ Yes ● No

Include Port Stats: ○ Yes ● No

Include Usage Category Stats: ○ Yes ● No

Include Application Stats: ○ Yes ● No

Figure 83 - Report Statistics

There are a variety of statistics that can be included. The more options that are selected, the longer it will take to generate the report. In addition, including more options will consume more of the available disk storage for the reports. Below is a description of each of the options within the statistics section.

Include Web Stats	When this option is enabled, the report will include web related statistics such as top visited domains, top blocked domain, visited URLs, blocked categories, as well other web

	browsing related statistics.
Include IP Stats (More Logging)	When this option is enabled, the report will include statistics related to IP Address accesses. This includes top visited IP Addresses, top Blocked IP Addresses, as well as other statistics related to IP Address detail.
Include Port Stats (More Logging)	When this option is enabled, the report will include statistics related to port accesses. This includes TCP and UDP accesses including top visited ports, top blocked ports, port usage by user, as well as upstream and downstream bandwidth by port.
Include Bandwidth Stats	When this option is enabled, the report will include high level bandwidth statistics related to general bandwidth usage such as overall, upstream and downstream usage.
Include Application Stats (More Logging)	When this option is enabled, the report will include usage relating to specific applications and specific usage categories.

5.4.3.4.3 *Email PDF Report Recipient*

This section allows the report to be emailed once generation is complete. Since report generation may take a while to complete, you may choose to configure these settings so that an email can be sent once the email generation process is complete to avoid having to wait for the report to complete.

5.4.3.4.3.1 Email Message Information

Enter the email information including the recipient, sender, cc, bcc, subject, and message body. This will send the email to another person which looks like it comes from you with a personalized message.

5.4.3.4.3.2 Report Contact Information

This information shows up on the cover page of the Emailed PDF Report. Enter the Name, Company Name, Address, City, State, Zip, Email, Phone and Fax.

5.4.3.4.3.3 Report Custom Introduction and Conclusion

This information shows up on the second page for the introduction and the last page which is the conclusion. Enter a custom introduction and a custom conclusion.

5.4.3.4.3.4 Additional Information

This information shows who the report was prepared by, add a logo, and who it was prepared for. This allows you to customize the report to show that you were the one who prepared it and who it was prepared for. The Logo URL allows you to add a link to an image (.gif or .jpg) to the cover page of the iBoss Report.

5.4.3.4.3.5 Report Type

This allows you to choose which type of report to send. There are four options to choose from: Executive, I.T., Full, and Custom. The Executive report has the least information in the report but is used for a quick overview. The I.T. Report show more information such as IP statistics, Port statistics, Application Statistics, and Bandwidth statistics. The Full Report shows all of the contained data. The Custom Report allows you to choose which you may choose which options to include in the report.

You may also choose to have the report automatically deleted once it is emailed. Please note that email reports only provide a high level summary of the report. If you would like to keep the report so that you can access the details and all of the drill down capability, do not select this option.

Note: You must have a configured SMTP server for the email setting to work. This is configured through "Settings" tab of the report manager.

5.4.3.4.4 *Users/Groups*

This section allows you to select which user groups you would like included in the report. The groups correspond to the iBoss Filtering Groups configured in the iBoss interface. All users within the group will be included in the report.

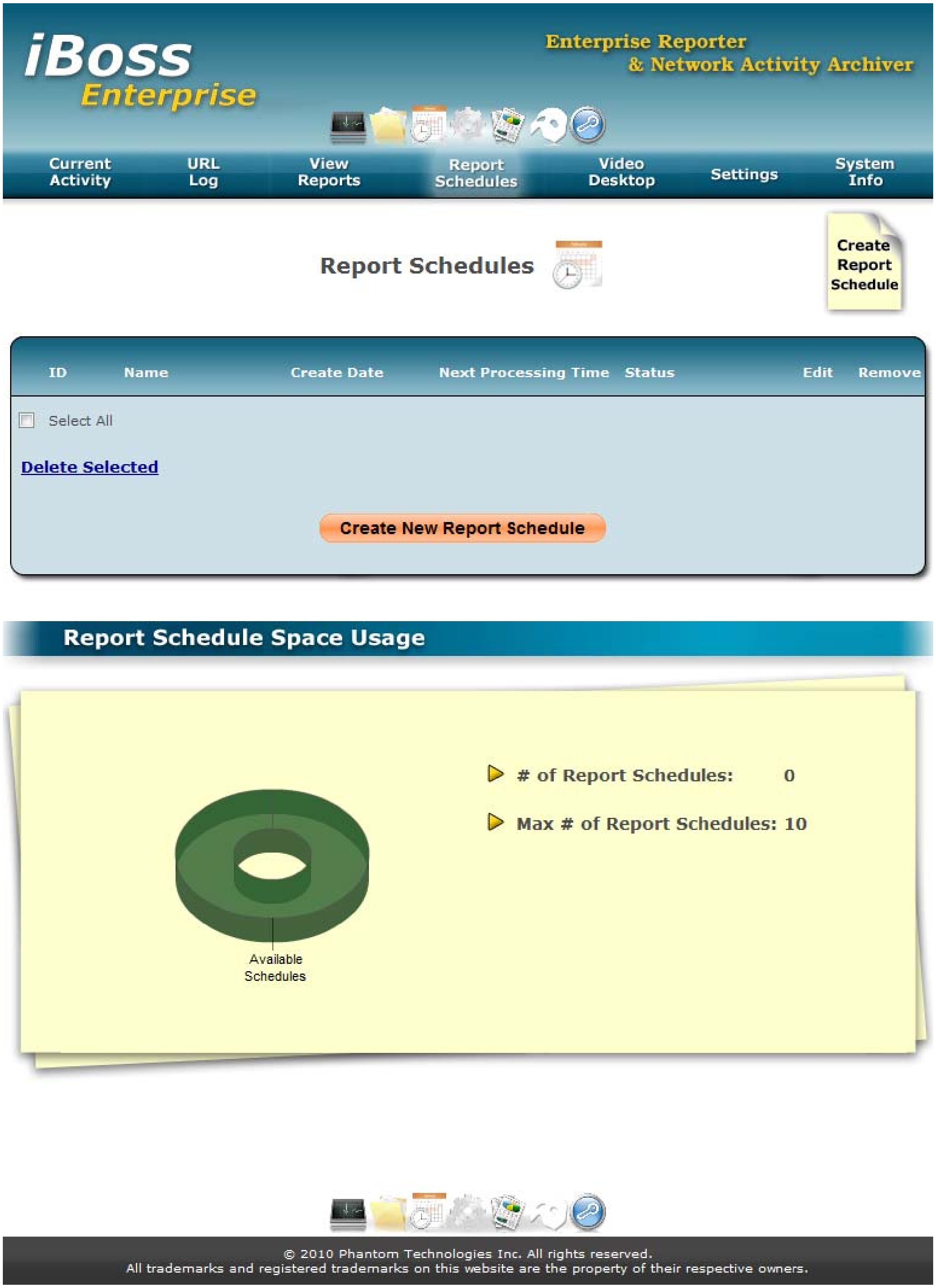
5.4.3.4.5 *Creating the Report*

Once you have configured these options, click on the "Create Report" button on the bottom of the page. This will trigger the generation of the report and take you back to the Generated Report screen. Please note that only one report generation can occur simultaneously. If there is another report generation in progress, this report will be queued and scheduled for generation.

You can view the status of the report generation by refreshing the generated reports page. To do this, click on the Generated Reports button on the top of that page. You can access the report while it is being generated, however the data will continue to change as more data is added to the report until the report generation process is complete. If the report includes the current day, statistics will continue to accumulate until the report complete at which point no more data for the current day will be added to the report.

5.4.4 Report Schedules

This section allows for the configuration of report generation schedules. Schedules allow you to generate reports for a specified interval of time and have them stored or emailed on a recurring basis. Report schedules also allow for the daily report to be emailed daily to specified recipients.



Report Schedules

ID	Name	Create Date	Next Processing Time	Status	Edit	Remove

□ Select All

Report Schedule Space Usage

- # of Report Schedules: 0
- Max # of Report Schedules: 10

© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 84 - Report Schedules

5.4.4.1 Deleting Report Schedules

You can select and delete any report schedule on this page by clicking on the “Remove” button next to the report schedule or selecting the checkboxes of the report schedules you wish to delete and clicking on the “Delete Selected” button. This will terminate the schedule immediately.

5.4.4.2 Editing Report Schedules

To edit a report schedule, click on the edit button next to the report schedule you wish to edit. This will take you to the report schedule editing screen. This screen is similar to adding a report schedule which is detailed in the next sections.

5.4.4.3 Report Schedule Processing

Report schedules are processed when the “Next Processing Time” has been reached which is detailed next to the report schedule. The scheduler will automatically adjust the next processing time automatically. If there are multiple schedules due to be processed at the same time, only one report schedule will be processed at a time. The others will be queued and each processed one at a time until all of the due schedules have been processed.

5.4.4.4 Report Schedule Types

There are two report schedule types, daily report email schedules and custom generated report schedules. Daily report email schedules allow you to email the auto-generated daily reports to specified recipients. It also allows you to enter a customized email message for the email. Custom generated report schedules allow you to create a custom report on a schedule that includes specific statistics, user groups, and more. You can additionally have the custom report emailed whenever a generation occurs.

5.4.4.5 Creating a Report Schedule

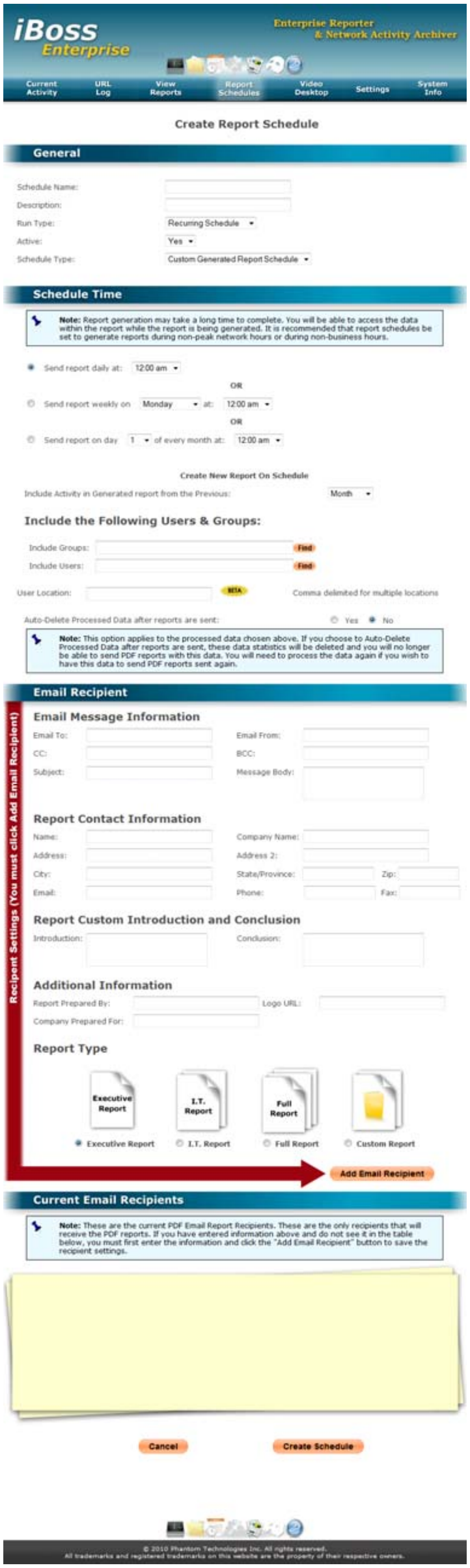
To create a report schedule, click on the “Create New Report Schedule” located at the bottom of the report schedule list.

5.4.4.5.1 *General Information*

The general information section allows you enter the following information:

Schedule Name	This is the name you would like to give this schedule.
Description	This allows for a short description of this schedule.
Run Type	This is the type of report that is chosen to be used. The options are Recurring report or Single Run Schedule.
Active	This is the option to turn the schedule active or inactive.
Schedule Type	This indicates the type of report schedule you would like to create. Report schedule types are described above. Daily report schedules allow you to email the auto-generated reports to specified email addresses while custom report schedules allow for the generation of custom reports

	on a schedule. You may also choose Url List Email Report Schedule.
Format (if Url List Email Report chosen)	This is the format in which the URL list will be emailed. Options are Html and Comma Separated Values CSV.



Create Report Schedule

General

Schedule Name:
Description:
Run Type: Recurring Schedule
Active: Yes
Schedule Type: Custom Generated Report Schedule

Schedule Time

Note: Report generation may take a long time to complete. You will be able to access the data within the report while the report is being generated. It is recommended that report schedules be set to generate reports during non-peak network hours or during non-business hours.

● Send report daily at: 12:00 am

OR

○ Send report weekly on Monday at: 12:00 am

OR

○ Send report on day 1 of every month at: 12:00 am

Create New Report On Schedule

Include Activity in Generated report from the Previous: Month

Include the Following Users & Groups:

Include Groups:
Include Users:

User Location: Comma delimited for multiple locations

Auto-Delete Processed Data after reports are sent: ○ Yes ● No

Note: This option applies to the processed data chosen above. If you choose to Auto-Delete Processed Data after reports are sent, these data statistics will be deleted and you will no longer be able to send PDF reports with this data. You will need to process the data again if you wish to have this data to send PDF reports sent again.

Email Recipient

Recipient Settings (You must click Add Email Recipient)

Email Message Information

Email To:
Email From:
CC:
BCC:
Subject:
Message Body:

Report Contact Information

Name:
Company Name:
Address:
Address 2:
City:
State/Province:
Zip:
Email:
Phone:
Fax:

Report Custom Introduction and Conclusion

Introduction:
Conclusion:

Additional Information

Report Prepared By:
Logo URL:
Company Prepared For:

Report Type

● Executive Report ○ I.T. Report ○ Full Report ○ Custom Report

Current Email Recipients

Note: These are the current PDF Email Report Recipients. These are the only recipients that will receive the PDF reports. If you have entered information above and do not see it in the table below, you must first enter the information and click the "Add Email Recipient" button to save the recipient settings.

© 2010 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 85 - Create a Report Schedule

5.4.4.5.2 *Daily Report Email Schedule Settings*

The options available for the daily report email schedule differ from the custom daily report. The daily report email schedule occurs once daily. You must specify email settings and the time you would like to have the daily report schedule processed. Daily report email schedules will contain information for the current day up to the time selected.

5.4.4.5.2.1 Report Schedule Email Settings

This section allows you to enter the details of where you would like to have the email sent to when it is ready. You can include a custom message in the email message body to create specialized reports.

5.4.4.5.2.1.1 Email Message Information

Enter the email information including the recipient, sender, cc, bcc, subject, and message body. This will send the email to another person which looks like it comes from you with a personalized message.

5.4.4.5.2.1.2 Report Contact Information

This information shows up on the cover page of the Emailed PDF Report. Enter the Name, Company Name, Address, City, State, Zip, Email, Phone and Fax.

5.4.4.5.2.1.3 Report Custom Introduction and Conclusion

This information shows up on the second page for the introduction and the last page which is the conclusion. Enter a custom introduction and a custom conclusion.

5.4.4.5.2.1.4 Additional Information

This information shows who the report was prepared by, add a logo, and who it was prepared for. This allows you to customize the report to show that you were the one who prepared it and who it was prepared for. The Logo URL allows you to add a link to an image (.gif or .jpg) to the cover page of the iBoss Report.

5.4.4.5.2.1.5 Report Type

This allows you to choose which type of report to send. There are four options to choose from: Executive, I.T., Full, and Custom. The Executive report has the least information in the report but is used for a quick overview. The I.T. Report show more information such as IP statistics, Port statistics, Application Statistics, and Bandwidth statistics. The Full Report shows all of the contained data. The Custom Report allows you to choose which you may choose which options to include in the report.

5.4.4.5.3 *Custom Generated Report Schedule Settings*

The custom report schedule settings involve configuring extra parameters in addition to those for the daily report schedule settings. The custom report schedule will generate a new report on the schedule (unlike the daily report email schedule).

5.4.4.5.3.1 General Settings

The general information section allows you enter the following information:

Schedule Name	This is the name you would like to give this schedule.
Description	This allows for a short description of this schedule.
Schedule Type	This indicates the type of report schedule you would like to create. Report schedule types are described above. Daily report schedules allow you to email the auto-generated reports to specified email addresses while custom report schedules allow for the generation of custom reports on a schedule.

5.4.4.5.3.2 Statistics

This section allows you to configure which statistics you would like in the custom generated report. The following are statistic options:

Web Stats	Web stats include statistics relating to web browsing activity. This includes top visited domains, top blocked domains, websites visited, and website category statistics.
Port Stats (More Logging)	Port Stats include statistics relating to TCP and UDP port usage on the network. This includes top used ports, top blocked ports, etc.
IP Stats (More Logging)	IP Stats include statistics relating to IP traffic on the network. This includes top accessed IP Addresses, top blocked IP Addresses, etc.
Bandwidth Stats	Bandwidth Stats include statistics relating to general bandwidth usage such as overall, downstream and upstream usage.
Application Stats (More Logging)	Application Stats include statistics specific to applications used on the network.

Note: Selecting More Performance or External Report Manager from within the iBoss Report Settings will only report Web and Bandwidth Statistics.

5.4.4.5.3.3 Email Settings

The email settings allow you to configure options relating to the emailing of the generated report. The following describes the settings in this section.

Email Report To	This is the email address where you would like the report sent to. You can use a semicolon between email addresses to add multiple recipients.
Email CC	This allows for an email carbon copy to be sent to another recipient.
Email BCC	This allows for an email blank carbon copy to be sent to another recipient.
Email Message Body	This allows you to customize the body of the email message.
Auto-delete after report is sent	If this option is enabled, the generated report will automatically be deleted once the report is emailed. This can be used to save disk space and to reduce the number of used generated reports.

5.4.4.5.3.4 Report Schedule Time

This section allows you to configure what time you would like the report schedule to run and the email report sent. There are several options for this section.

You can choose to have the report sent daily at a specified time, weekly at a specified time, or on a specific day of the month at a specified time. Select the appropriate option and configure the time you would like to have this report generated and emailed.

5.4.4.5.3.5 Users

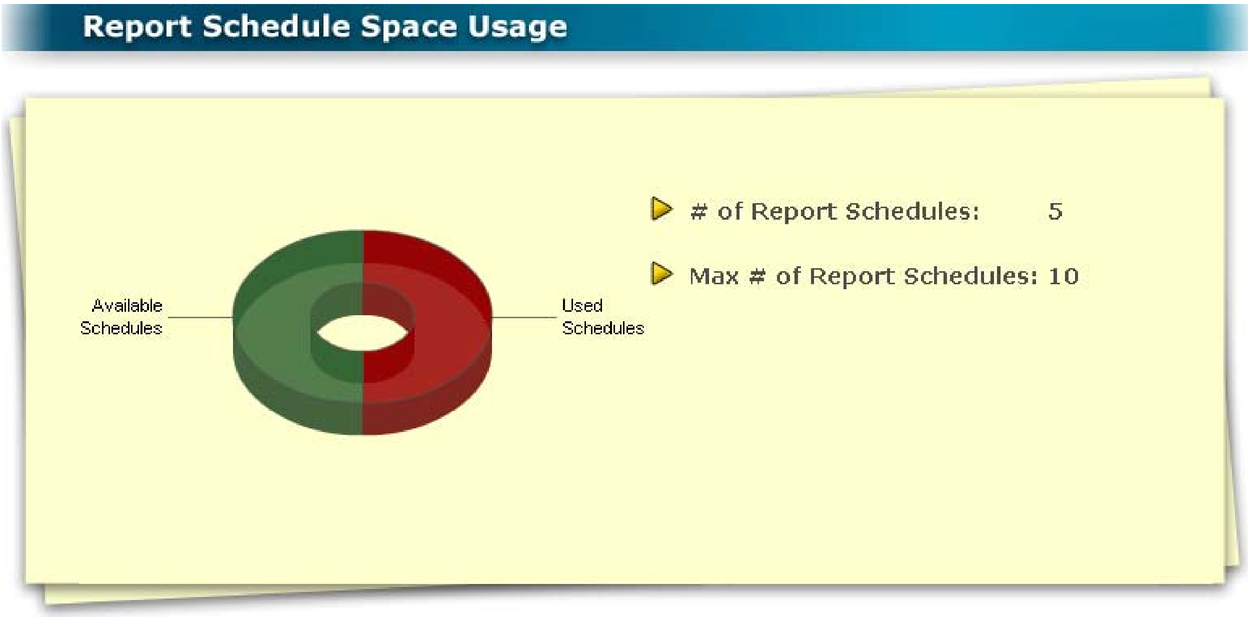
This section allows you to select which user groups will be included in the report. All users inside the selected groups will be included in the generated report. The *Other group contains miscellaneous traffic that might not have been identified on the network.

5.4.4.5.3.6 Create the Report Schedule

When you are done configuring the options for the report, click on the “Create Schedule” button on the bottom of the page. This will return you to the report schedules overview page. This page will show the next processing time for the report schedule.

5.4.4.6 Report Schedule Space Usage Section

The iBoss has a limited number of active report schedules that can be added. This section shows how many available report schedules are available for creation and how many report schedules have been created.



# of Report Schedules: 5

Max # of Report Schedules: 10

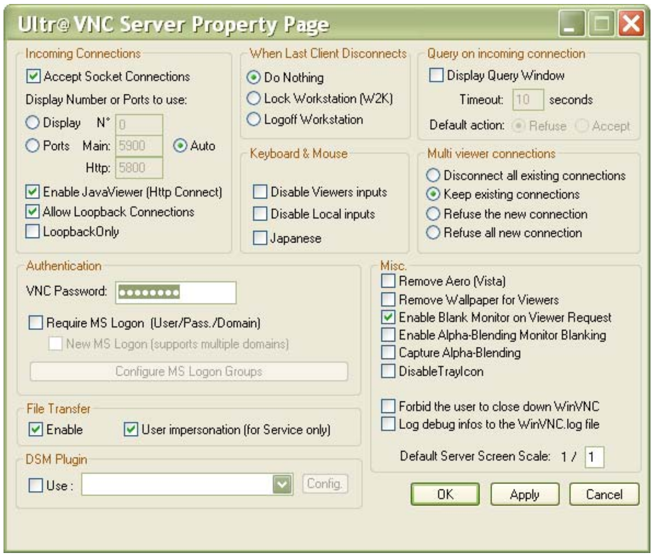
Figure 86 - Report Schedule Space Usage

5.4.5 Automatic Desktop Recording/Monitor/Control (DRMC)

This is an add-on feature to the iBoss. This section contains the setup the DRMC feature on the iBoss with the computers on your network. The recording, viewing and controlling of desktops is done by integrating with VNC. VNC (Virtual Network Computing) is a desktop sharing application that allows remote access to another computer. There are many programs that are available that offer VNC and is compatible with Mac, Windows, and Linux. We recommend using UltraVNC (uvnc.com).

5.4.5.1 Installing VNC

Once you have downloaded and installed the VNC program on the computer, you will need to configure it. If you already have it installed and setup, you will need to know the port number and password that are in the settings for the VNC program on the computer. If you are first setting it up, you may start the VNC server program and go to the Admin Properties. This will allow you to configure the port, password, and other settings of the VNC program. Please keep the settings you set for this program handy as you will need it to register the computer to the iBoss DRMC feature. Uncheck the options for Removing the wallpaper. For Multi viewer connections, select Keep existing connections and check the Allow Loopback Connections. Here is an example of recommended settings:



Ultr@VNC Server Property Page

Incoming Connections
☑ Accept Socket Connections
Display Number or Ports to use:
○ Display N° 0
○ Ports Main: 5900 ● Auto
Http: 5800
☑ Enable JavaViewer (Http Connect)
☑ Allow Loopback Connections
□ LoopbackOnly

When Last Client Disconnects
● Do Nothing
○ Lock Workstation (W2K)
○ Logoff Workstation

Keyboard & Mouse
□ Disable Viewers inputs
□ Disable Local inputs
□ Japanese

Query on incoming connection
□ Display Query Window
Timeout: 10 seconds
Default action: ● Refuse ○ Accept

Multi viewer connections
○ Disconnect all existing connections
● Keep existing connections
○ Refuse the new connection
○ Refuse all new connection

Authentication
VNC Password: ••••••••
□ Require MS Logon (User/Pass./Domain)
□ New MS Logon (supports multiple domains)
Configure MS Logon Groups

File Transfer
☑ Enable ☑ User impersonation (for Service only)

DSM Plugin
□ Use : Config.

Misc.
□ Remove Aero (Vista)
□ Remove Wallpaper for Viewers
☑ Enable Blank Monitor on Viewer Request
□ Enable Alpha-Blending Monitor Blanking
□ Capture Alpha-Blending
□ DisableTrayIcon
□ Forbid the user to close down WinVNC
□ Log debug infos to the WinVNC.log file
Default Server Screen Scale: 1 / 1

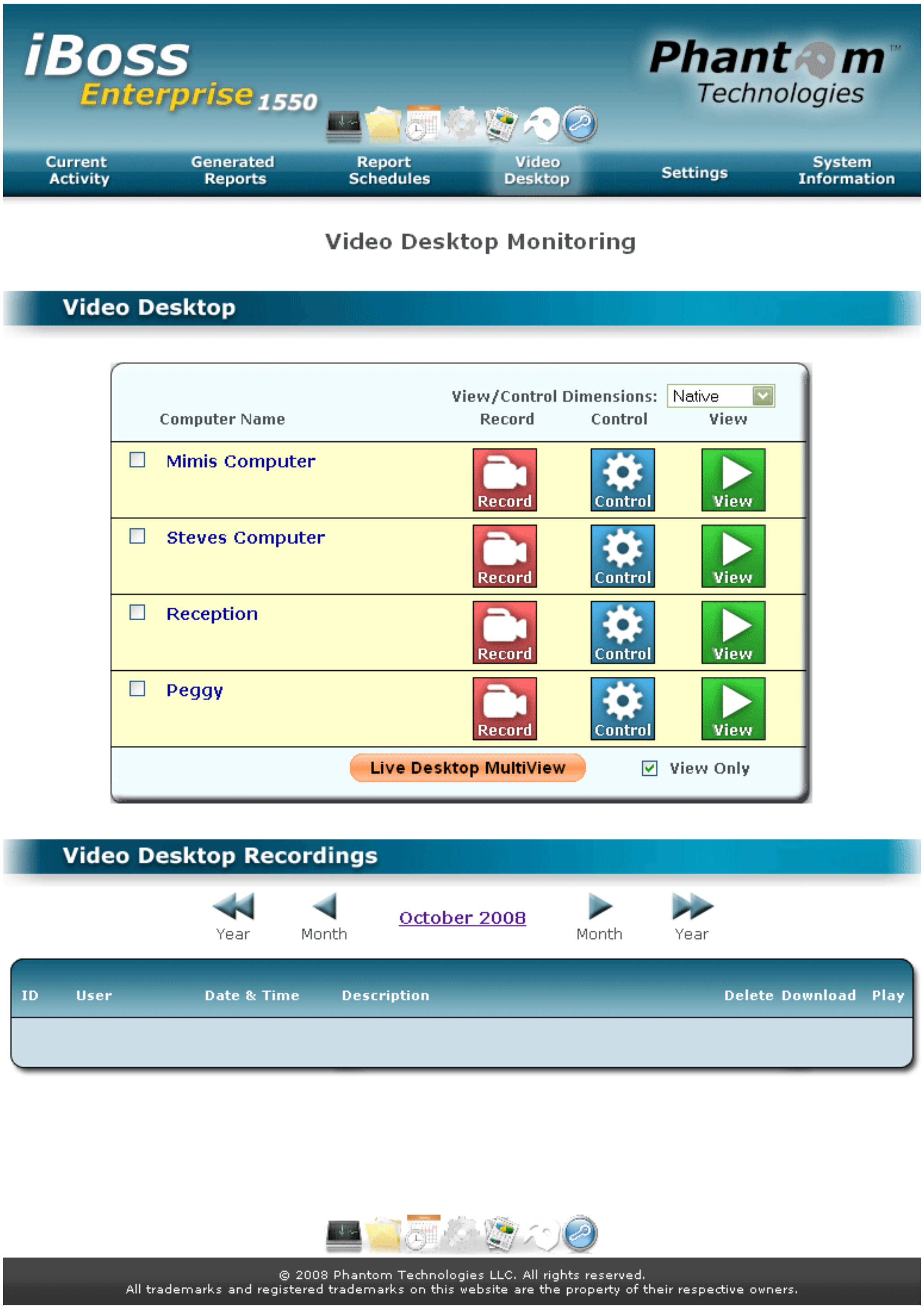
OK Apply Cancel

Figure 87 - UVNC Properties

5.4.5.2 Registering a Computer to DRMC

To register a computer to the DRMC feature, you will need to identify the computer through the iBoss. Please refer to the Identifying Computers section for more information. There will be 3 additional settings that are present when identifying computers; Enable/Disable VNC integration, VNC password, and VNC port. Enter these settings for the computer that you are identifying. Once you have identified this computer and enabled these settings, the computer will show up under the Video Desktop section of the reports.

5.4.5.3 Video Desktop



Video Desktop Monitoring

Video Desktop

View/Control Dimensions: Native

	Computer Name	Record	Control	View
□	Mimis Computer	Record	Control	View
□	Steves Computer	Record	Control	View
□	Reception	Record	Control	View
□	Peggy	Record	Control	View

☑ View Only

Video Desktop Recordings

October 2008

ID	User	Date & Time	Description	Delete	Download	Play

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 88 - Video Desktop Monitoring

This section will show you all the computers that are identified with the DRMC feature enabled. You will be able to manually Record, Control and View the desktops straight from this screen.

5.4.5.3.1 *Live Desktop MultiView*

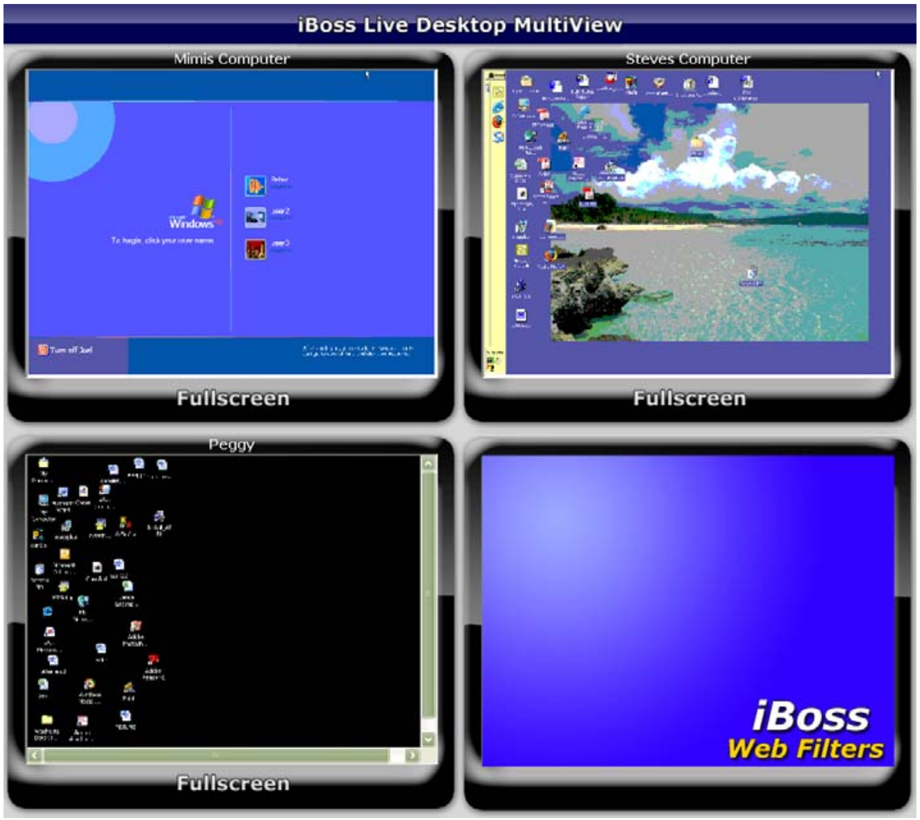


Figure 89 - Live Desktop MultiView

This option allows you to select multiple computers and view up to 10 different screens simultaneously. Select the computers you want to view and click the "Live Desktop MultiView". When viewing the desktops, you may click the Fullscreen button under any of the windows to just view one desktop.

5.4.5.4 Video Desktop Recordings

This section will store all of the desktop recordings. All of the recordings are saved as .swf (Adobe Flash) files. In this section, you may delete, download, or play the recording. Since they are .swf files, you may view them in any standard web browser (with the flash plug-in).

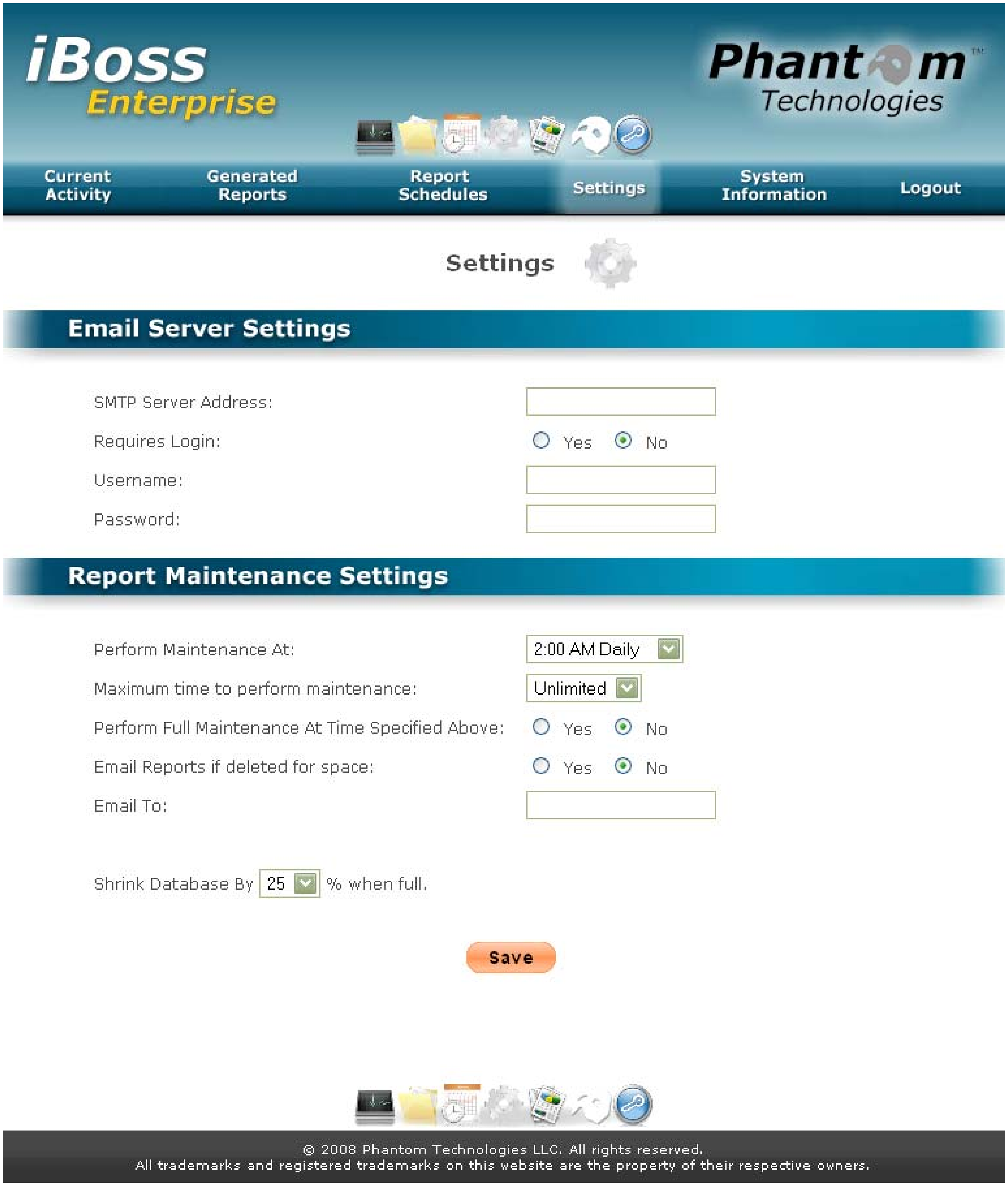
5.4.5.5 Recording Thresholds

Recording thresholds can be set to start recording a user's desktop automatically once a certain violation threshold is reached. For example, if a user goes to an Adult site 5 times within a minute, it will start recording their desktop for 1 minute. These settings can be configured within the iBoss interface, under the Report Settings in Preferences.

Please refer to the Video Desktop Recording Settings section for more information.

5.4.6 Report Manager Settings

This section contains settings used globally for the report manager which include email server settings and other configurable options. Before any email report can be sent via email, the email server settings must be configured.



Settings

Email Server Settings

SMTP Server Address:	
Requires Login:	○ Yes ● No
Username:	
Password:	

Report Maintenance Settings

Perform Maintenance At:	2:00 AM Daily
Maximum time to perform maintenance:	Unlimited
Perform Full Maintenance At Time Specified Above:	○ Yes ● No
Email Reports if deleted for space:	○ Yes ● No
Email To:	

Shrink Database By 25 % when full.

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 90 - Report Manager Settings

5.4.6.1 Email Server Settings

This section allows you to configure the SMTP server you would like the iBoss to use in order to send email reports.

SMTP Server Address	This is the domain or IP Address of the SMTP mail server you would like to use.
Requires Login	If your server requires a username and password, set this option to Yes.
Username	This is the username for servers that require login. If the “Requires Login” option is set to false, you can leave this option blank.
Password	This is the password of the user for servers that require login.

5.4.6.2 Report Maintenance Settings

These settings allow you to configure the maintenance options for the report manager. Maintenance occurs once per day.

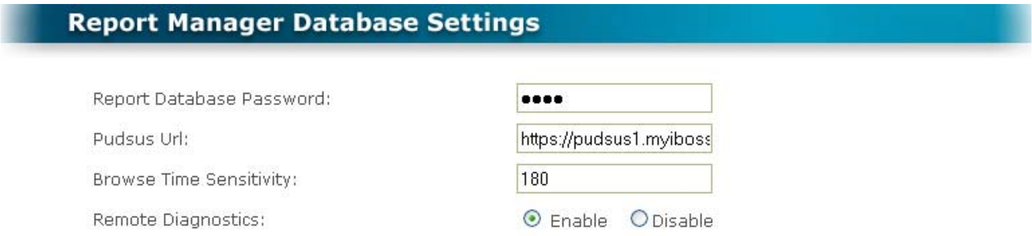
Perform Maintenance At	This is the time you would like maintenance to occur. Configure this option for a time when the network has the lightest load.
Maximum time to perform maintenance	This option allows you to limit the maximum maintenance time. Although maintenance may not take too long to complete, if the report manager is shrinking the database or performing other intensive routines, maintenance may take a long time to complete. It is important that the iBoss is given enough time to complete all of its tasks. The Unlimited option is recommended.
Perform Full maintenance at the specified time above	This option allows you to configure a full maintenance cycle to occur at the specified time. **It is highly recommended that this option is set to disabled. The report manager database will be locked if full maintenance is enabled while maintenance is taking place.**
Email Reports if deleted for space	This option allows you to have reports emailed if they need to be deleted for space.
Email To	If the above option is yes, this is the email address where you would like the report sent to.
Shrink Database By X When full	This option allows you to configure the iBoss to shrink the database by a certain percentage once the maximum has been reached.

5.4.7 External Report Manager (Enterprise Reporter) Settings

Figure 91 - External Report Manager Settings

*These settings are only in the External iBoss Enterprise Reporter.

5.4.7.1 Report Manager Database Settings (only in external report manager)



Report Manager Database Settings

Report Database Password:	••••
Pudsus Url:	https://pudsus1.myiboss
Browse Time Sensitivity:	180
Remote Diagnostics:	● Enable ○ Disable

Figure 92 - Report Manager Database Settings

These settings are only in the External iBoss Enterprise Reporter. This section allows you to configure the Enterprise Reporter Database Settings for the iBoss to report to.

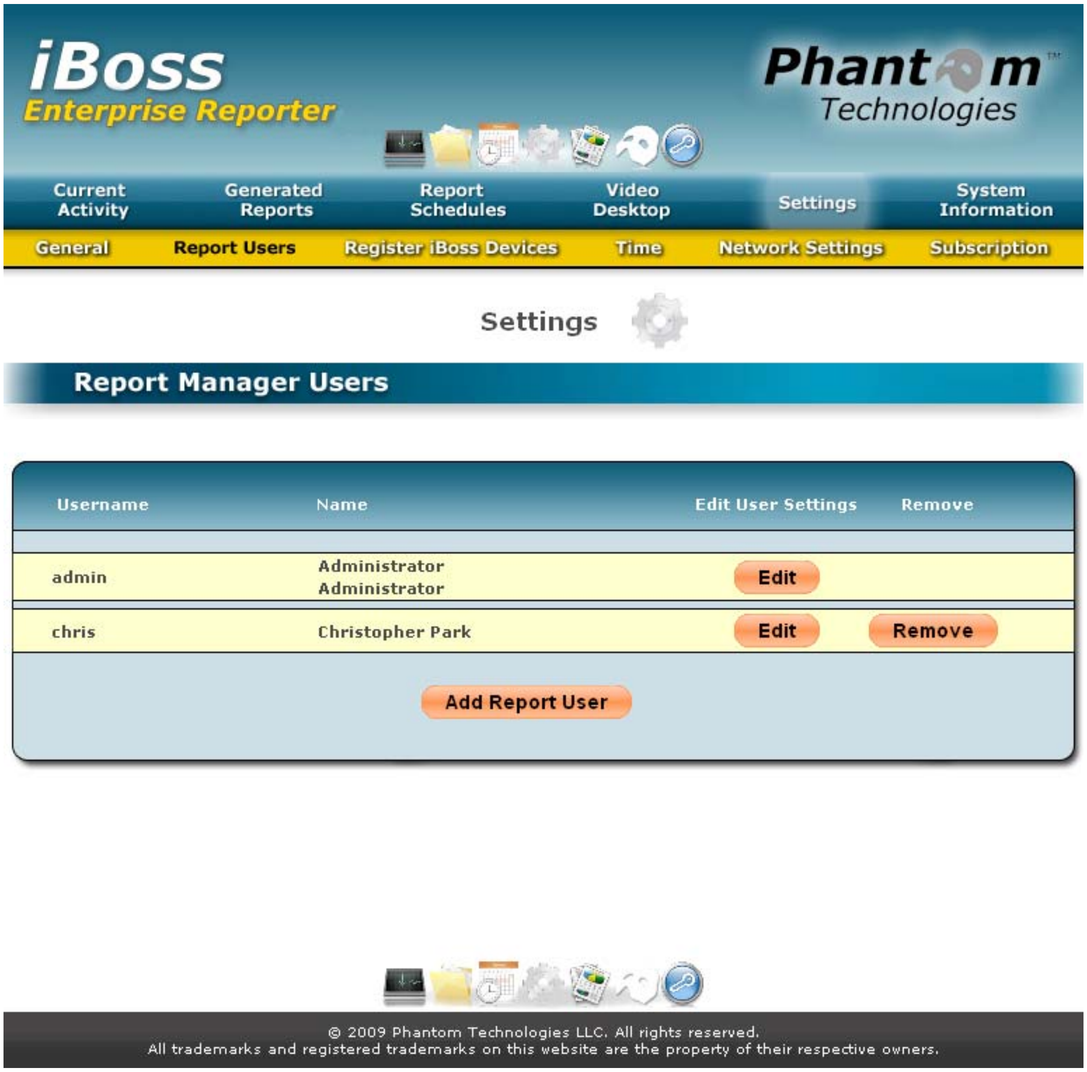
Report Database Password - The default Password is **ibossdb.** This can be left by default as the Enterprise Reporter will only allow connections from registered iBoss units however, it is recommended to change this password. Keep this password handy as you will need it to register iBoss units to it.

Pudsus Url – This is the URL where the iBoss Enterprise Reporter gets its updates from. Do not change this URL unless told to do so by a Phantom Technologies Technician. This may cause the Enterprise Reporter to function improperly if changed.

Browse Time Sensitivity – This option is for the time usage statistics of how long a URL is counted as being viewed after first accessed. This is only if there is no more traffic after hitting a website as it limits to this amount in seconds.

Remote Diagnostics – This option allows you to enable Remote Diagnostics for a Phantom Technologies technician to assist you remotely.

5.4.7.2 Report Users (only in external report manager)



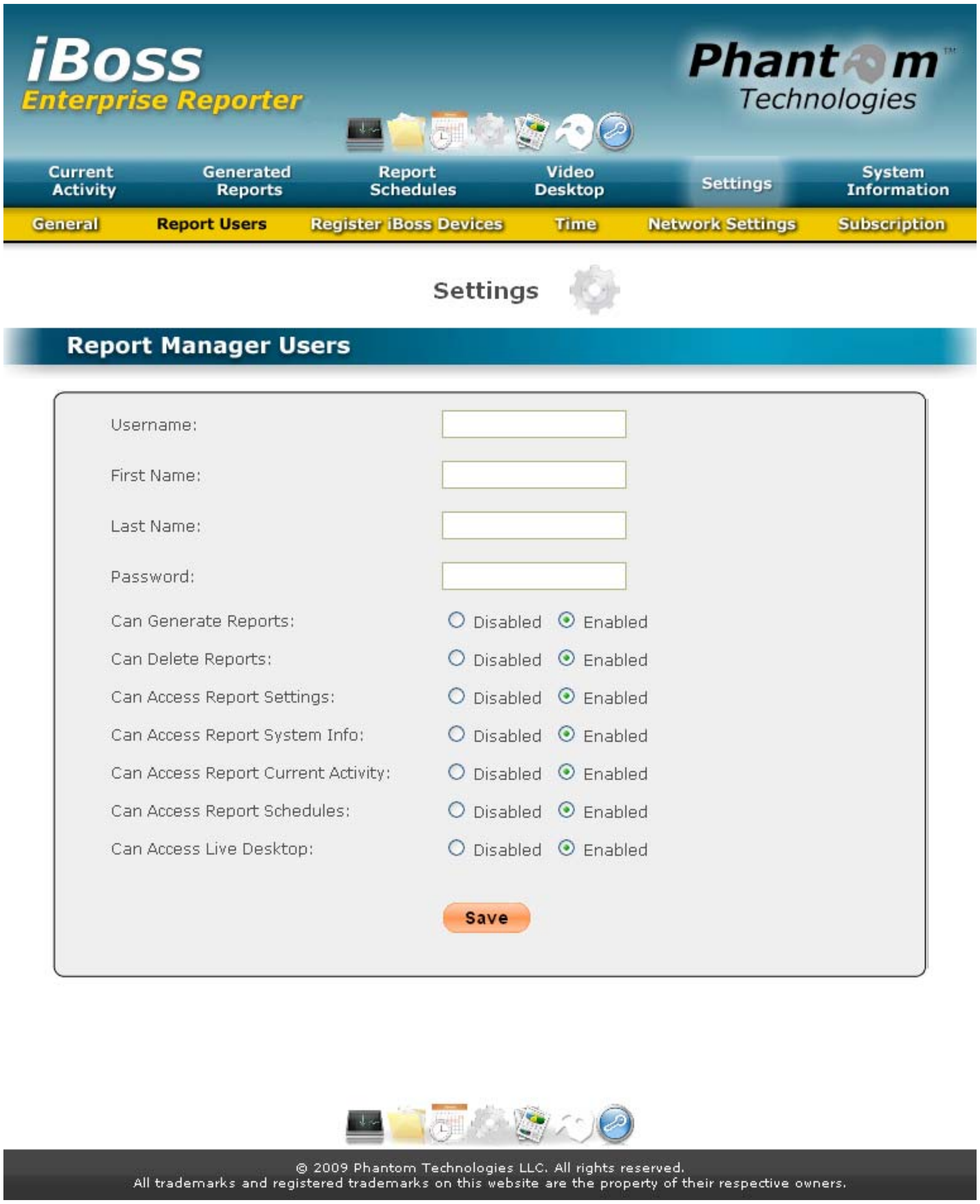
Username	Name	Edit User Settings	Remove
admin	Administrator Administrator	Edit	
chris	Christopher Park	Edit	Remove

Figure 93 - Report Users

This section allows you to add/edit users that can log into the Enterprise Reporter. The default user is “**admin**” which has no password by default. It is recommended to click “Edit” and set a password for the Administrator.

To add a user, click Add Report User

5.4.7.2.1 *Add Report User*



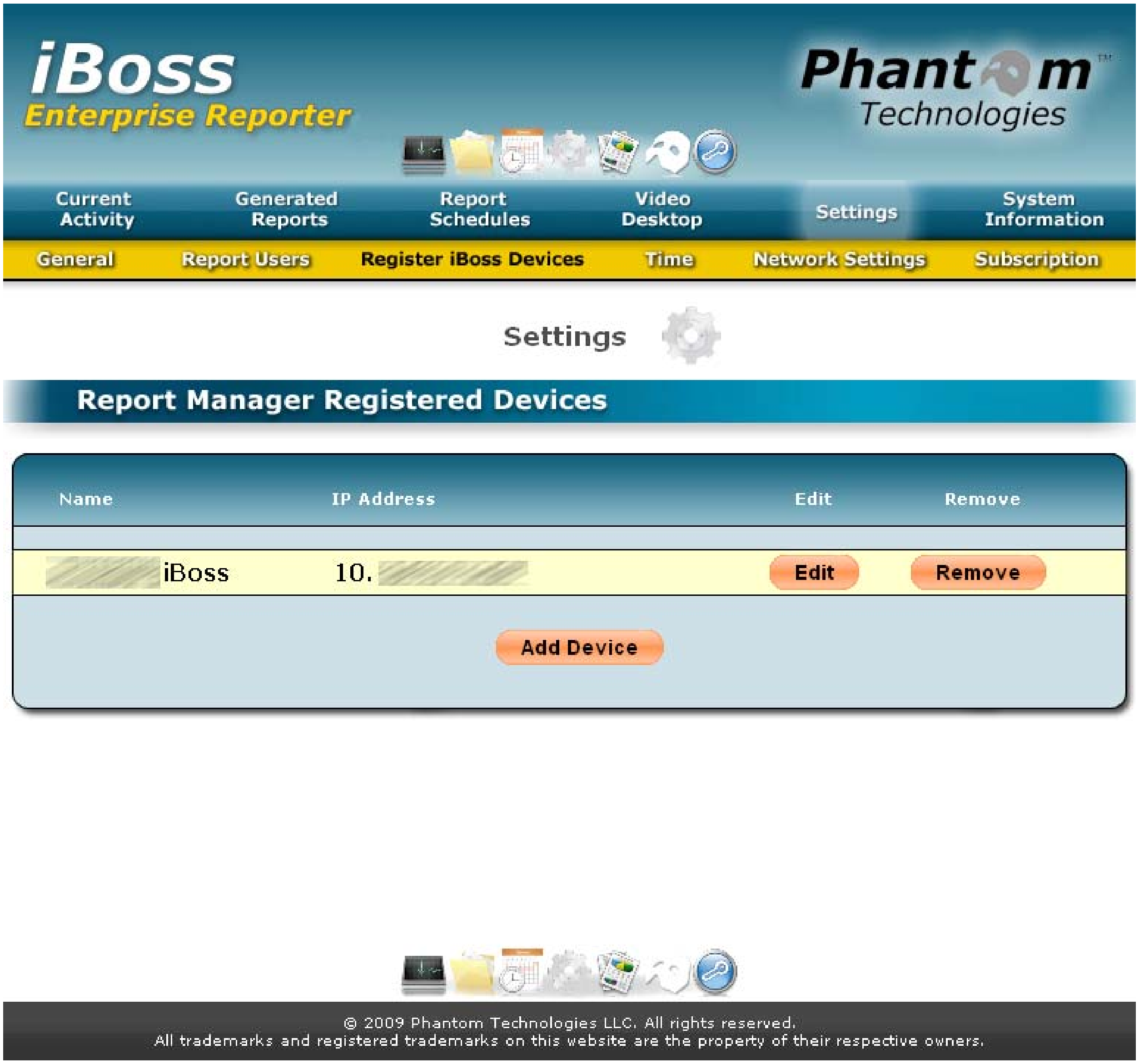
Username:		
First Name:		
Last Name:		
Password:		
Can Generate Reports:	○ Disabled	● Enabled
Can Delete Reports:	○ Disabled	● Enabled
Can Access Report Settings:	○ Disabled	● Enabled
Can Access Report System Info:	○ Disabled	● Enabled
Can Access Report Current Activity:	○ Disabled	● Enabled
Can Access Report Schedules:	○ Disabled	● Enabled
Can Access Live Desktop:	○ Disabled	● Enabled

Figure 94 - Add Report Manager User

To add a user, enter the Username, First Name, Last Name, and Password. Then select which sections of the report the user can access. The options to choose from are Can Generate Reports, Can Delete Reports, Can Access Report Settings, Can Access Report System Info, Can Access Report Current Activity, Can Access Report Schedules, and Can Access Live Desktop.

After you are done settings all of the settings, click Save.

5.4.7.3 Register iBoss Devices (only in external report manager)



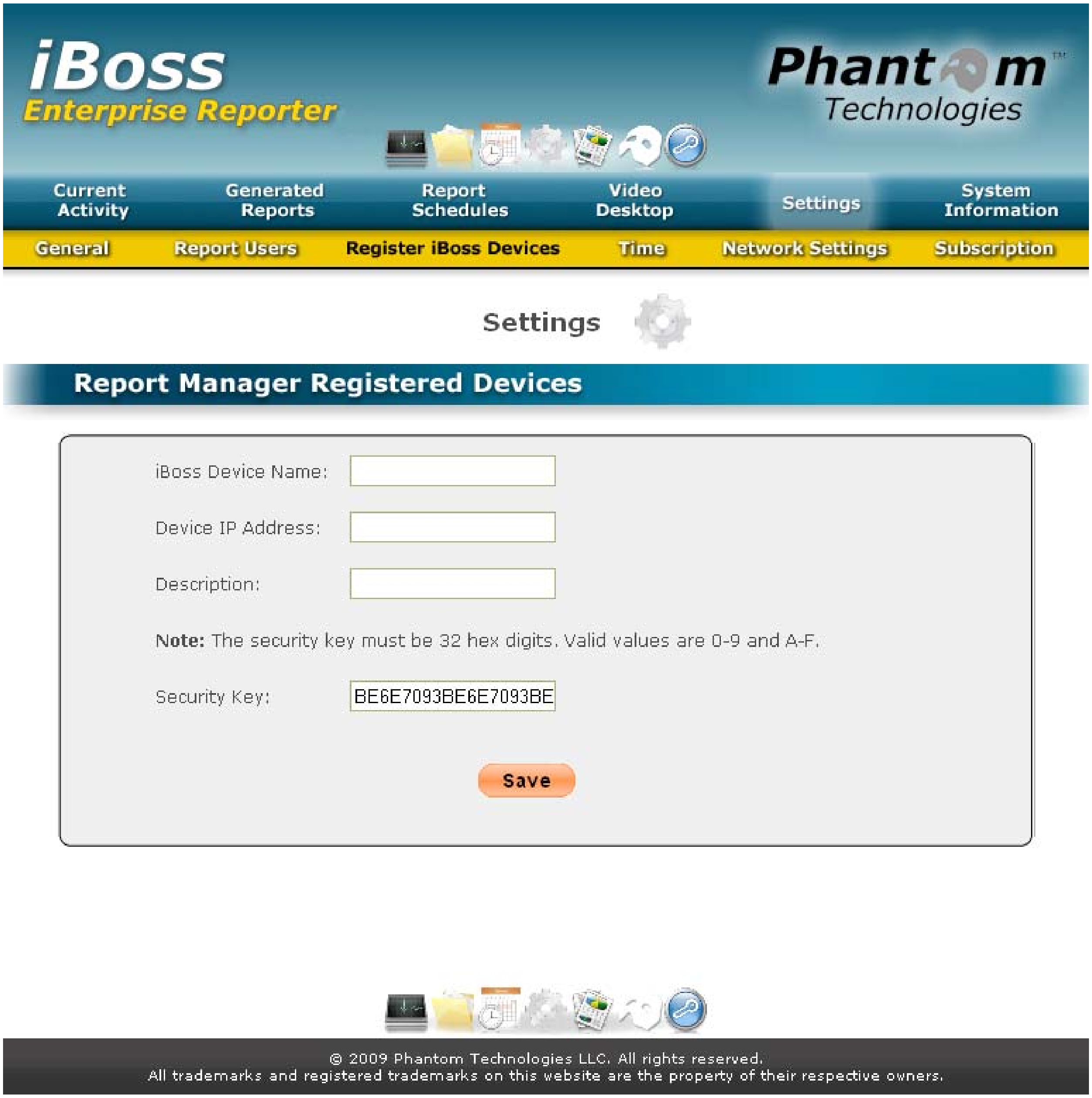
Name	IP Address	Edit	Remove
[redacted] iBoss	10. [redacted]	Edit	Remove

Figure 95 - Register iBoss Devices

This section allows you to add/edit/remove iBoss Devices to log to the external Report Manager. You will need to register any iBoss devices that you wish to have reporting to the external report manager.

To add an iBoss Device, click Add Device.

5.4.7.3.1 *Register an iBoss Device*



iBoss Device Name:

Device IP Address:

Description:

Note: The security key must be 32 hex digits. Valid values are 0-9 and A-F.

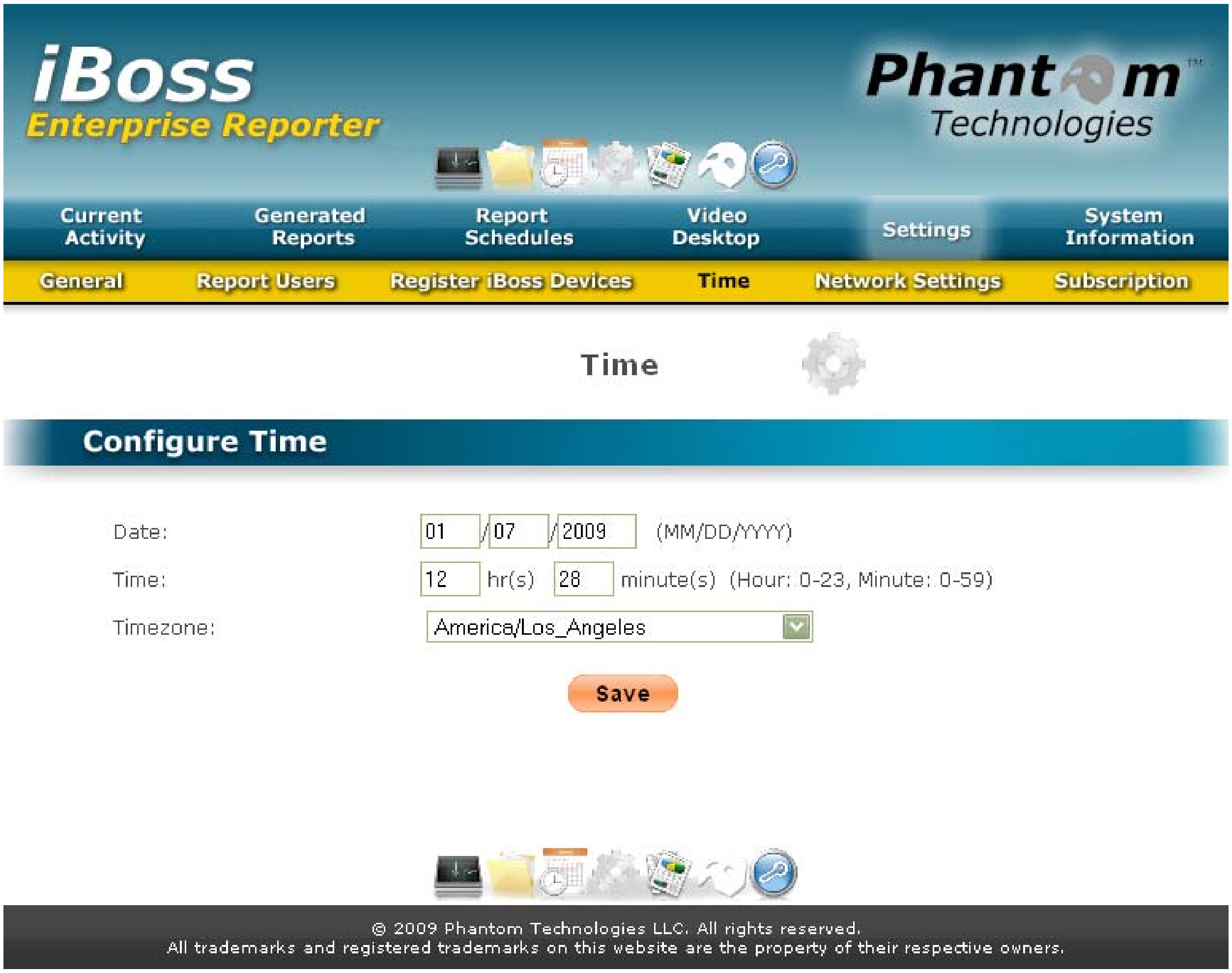
Security Key: BE6E7093BE6E7093BE

Figure 96 – Register an iBoss Device

To add an iBoss Device, enter the iBoss Device Name, Device IP Address, Description, and Security key. You may change the security key to a 32 hex digit key. **Please keep this key handy as you will need it when registering the iBoss settings to point to the external report manager.**

Please refer to the Report Settings of the iBoss Interface for instructions on how to configure the External Report Manager Settings.

5.4.7.4 Configure Time (only in external report manager)



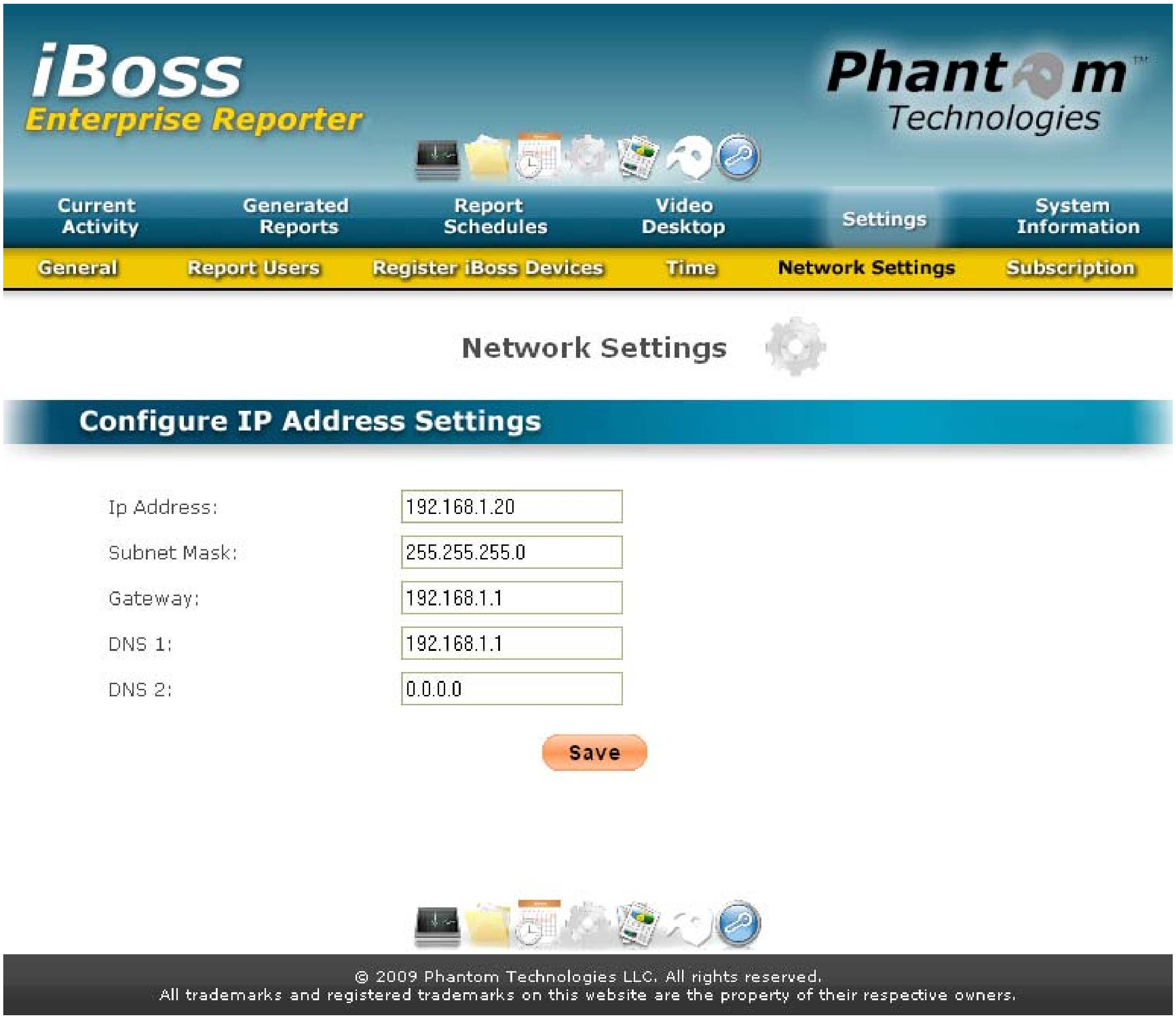
Date:	01 / 07 / 2009 (MM/DD/YYYY)
Time:	12 hr(s) 28 minute(s) (Hour: 0-23, Minute: 0-59)
Timezone:	America/Los_Angeles

Save
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 97 - Configure Time

This section allows you to set the time zone and time for the external report manager. After changing the correct time zone, click Save. The iBoss Enterprise Reporter will need to reboot after saving.

5.4.7.5 Network Settings (only in external report manager)



iBoss Enterprise Reporter
Phantom Technologies
Current Activity
Generated Reports
Report Schedules
Video Desktop
Settings
System Information
General
Report Users
Register iBoss Devices
Time
Network Settings
Subscription
Network Settings
Configure IP Address Settings

Ip Address: 192.168.1.20
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
DNS 1: 192.168.1.1
DNS 2: 0.0.0.0

Save
© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 98 - Configure IP Address Settings

This section allows you to set the network settings for the external report manager. You may set the IP address, Subnet Mask, Gateway, DNS 1, and DNS 2. After entering the settings, click Save. The iBoss Enterprise Reporter will need to reboot after saving.

Default iBoss Enterprise Reporter IP Address Settings

IP Address	192.168.1.20
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS 1	192.168.1.1
DNS 2	0.0.0.0

You may set these settings through the serial console. Please refer to the serial console settings in the iBoss serial console section.

5.4.7.6 Subscription (only in the external report manager)

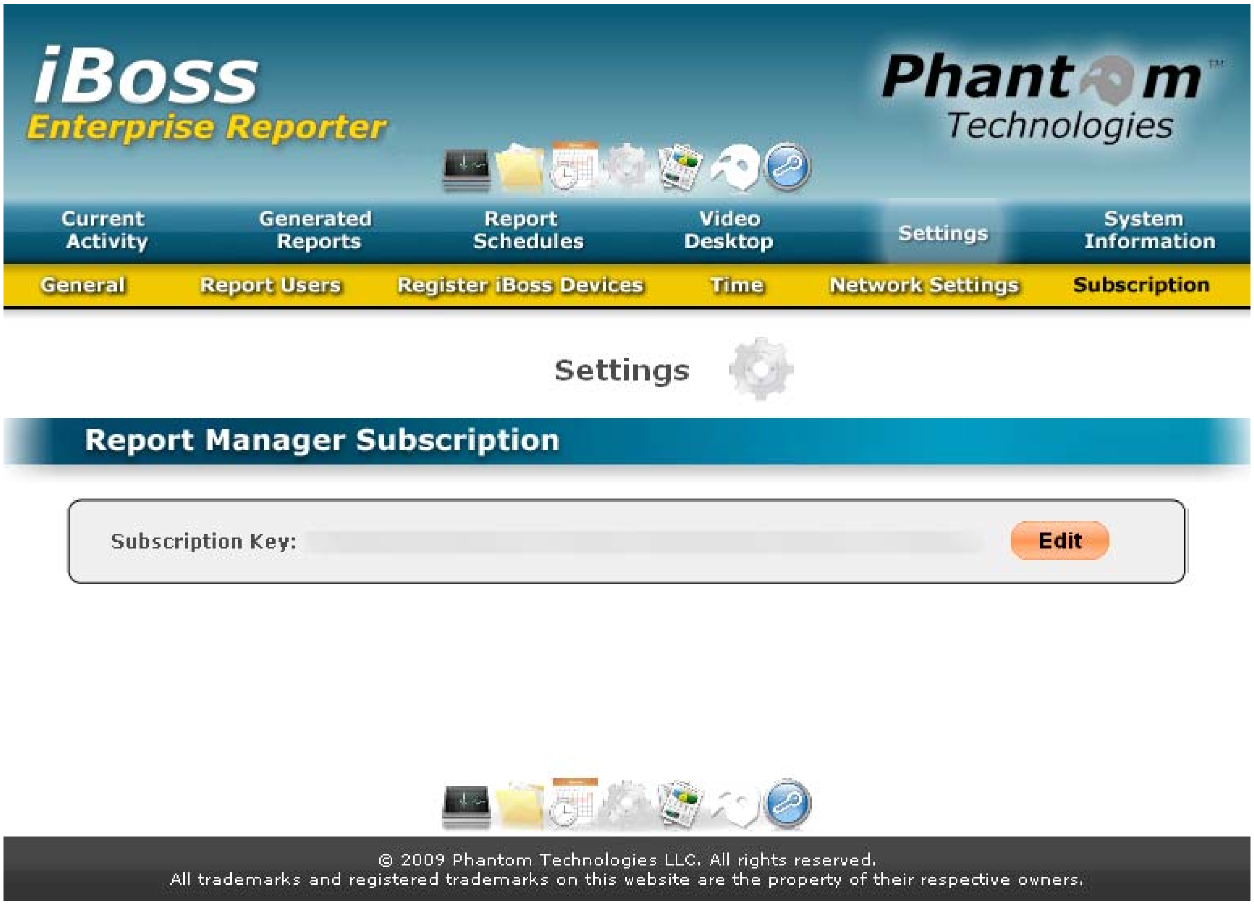


Figure 99 – Subscription

This section allows you to enter the subscription key. You may click Edit to enter the key. Once you enter the key click Edit to save the key and then Confirm. The report manager will need to be connected to the Internet to be able to confirm this key. Please make sure it is plugged into the network to be able to verify the subscription key.

Note: The report manager will not process log data and will not fully function if your subscription is not active.

5.4.8 Report Manager System Information

This section contains system information pertaining to the iBoss. This includes the system log, the system uptime, and the database size. From this page, you can view and clear the system event log. In addition, you can view how much disk space the report manager is consuming and how much disk space is available. When the maximum is reached, the database will automatically shrink on the maintenance interval.

5.5 Viewing Reports

You may view reports by clicking on the report you wish to view from the "Generated Reports" section of the report manager. When you click on the report, you will be taken to the web statistics section of the report.

There are five main subsections in the reports; Web, Port Statistics, IP Statistics, Bandwidth Statistics, and Application Statistics. They are described below.

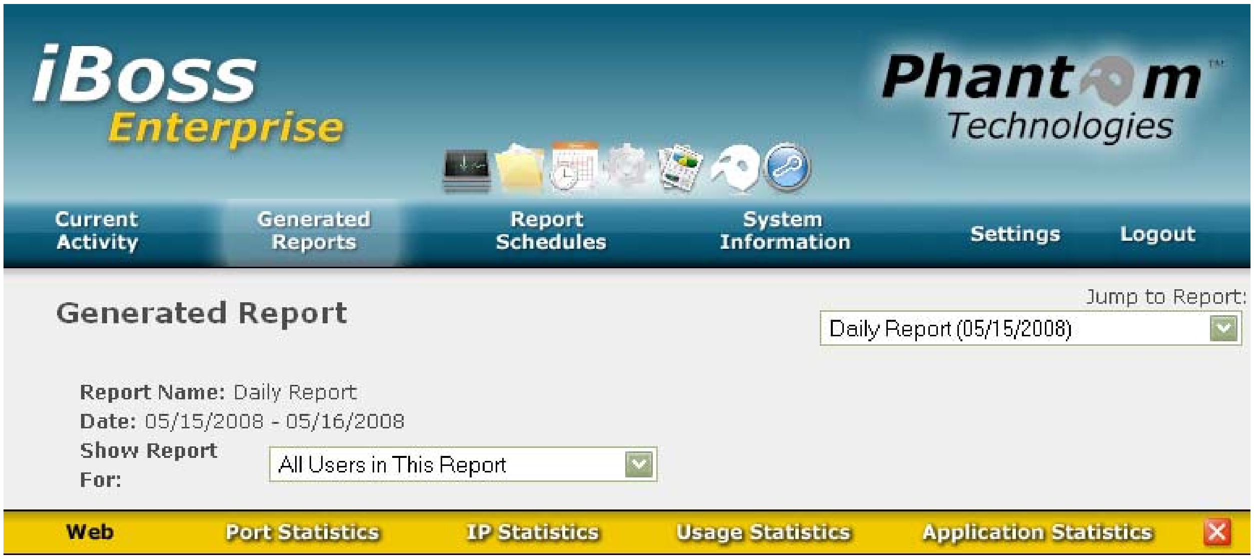
Note: The Port, IP, and Application Stats are not visible when in High Performance Mode and while using an External Report Manager.

Web Stats	Web stats include statistics relating to web browsing activity. This includes top visited domains, top blocked domains, websites visited, and website category statistics.
Port Stats	Port Stats include statistics relating to TCP and UDP port usage on the network. This includes top used ports, top blocked ports, etc.
IP Stats	IP Stats include statistics relating to IP traffic on the network. This includes top accessed IP Addresses, top blocked IP Addresses, etc.
Bandwidth Stats	Bandwidth Stats include statistics relating to general bandwidth usage such as overall, downstream and upstream usage.
Application Stats	Application Stats include statistics specific to applications used on the network.

Most of the items within the report manager are "clickable". The report manager allows deep drilldown functionality to provide very detailed information very easily.

5.5.1 Report Information Section

When viewing any of the report pages, the report information section will be visible at the top of the page. This section gives you information regarding the current report and allows you to switch between reports easily.



Generated Report

Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Figure 100 - Report Information Section

The report information bar contains the name of the report, as well as the date range that this report covers.

5.5.1.1 Showing Report Information for Particular Users

Under the option "Show Report For", you have the capability of selecting which report information is presented on the page. If "All Users in This Report" is selected, the information in the report pages you are viewing will contain information regarding all users in the report.

If you would like to view information for a particular user in the report, select the user from the drop down list. Only users that belong to the groups included in the report will be show here. Once a user is selected, all statistics on the page pertain to the particular user.

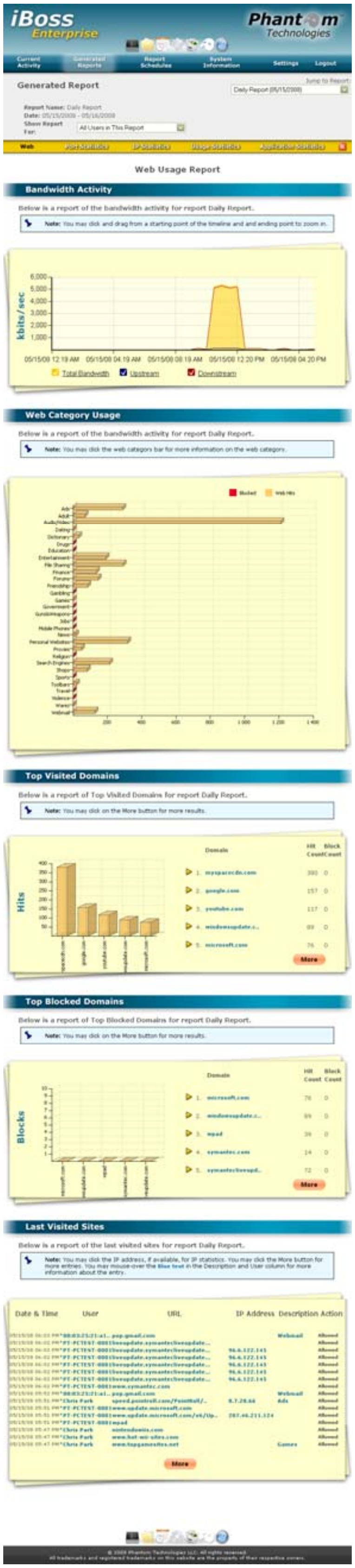
Regardless of whether you have all users selected or a particular user, the information presented will look the same and is consistent. The only thing that changes is the information on the page, not the structure.

5.5.1.2 Quickly switching between reports

The top right section of the report information bar has a drop down list which allows you to quickly switch between reports. Simply select a report from the drop down list and the current report page will be updated with the information from the newly selected report. This is useful for comparing information between two or more reports.

5.5.2 Web Usage Statistics

This section contains information related to web browsing. This includes websites visited, top visited domains, top blocked domains, web category usage as well as other statistics. As stated above, most of the items are clickable and can be drilled down for more detail.



Generated Report

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Web Usage Report

Bandwidth Activity

Below is a report of the bandwidth activity for report Daily Report.

Note: You may click and drag from a starting point of the timeline and and ending point to zoom in.

Web Category Usage

Below is a report of the bandwidth activity for report Daily Report.

Note: You may click the web category bar for more information on the web category.

Top Visited Domains

Below is a report of Top Visited Domains for report Daily Report.

Note: You may click on the More button for more results.

Domain	Hit Count	Block Count
1. myspacecdn.com	380	0
2. google.com	157	0
3. youtube.com	117	0
4. windowsupdate.c...	89	0
5. microsoft.com	76	0

Top Blocked Domains

Below is a report of Top Blocked Domains for report Daily Report.

Note: You may click on the More button for more results.

Domain	Hit Count	Block Count
1. microsoft.com	78	0
2. windowsupdate.c...	89	0
3. wpad	39	0
4. symantec.com	14	0
5. symantecliveupd...	72	0

Last Visited Sites

Below is a report of the last visited sites for report Daily Report.

Note: You may click the IP address, if available, for IP statistics. You may click the More button for more entries. You may mouse-over the Blue text in the Description and User column for more information about the entry.

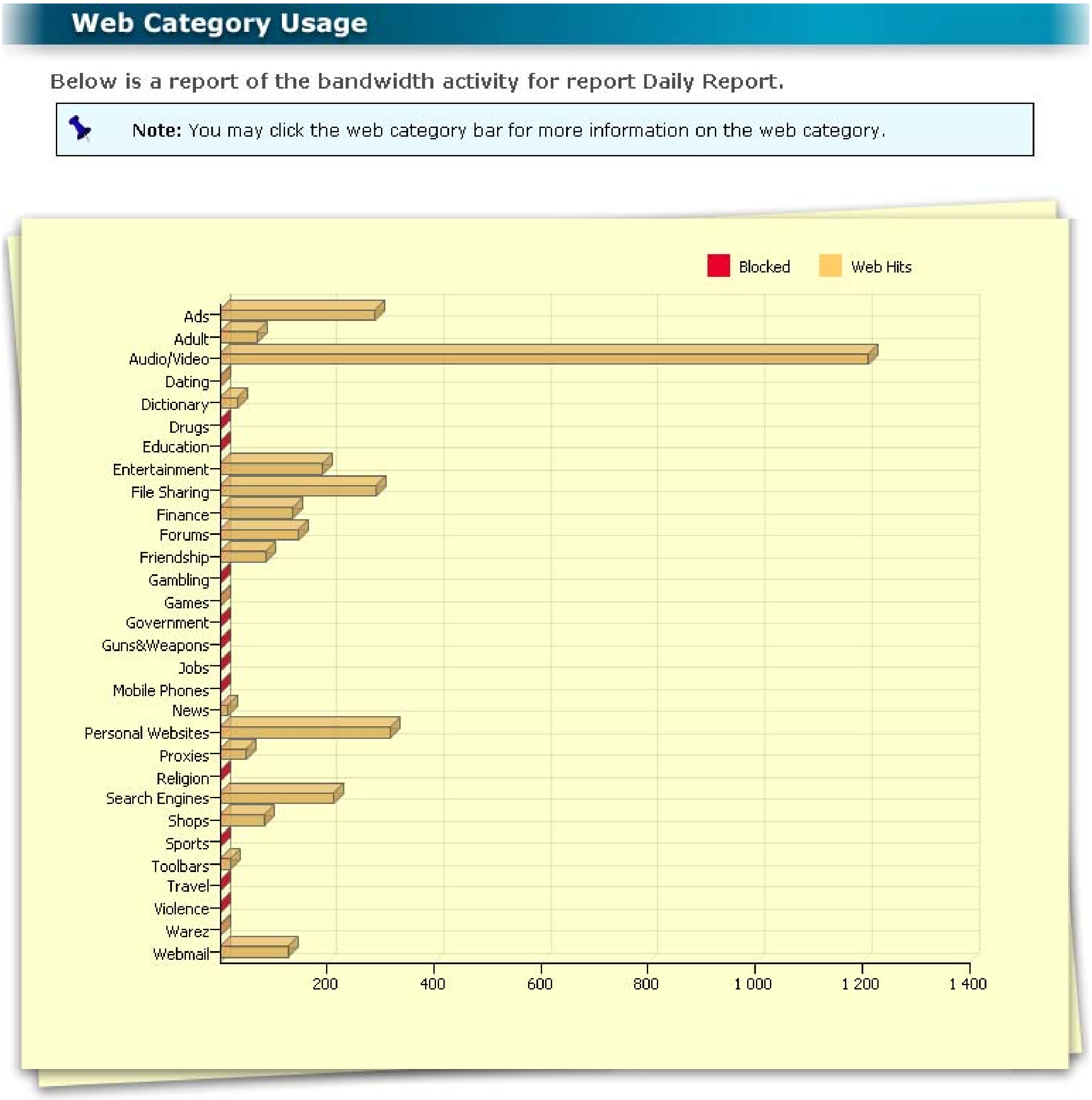
Date & Time	User	URL	IP Address	Description	Action
05/15/08 04:03 PM	*00:03:25:21:a1...	pop.gmail.com		Webmail	Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...			Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 04:02 PM	*PT-PCTEST-0001	www.symantec.com			Allowed
05/15/08 03:52 PM	*00:03:25:21:a1...	pop.gmail.com		Webmail	Allowed
05/15/08 03:51 PM	*Chris Park	speed.pointroll.com/PointRoll/...	8.7.28.66	Ads	Allowed
05/15/08 03:51 PM	*PT-PCTEST-0001	www.update.microsoft.com			Allowed
05/15/08 03:51 PM	*PT-PCTEST-0001	www.update.microsoft.com/v6/Up...	207.46.211.124		Allowed
05/15/08 03:51 PM	*PT-PCTEST-0001	wpad			Allowed
05/15/08 03:47 PM	*Chris Park	nintendowiis.com			Allowed
05/15/08 03:47 PM	*Chris Park	www.hot-wii-sites.com			Allowed
05/15/08 03:47 PM	*Chris Park	www.topgamesites.net		Games	Allowed

More

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 101 - Web Usage Statistics

The first section contains an overall bandwidth graph. This graph pertains to the current selected user or all users if “All Users in This Report” is selected. This will allow you to determine bandwidth usage by user or by report. The graph provides total bandwidth as well as downstream and upstream bandwidth. This also shows the number of hits and blocks per category.



Web Category Usage

Below is a report of the bandwidth activity for report Daily Report.

Note: You may click the web category bar for more information on the web category.

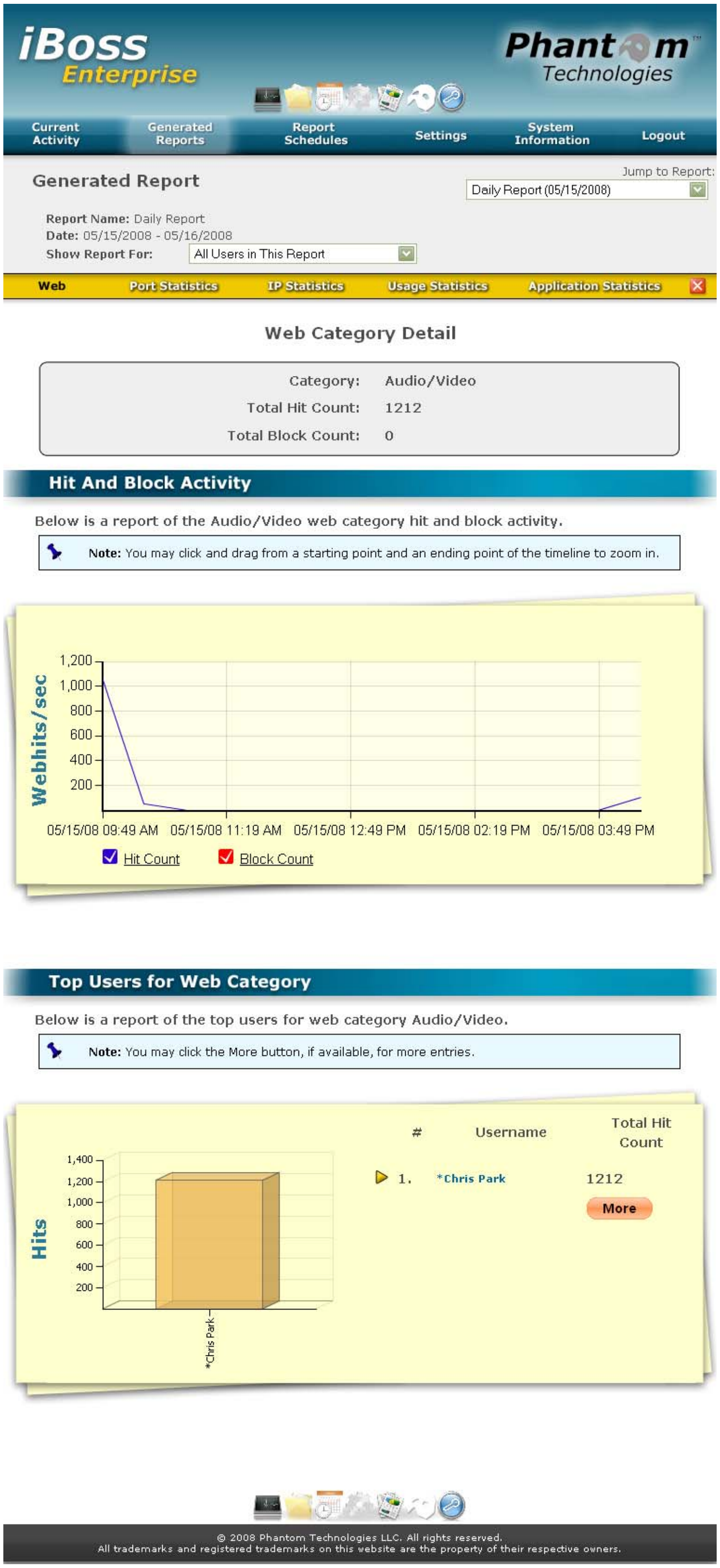
Figure 102 - Web Category Usage

5.5.2.1 Web Category Usage

The next section shows overall web category usage. It displays both total accesses and blocked accesses relative to each other. You can click on any of these bars to get more detail about the particular category usage.

5.5.2.1.1 *Web Category Detail*

If you click on the bar for a particular web category, you are taken to a detail page showing information pertaining to that particular category.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Web Category Detail

Category: Audio/Video
Total Hit Count: 1212
Total Block Count: 0

Hit And Block Activity

Below is a report of the Audio/Video web category hit and block activity.

Note: You may click and drag from a starting point and an ending point of the timeline to zoom in.

Top Users for Web Category

Below is a report of the top users for web category Audio/Video.

Note: You may click the More button, if available, for more entries.

#	Username	Total Hit Count
1.	*Chris Park	1212

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 103 - Web Category Detail

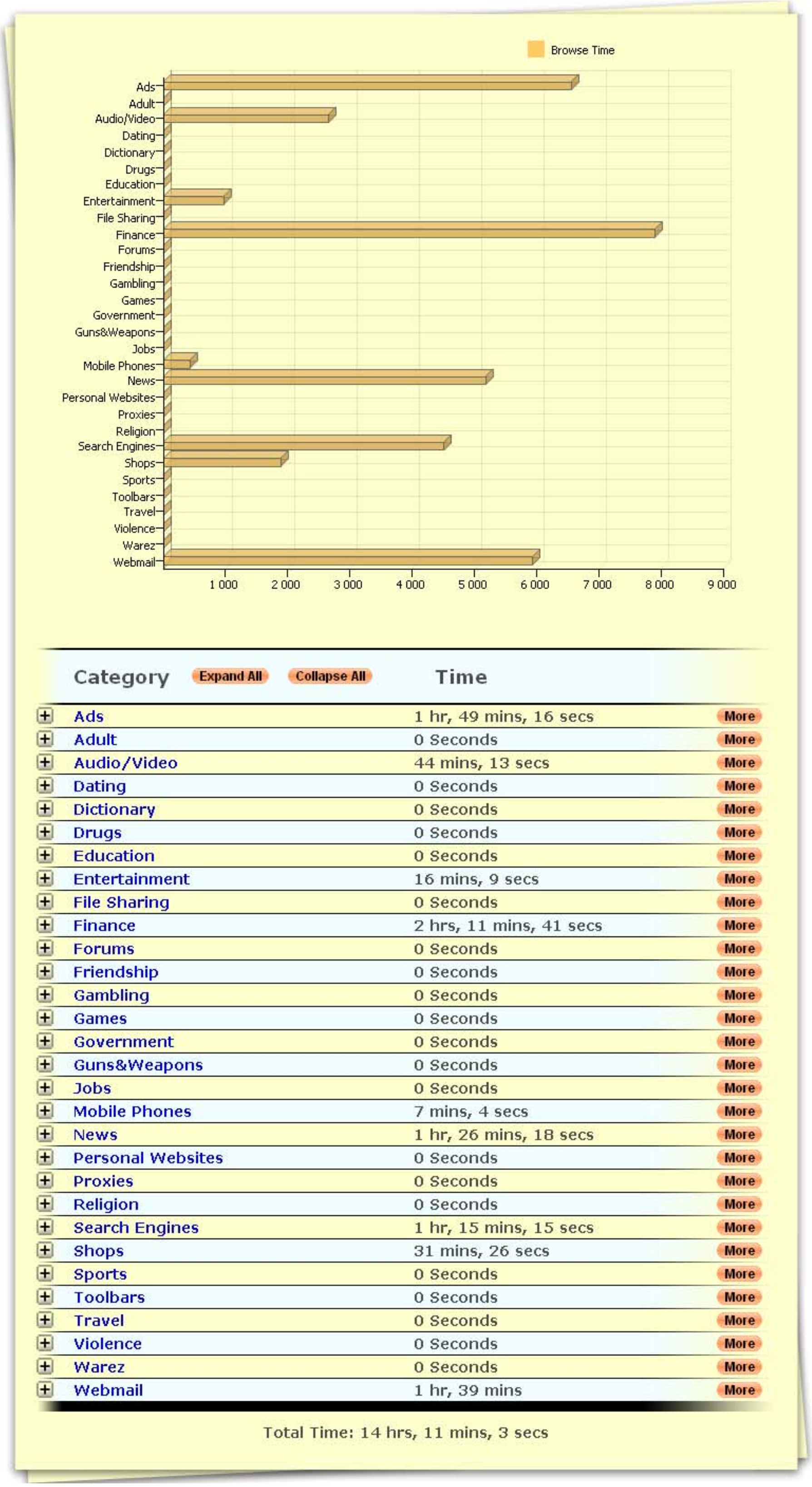
5.5.2.1.1.1 Hit and Block Category Detail Graph

The Hit and Block Activity graph show the activity for the currently selected category. This will give you an indication of use throughout the report period for the category selected. Remember, the information reflected on this page and the graph, pertain to either the currently selected user or all users if that option is selected in the report information section at the top.

5.5.2.1.1.2 Top Users for Web Category

This section lists the top users for the selected category. Users are ordered by highest hit count first. Click on the "More" button to get a full list of users for this category. The full list can be sorted by a variety of parameters.

5.5.2.2 Category Time Usage



	Category	Time	
⊞	Ads	1 hr, 49 mins, 16 secs	More
⊞	Adult	0 Seconds	More
⊞	Audio/Video	44 mins, 13 secs	More
⊞	Dating	0 Seconds	More
⊞	Dictionary	0 Seconds	More
⊞	Drugs	0 Seconds	More
⊞	Education	0 Seconds	More
⊞	Entertainment	16 mins, 9 secs	More
⊞	File Sharing	0 Seconds	More
⊞	Finance	2 hrs, 11 mins, 41 secs	More
⊞	Forums	0 Seconds	More
⊞	Friendship	0 Seconds	More
⊞	Gambling	0 Seconds	More
⊞	Games	0 Seconds	More
⊞	Government	0 Seconds	More
⊞	Guns&Weapons	0 Seconds	More
⊞	Jobs	0 Seconds	More
⊞	Mobile Phones	7 mins, 4 secs	More
⊞	News	1 hr, 26 mins, 18 secs	More
⊞	Personal Websites	0 Seconds	More
⊞	Proxies	0 Seconds	More
⊞	Religion	0 Seconds	More
⊞	Search Engines	1 hr, 15 mins, 15 secs	More
⊞	Shops	31 mins, 26 secs	More
⊞	Sports	0 Seconds	More
⊞	Toolbars	0 Seconds	More
⊞	Travel	0 Seconds	More
⊞	Violence	0 Seconds	More
⊞	Warez	0 Seconds	More
⊞	Webmail	1 hr, 39 mins	More

Total Time: 14 hrs, 11 mins, 3 secs

Figure 104 - Category Time Usage

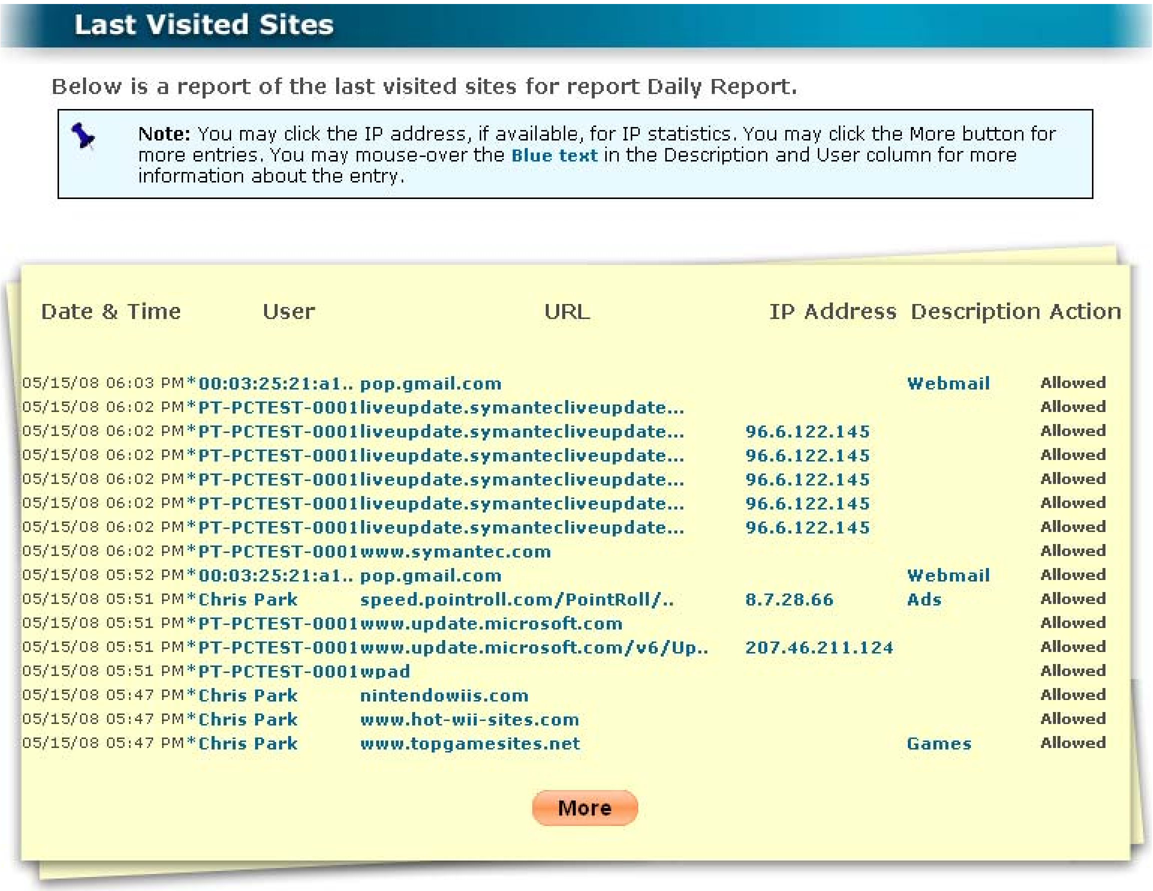
This section shows you the top categories based on time usage. This will also show you in Hours, Minutes, and seconds of the amount of time spent on each category. You may press the expand button to see the Top 5 Users for a specific category.

5.5.2.3 Top Visited and Blocked Domain

This section lists the top visited domains as well as the top blocked domains. You get a full list of domains with the ability to sort by a variety of parameters by clicking on the “More” button.

5.5.2.4 Visited Websites

This section gives a detailed list of the visited websites for the report period.



Last Visited Sites

Below is a report of the last visited sites for report Daily Report.

Note: You may click the IP address, if available, for IP statistics. You may click the More button for more entries. You may mouse-over the **Blue text** in the Description and User column for more information about the entry.

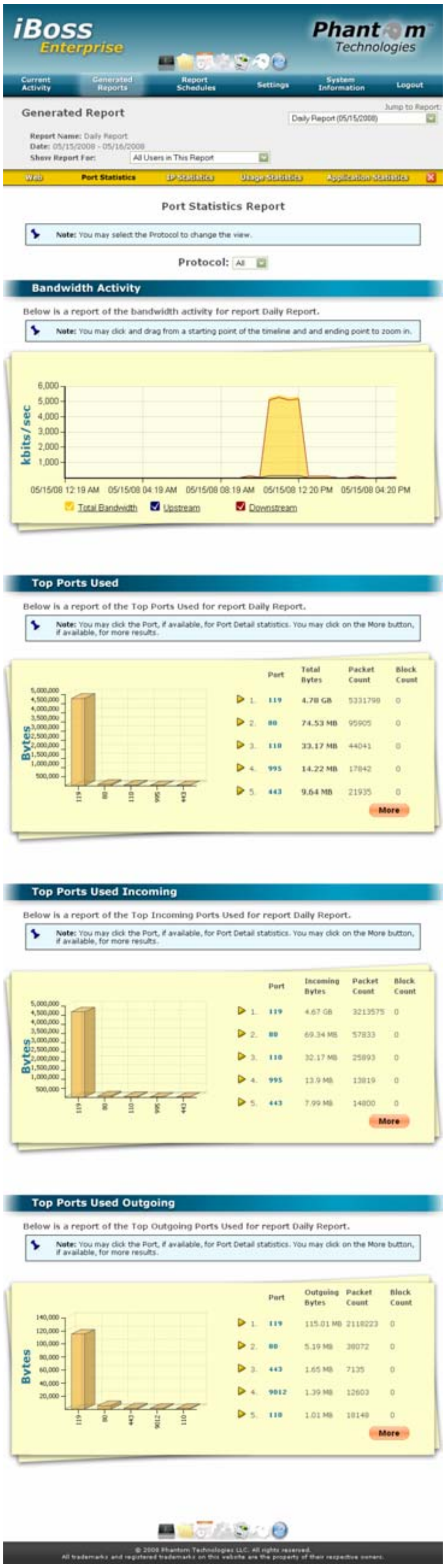
Date & Time	User	URL	IP Address	Description	Action
05/15/08 06:03 PM	*00:03:25:21:a1..	pop.gmail.com		Webmail	Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...			Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	liveupdate.symantecliveupdate...	96.6.122.145		Allowed
05/15/08 06:02 PM	*PT-PCTEST-0001	www.symantec.com			Allowed
05/15/08 05:52 PM	*00:03:25:21:a1..	pop.gmail.com		Webmail	Allowed
05/15/08 05:51 PM	*Chris Park	speed.pointroll.com/PointRoll/..	8.7.28.66	Ads	Allowed
05/15/08 05:51 PM	*PT-PCTEST-0001	www.update.microsoft.com			Allowed
05/15/08 05:51 PM	*PT-PCTEST-0001	www.update.microsoft.com/v6/Up..	207.46.211.124		Allowed
05/15/08 05:51 PM	*PT-PCTEST-0001	wpad			Allowed
05/15/08 05:47 PM	*Chris Park	nintendowiis.com			Allowed
05/15/08 05:47 PM	*Chris Park	www.hot-wii-sites.com			Allowed
05/15/08 05:47 PM	*Chris Park	www.topgamesites.net		Games	Allowed

Figure 105 - Last Visited Websites

It contains information such as the date and time the site was visited, the user that visited the site, and whether the site was allowed or blocked. Place your mouse over certain fields such as Description to get more detailed information. You can get a full list by clicking on the “More” button. This full list can be sorted by a variety of parameters.

5.5.3 Port Statistics

The port statistic section provides information regarding TCP and UDP traffic port usage. In this section you can determine how your Internet traffic is utilizing ports in order to identity potential problems and optimize the network.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Port Statistics Report

Note: You may select the Protocol to change the view.

Protocol: All

Bandwidth Activity

Below is a report of the bandwidth activity for report Daily Report.

Note: You may click and drag from a starting point of the timeline and and ending point to zoom in.

Top Ports Used

Below is a report of the Top Ports Used for report Daily Report.

Note: You may click the Port, if available, for Port Detail statistics. You may click on the More button, if available, for more results.

	Port	Total Bytes	Packet Count	Block Count
1.	119	4.78 GB	5331798	0
2.	80	74.53 MB	95905	0
3.	110	33.17 MB	44041	0
4.	995	14.22 MB	17842	0
5.	443	9.64 MB	21935	0

Top Ports Used Incoming

Below is a report of the Top Incoming Ports Used for report Daily Report.

Note: You may click the Port, if available, for Port Detail statistics. You may click on the More button, if available, for more results.

	Port	Incoming Bytes	Packet Count	Block Count
1.	119	4.67 GB	3213575	0
2.	80	69.34 MB	57833	0
3.	110	32.17 MB	25893	0
4.	995	13.9 MB	13819	0
5.	443	7.99 MB	14800	0

Top Ports Used Outgoing

Below is a report of the Top Outgoing Ports Used for report Daily Report.

Note: You may click the Port, if available, for Port Detail statistics. You may click on the More button, if available, for more results.

	Port	Outgoing Bytes	Packet Count	Block Count
1.	119	115.01 MB	2118223	0
2.	80	5.19 MB	38072	0
3.	443	1.65 MB	7135	0
4.	9012	1.39 MB	12603	0
5.	110	1.01 MB	18148	0

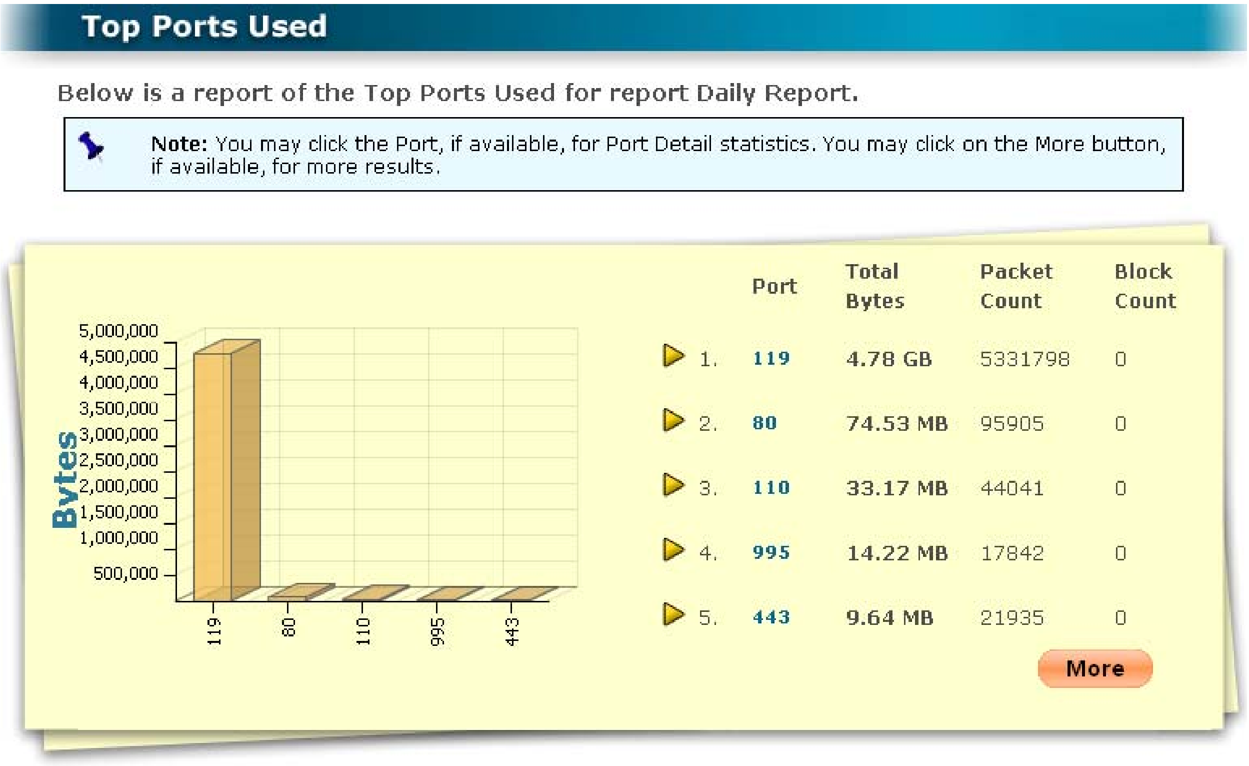
Figure 106 – Port Statistics

5.5.3.1 Bandwidth Activity

This graph shows the total bandwidth activity throughout the report period. This graph is contained in all of the top level report subsections for reference.

5.5.3.2 Top Ports Used

The following sections in this subsection contain the top ports used. The port usage is broken into three sections; Top Ports Used (which includes both upstream and downstream usage), Top Incoming Ports Used (which includes downstream port usage), and Top Outgoing Ports Used (which includes upstream port usage). You can mouse over a variety of items on this page (like the ports themselves) to get more detail on the port.



Top Ports Used

Below is a report of the Top Ports Used for report Daily Report.

Note: You may click the Port, if available, for Port Detail statistics. You may click on the More button, if available, for more results.

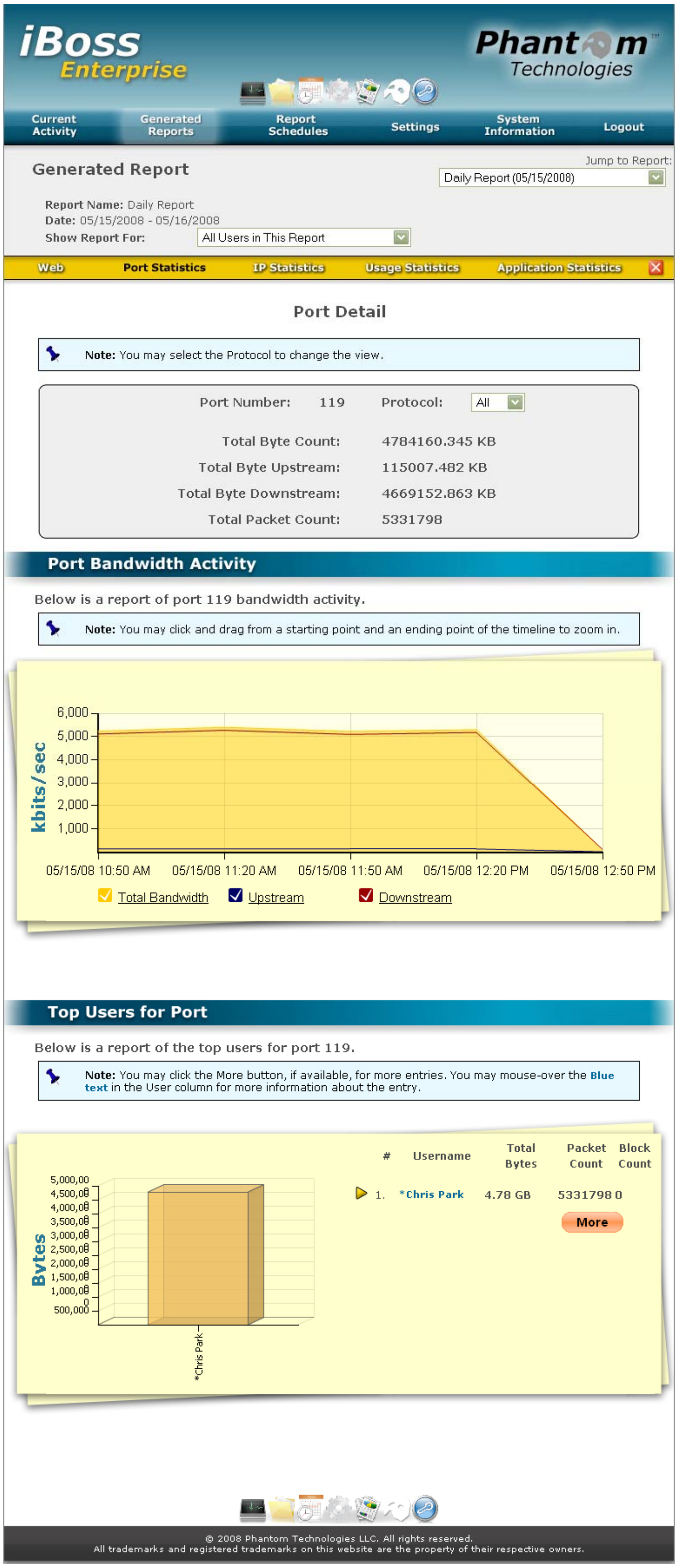
	Port	Total Bytes	Packet Count	Block Count
▷ 1.	119	4.78 GB	5331798	0
▷ 2.	80	74.53 MB	95905	0
▷ 3.	110	33.17 MB	44041	0
▷ 4.	995	14.22 MB	17842	0
▷ 5.	443	9.64 MB	21935	0

Figure 107 - Top Used Ports

If you click on the "More" button in any of these sections, you will get a full list of ports which can be sorted by a variety of criteria.

5.5.3.2.1 *Port Detail*

By clicking on any of the listed ports on this page, you will be taken to a full detail page for that port.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Port Detail

Note: You may select the Protocol to change the view.

Port Number: 119   Protocol: All

Total Byte Count:	4784160.345 KB
Total Byte Upstream:	115007.482 KB
Total Byte Downstream:	4669152.863 KB
Total Packet Count:	5331798

Port Bandwidth Activity

Below is a report of port 119 bandwidth activity.

Note: You may click and drag from a starting point and an ending point of the timeline to zoom in.

Top Users for Port

Below is a report of the top users for port 119.

Note: You may click the More button, if available, for more entries. You may mouse-over the **Blue text** in the User column for more information about the entry.

#	Username	Total Bytes	Packet Count	Block Count
1.	*Chris Park	4.78 GB	5331798	0

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 108 - Port Detail

The port detail page contains information pertaining to a specific port.

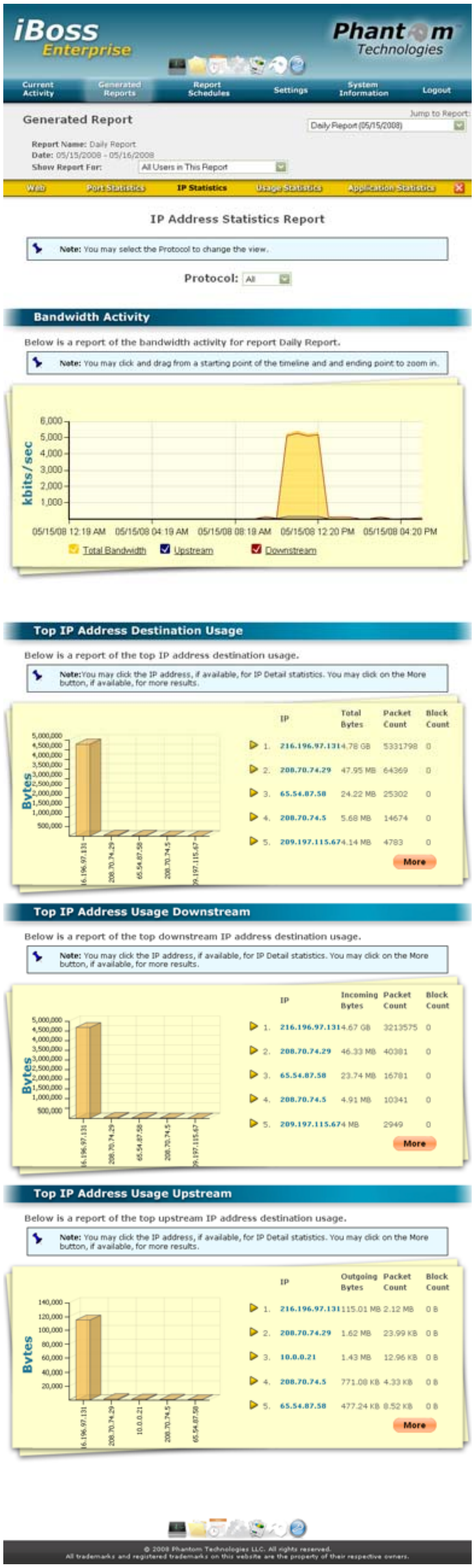
The page also allows you to view specific details about the port such as total bandwidth through the port, TCP traffic, or UDP traffic. To change to a particular protocol, select the protocol TCP, UDP, or All from the drop down list labeled “Protocol” near the top. All information on the page will adjust to reflect only the selected protocol.

This page also contains the bandwidth activity throughout the report period for this particular port. You can use this to determine when and how the particular port is being utilized.

Toward the bottom, a list of users for the port is listed sorted from highest use to lowest. This allows you to determine which user is utilizing the port the most. You can get a full list of these users by clicking on the “More” button.

5.5.4 IP Statistics

The IP Address statistic section provides information regarding IP Address destination usage from your network. In this section you can determine how your Internet traffic is utilizing different IP Address destinations in order to identity potential problems and optimize the network.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

IP Address Statistics Report

Note: You may select the Protocol to change the view.

Protocol: All

Bandwidth Activity

Below is a report of the bandwidth activity for report Daily Report.

Note: You may click and drag from a starting point of the timeline and and ending point to zoom in.

☑ Total Bandwidth ☑ Upstream ☑ Downstream

Top IP Address Destination Usage

Below is a report of the top IP address destination usage.

Note: You may click the IP address, if available, for IP Detail statistics. You may click on the More button, if available, for more results.

	IP	Total Bytes	Packet Count	Block Count
1.	216.196.97.131	4.78 GB	5331798	0
2.	208.70.74.29	47.95 MB	64369	0
3.	65.54.87.58	24.22 MB	25302	0
4.	208.70.74.5	5.68 MB	14674	0
5.	209.197.115.67	4.14 MB	4783	0

Top IP Address Usage Downstream

Below is a report of the top downstream IP address destination usage.

Note: You may click the IP address, if available, for IP Detail statistics. You may click on the More button, if available, for more results.

	IP	Incoming Bytes	Packet Count	Block Count
1.	216.196.97.131	4.67 GB	3213575	0
2.	208.70.74.29	46.33 MB	40381	0
3.	65.54.87.58	23.74 MB	16781	0
4.	208.70.74.5	4.91 MB	10341	0
5.	209.197.115.67	4 MB	2949	0

Top IP Address Usage Upstream

Below is a report of the top upstream IP address destination usage.

Note: You may click the IP address, if available, for IP Detail statistics. You may click on the More button, if available, for more results.

	IP	Outgoing Bytes	Packet Count	Block Count
1.	216.196.97.131	115.01 MB	2.12 MB	0 B
2.	208.70.74.29	1.62 MB	23.99 KB	0 B
3.	10.0.0.21	1.43 MB	12.96 KB	0 B
4.	208.70.74.5	771.08 KB	4.33 KB	0 B
5.	65.54.87.58	477.24 KB	8.52 KB	0 B

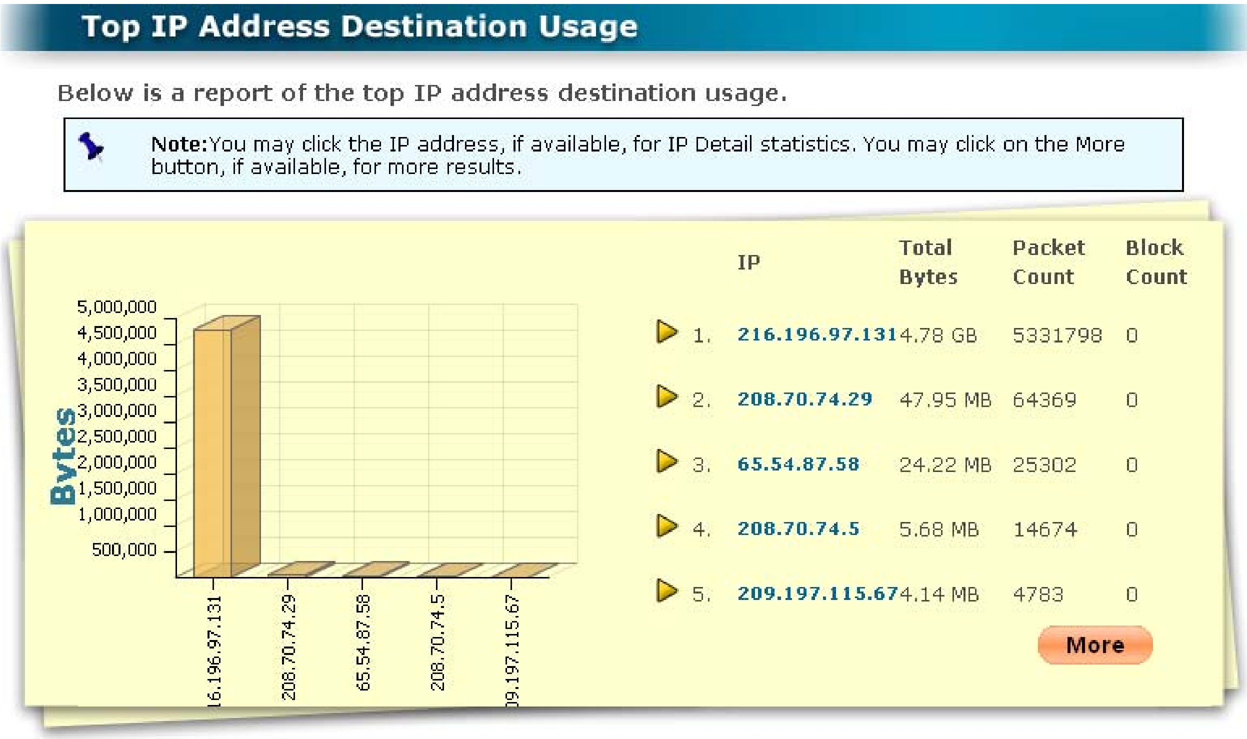
Figure 109 - IP Address Statistics

5.5.4.1 Bandwidth Activity

This graph shows the total bandwidth activity throughout the report period. This graph is contained in all of the top level report subsections for reference.

5.5.4.2 Top IP Address Utilization

The following sections in this subsection contain the top IP Address destinations used. The usage is broken into three sections; Top IP Address Destinations (which includes both upstream and downstream usage), Top IP Address usage downstream (which includes downstream usage), and Top IP Address usage upstream (which includes upstream usage). You can mouse over a variety of items on this page (like the IP Addresses themselves) to get more details.



Top IP Address Destination Usage

Below is a report of the top IP address destination usage.

Note: You may click the IP address, if available, for IP Detail statistics. You may click on the More button, if available, for more results.

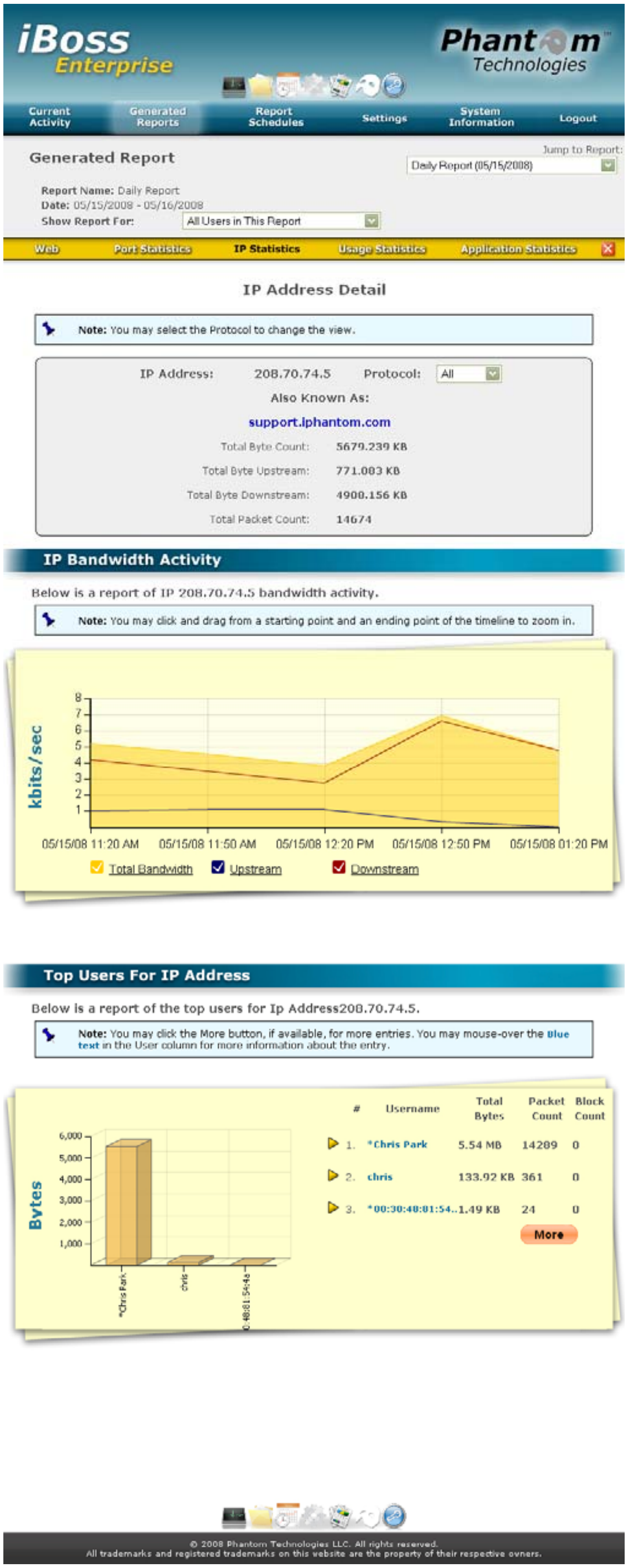
	IP	Total Bytes	Packet Count	Block Count
1.	216.196.97.131	4.78 GB	5331798	0
2.	208.70.74.29	47.95 MB	64369	0
3.	65.54.87.58	24.22 MB	25302	0
4.	208.70.74.5	5.68 MB	14674	0
5.	209.197.115.67	4.14 MB	4783	0

Figure 110 - Top IP Address Utilization

If you click on the “More” button in any of these sections, you will get a full list of IP Addresses which can be sorted by a variety of criteria.

5.5.4.2.1 *IP Address Detail*

By clicking on any of the listed IP Addresses on this page, you will be taken to a full detail page for that IP Address.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

IP Address Detail

Note: You may select the Protocol to change the view.

IP Address: 208.70.74.5 Protocol: All

Also Known As:

support.iphantom.com

Total Byte Count:	5679.239 KB
Total Byte Upstream:	771.083 KB
Total Byte Downstream:	4900.156 KB
Total Packet Count:	14674

IP Bandwidth Activity

Below is a report of IP 208.70.74.5 bandwidth activity.

Note: You may click and drag from a starting point and an ending point of the timeline to zoom in.

Top Users For IP Address

Below is a report of the top users for Ip Address208.70.74.5.

Note: You may click the More button, if available, for more entries. You may mouse-over the **Blue text** in the User column for more information about the entry.

#	Username	Total Bytes	Packet Count	Block Count
1.	*Chris Park	5.54 MB	14289	0
2.	chris	133.92 KB	361	0
3.	*00:30:48:81:54..	1.49 KB	24	0

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 111 - Top IP Address Detail

The IP Address detail page contains information pertaining to a specific IP Address.

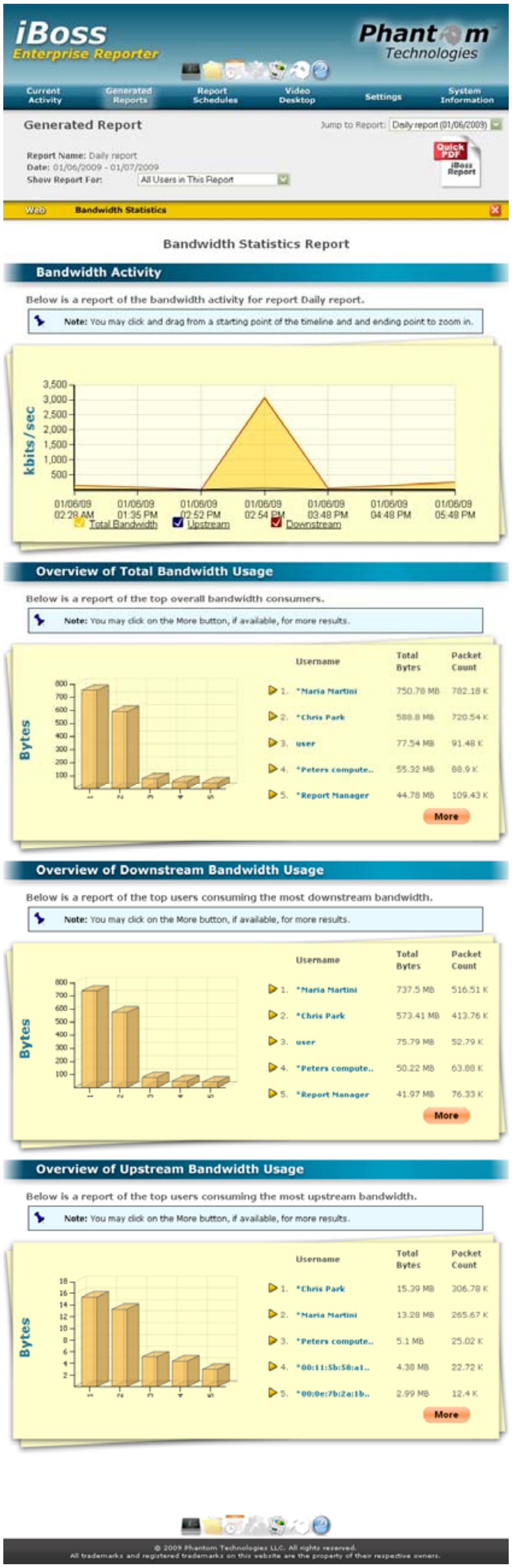
The page also allows you to view specific details about the IP Address such as total bandwidth to/from the destination, only TCP traffic to/from the destination, or only UDP traffic to/from the destination. To change to a particular protocol, select the protocol TCP, UDP, or All from the drop down list labeled “Protocol” near the top. All information on the page will adjust to reflect only the selected protocol.

This page also contains a graph with the bandwidth activity throughout the report period for this particular IP Address. You can use this to determine when and how the particular IP Address is being utilized.

Toward the bottom, a list of top users utilizing the IP Address is listed. The list is sorted from highest use to lowest. This allows you to determine which user is utilizing the IP Address the most. You can get a full list of these users by clicking on the “More” button.

5.5.5 Bandwidth Statistics

The Bandwidth statistic section provides information regarding general bandwidth usages from your network. General bandwidth includes overall, downstream and upstream usage.



Generated Report

Jump to Report: Daily report (01/06/2009)

Report Name: Daily report
Date: 01/06/2009 - 01/07/2009
Show Report For: All Users in This Report

Bandwidth Statistics Report

Bandwidth Activity

Below is a report of the bandwidth activity for report Daily report.

Note: You may click and drag from a starting point of the timeline and and ending point to zoom in.

Overview of Total Bandwidth Usage

Below is a report of the top overall bandwidth consumers.

Note: You may click on the More button, if available, for more results.

	Username	Total Bytes	Packet Count
1.	*Maria Martini	750.78 MB	782.18 K
2.	*Chris Park	588.8 MB	720.54 K
3.	user	77.54 MB	91.48 K
4.	*Peters compute..	55.32 MB	88.9 K
5.	*Report Manager	44.78 MB	109.43 K

Overview of Downstream Bandwidth Usage

Below is a report of the top users consuming the most downstream bandwidth.

Note: You may click on the More button, if available, for more results.

	Username	Total Bytes	Packet Count
1.	*Maria Martini	737.5 MB	516.51 K
2.	*Chris Park	573.41 MB	413.76 K
3.	user	75.79 MB	52.79 K
4.	*Peters compute..	50.22 MB	63.88 K
5.	*Report Manager	41.97 MB	76.33 K

Overview of Upstream Bandwidth Usage

Below is a report of the top users consuming the most upstream bandwidth.

Note: You may click on the More button, if available, for more results.

	Username	Total Bytes	Packet Count
1.	*Chris Park	15.39 MB	306.78 K
2.	*Maria Martini	13.28 MB	265.67 K
3.	*Peters compute..	5.1 MB	25.02 K
4.	*00:11:5b:58:a1..	4.38 MB	22.72 K
5.	*00:0e:7b:2a:1b..	2.99 MB	12.4 K

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

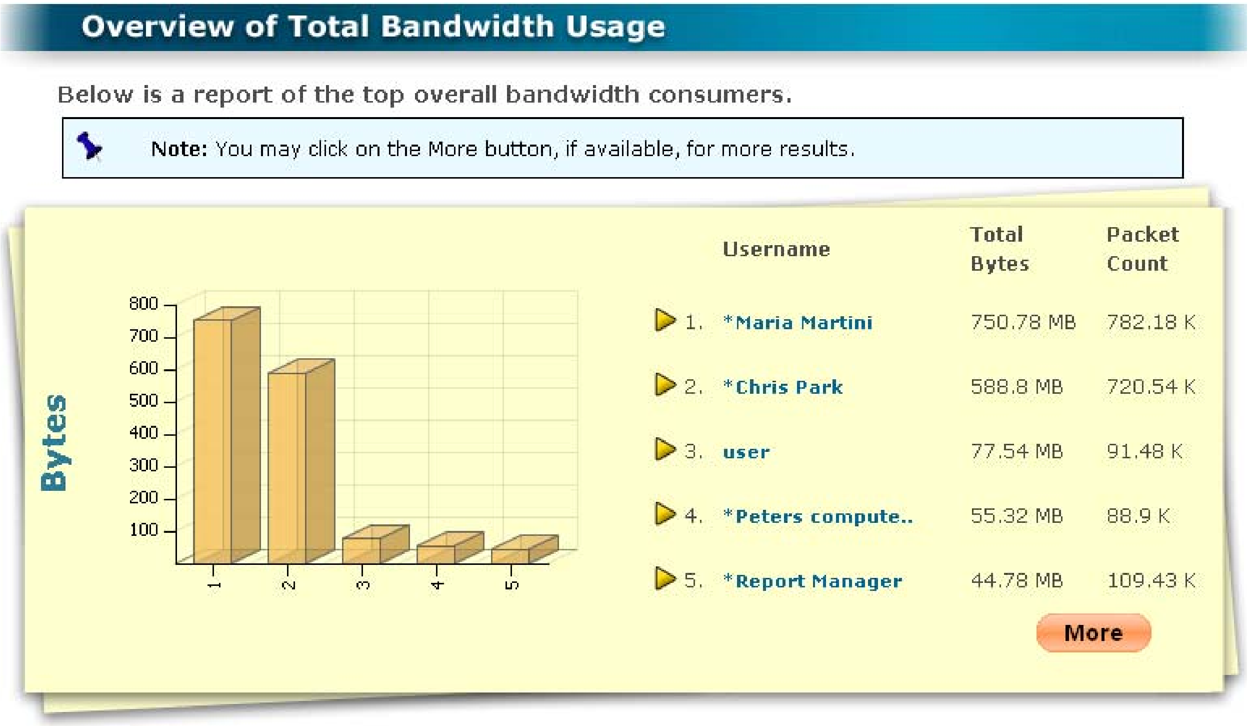
Figure 112 - Bandwidth Statistics

5.5.5.1 Bandwidth Activity

This graph shows the total bandwidth activity throughout the report period. This graph is contained in all of the top level report subsections for reference.

5.5.5.2 Overview of Total Bandwidth Usage

The following sections in this subsection contain the overview of total bandwidth usage. The bandwidth usage is broken into three sections; Overview of Overall usage, Overview of downstream usage, and overview of upstream usage. You can mouse over a variety of items on this page (like users themselves) to get more details.



Overview of Total Bandwidth Usage

Below is a report of the top overall bandwidth consumers.

Note: You may click on the More button, if available, for more results.

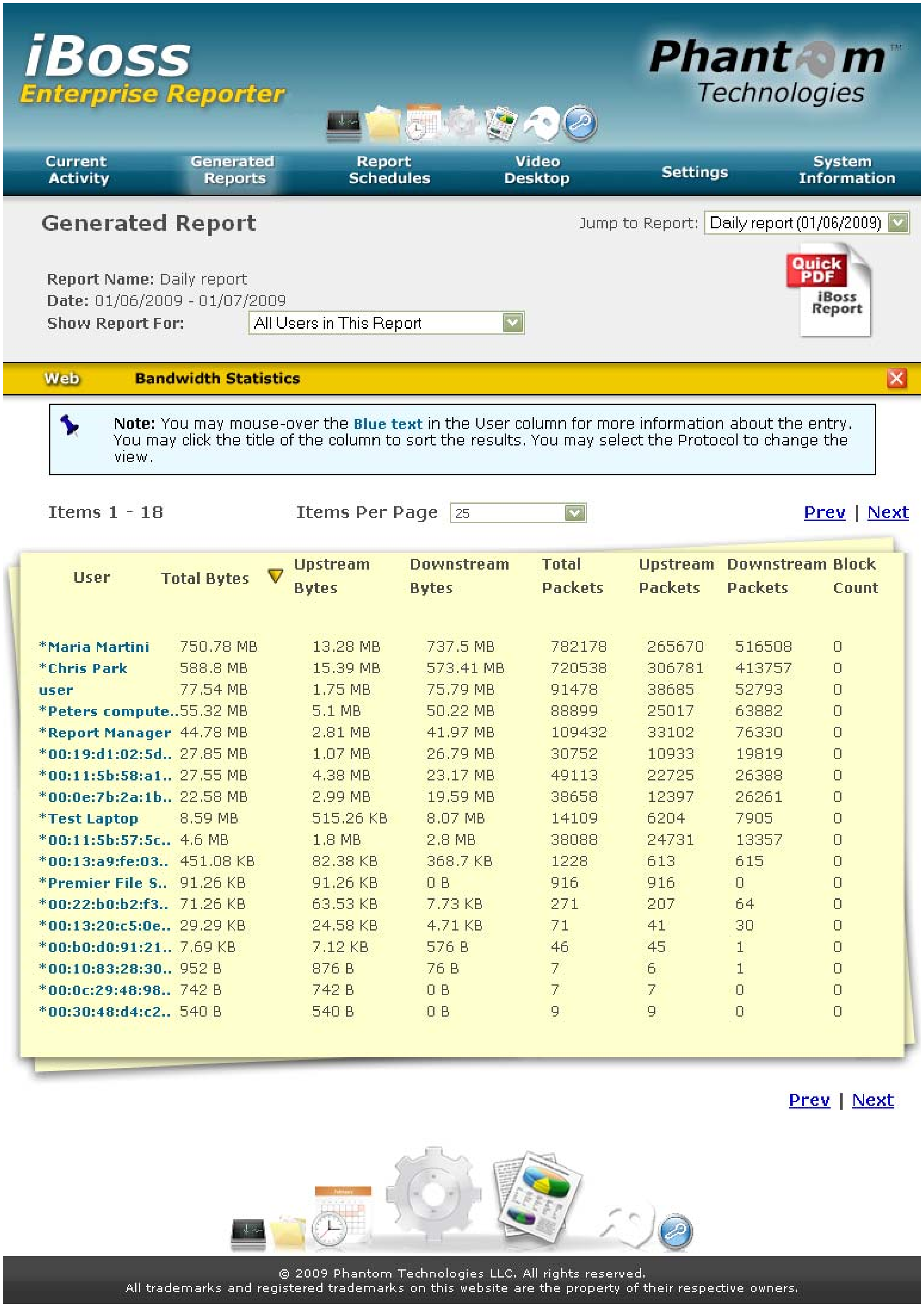
	Username	Total Bytes	Packet Count
1.	*Maria Martini	750.78 MB	782.18 K
2.	*Chris Park	588.8 MB	720.54 K
3.	user	77.54 MB	91.48 K
4.	*Peters compute..	55.32 MB	88.9 K
5.	*Report Manager	44.78 MB	109.43 K

Figure 113 – Overview of Total Bandwidth Usage

If you click on the “More” button in any of these sections, you will get a full list of the users that can be sorted by a variety of criteria.

5.5.5.2.1 *Bandwidth Usage Detail*

By clicking on any of the more buttons on this page, you will be taken to a full detail page for bandwidth usage.



Generated Report

Jump to Report: Daily report (01/06/2009)

Report Name: Daily report
Date: 01/06/2009 - 01/07/2009
Show Report For: All Users in This Report

Bandwidth Statistics

Note: You may mouse-over the **Blue text** in the User column for more information about the entry. You may click the title of the column to sort the results. You may select the Protocol to change the view.

Items 1 - 18 Items Per Page 25

User	Total Bytes	Upstream Bytes	Downstream Bytes	Total Packets	Upstream Packets	Downstream Packets	Block Count
*Maria Martini	750.78 MB	13.28 MB	737.5 MB	782178	265670	516508	0
*Chris Park	588.8 MB	15.39 MB	573.41 MB	720538	306781	413757	0
user	77.54 MB	1.75 MB	75.79 MB	91478	38685	52793	0
*Peters compute..	55.32 MB	5.1 MB	50.22 MB	88899	25017	63882	0
*Report Manager	44.78 MB	2.81 MB	41.97 MB	109432	33102	76330	0
*00:19:d1:02:5d..	27.85 MB	1.07 MB	26.79 MB	30752	10933	19819	0
*00:11:5b:58:a1..	27.55 MB	4.38 MB	23.17 MB	49113	22725	26388	0
*00:0e:7b:2a:1b..	22.58 MB	2.99 MB	19.59 MB	38658	12397	26261	0
*Test Laptop	8.59 MB	515.26 KB	8.07 MB	14109	6204	7905	0
*00:11:5b:57:5c..	4.6 MB	1.8 MB	2.8 MB	38088	24731	13357	0
*00:13:a9:fe:03..	451.08 KB	82.38 KB	368.7 KB	1228	613	615	0
*Premier File S..	91.26 KB	91.26 KB	0 B	916	916	0	0
*00:22:b0:b2:f3..	71.26 KB	63.53 KB	7.73 KB	271	207	64	0
*00:13:20:c5:0e..	29.29 KB	24.58 KB	4.71 KB	71	41	30	0
*00:b0:d0:91:21..	7.69 KB	7.12 KB	576 B	46	45	1	0
*00:10:83:28:30..	952 B	876 B	76 B	7	6	1	0
*00:0c:29:48:98..	742 B	742 B	0 B	7	7	0	0
*00:30:48:d4:c2..	540 B	540 B	0 B	9	9	0	0

© 2009 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

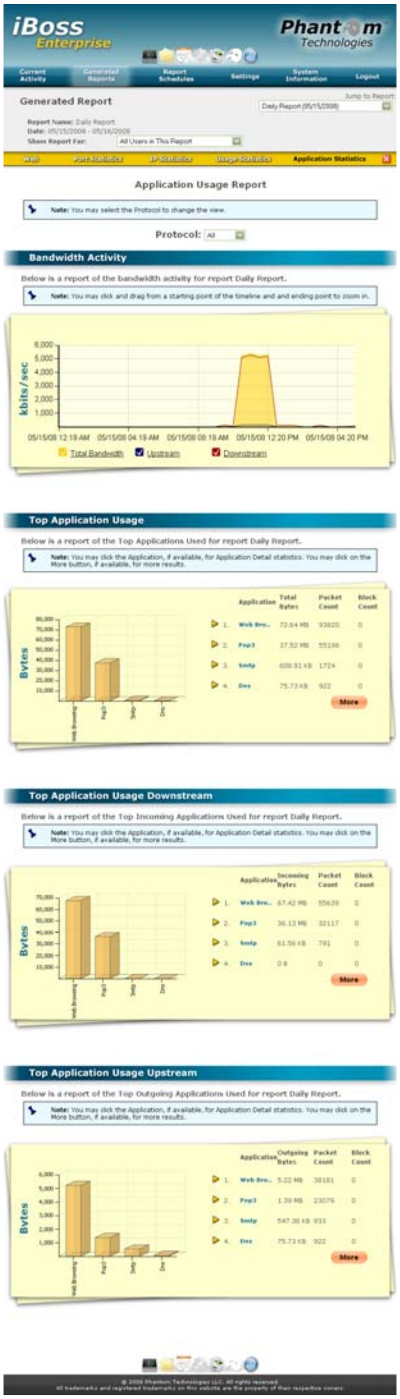
Figure 114 – Bandwidth Usage Detail

The bandwidth usage detail page contains information on all users and bandwidth information.

The page also allows you to sort by Total Bytes, Upstream Bytes, Downstream Bytes, Total Packets, Upstream Packets, Downstream Packets, and Block count.

5.5.6 Application Statistics

The application statistic section provides information regarding specific application usage on your network. In this section you can determine how your different network applications are utilizing the traffic on the network in order to identity potential problems and optimize the network.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Application Usage Report

Note: You may select the Protocol to change the view.

Protocol: All

Bandwidth Activity

Below is a report of the bandwidth activity for report Daily Report.

Note: You may click and drag from a starting point of the timeline and and ending point to zoom in.

Top Application Usage

Below is a report of the Top Applications Used for report Daily Report.

Note: You may click the Application, if available, for Application Detail statistics. You may click on the More button, if available, for more results.

	Application	Total Bytes	Packet Count	Block Count
1.	Web Bro..	72.64 MB	93820	0
2.	Pop3	37.52 MB	55196	0
3.	Smtp	608.91 KB	1724	0
4.	Dns	75.73 KB	922	0

Top Application Usage Downstream

Below is a report of the Top Incoming Applications Used for report Daily Report.

Note: You may click the Application, if available, for Application Detail statistics. You may click on the More button, if available, for more results.

	Application	Incoming Bytes	Packet Count	Block Count
1.	Web Bro..	67.42 MB	55639	0
2.	Pop3	36.13 MB	32117	0
3.	Smtp	61.56 KB	791	0
4.	Dns	0 B	0	0

Top Application Usage Upstream

Below is a report of the Top Outgoing Applications Used for report Daily Report.

Note: You may click the Application, if available, for Application Detail statistics. You may click on the More button, if available, for more results.

	Application	Outgoing Bytes	Packet Count	Block Count
1.	Web Bro..	5.22 MB	38181	0
2.	Pop3	1.39 MB	23079	0
3.	Smtp	547.36 KB	933	0
4.	Dns	75.73 KB	922	0

© 2008 Phantom Technologies LLC. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

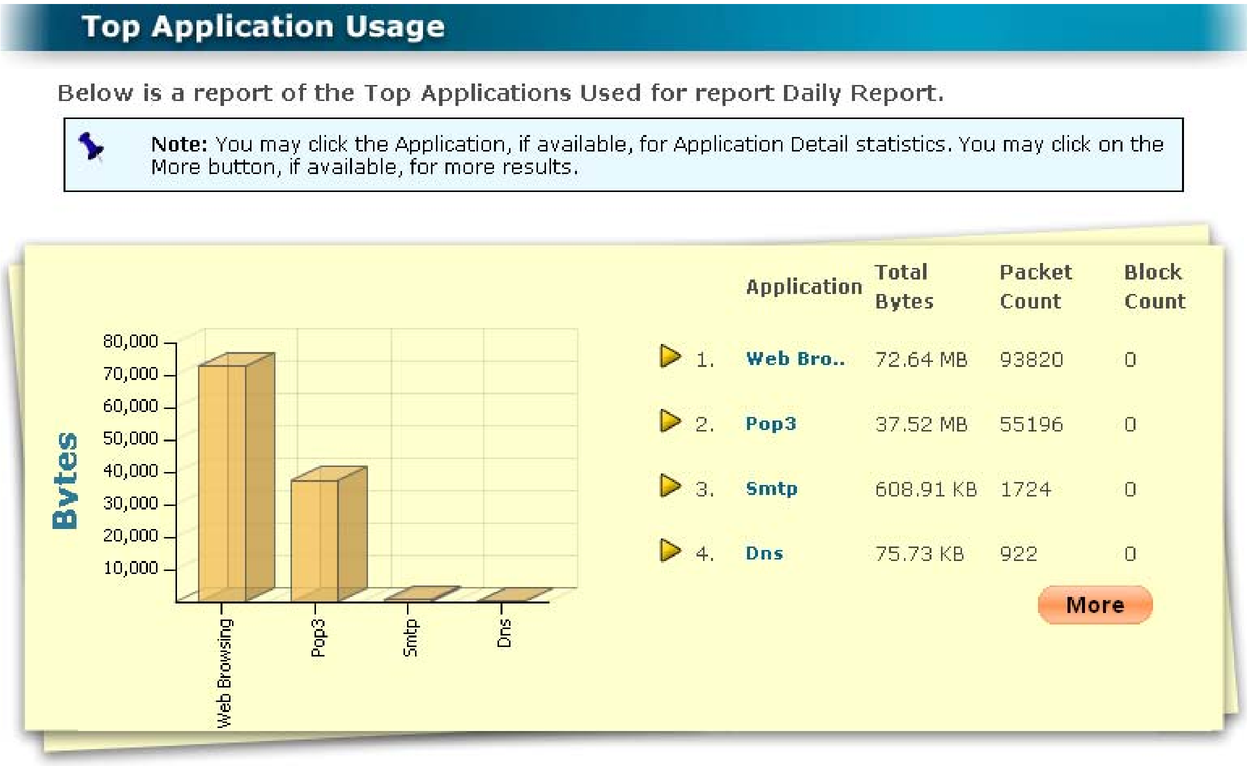
Figure 115 - Application Statistics

5.5.6.1 Bandwidth Activity

This graph shows the total bandwidth activity throughout the report period. This graph is contained in all of the top level report subsections for reference.

5.5.6.2 Top Applications

The following sections in this subsection contain the top network applications used. The usage is broken into three sections; Top overall usage, top downstream usage, and top upstream usage. You can mouse over a variety of items on this page (like the applications themselves) to get more details.



Top Application Usage

Below is a report of the Top Applications Used for report Daily Report.

Note: You may click the Application, if available, for Application Detail statistics. You may click on the More button, if available, for more results.

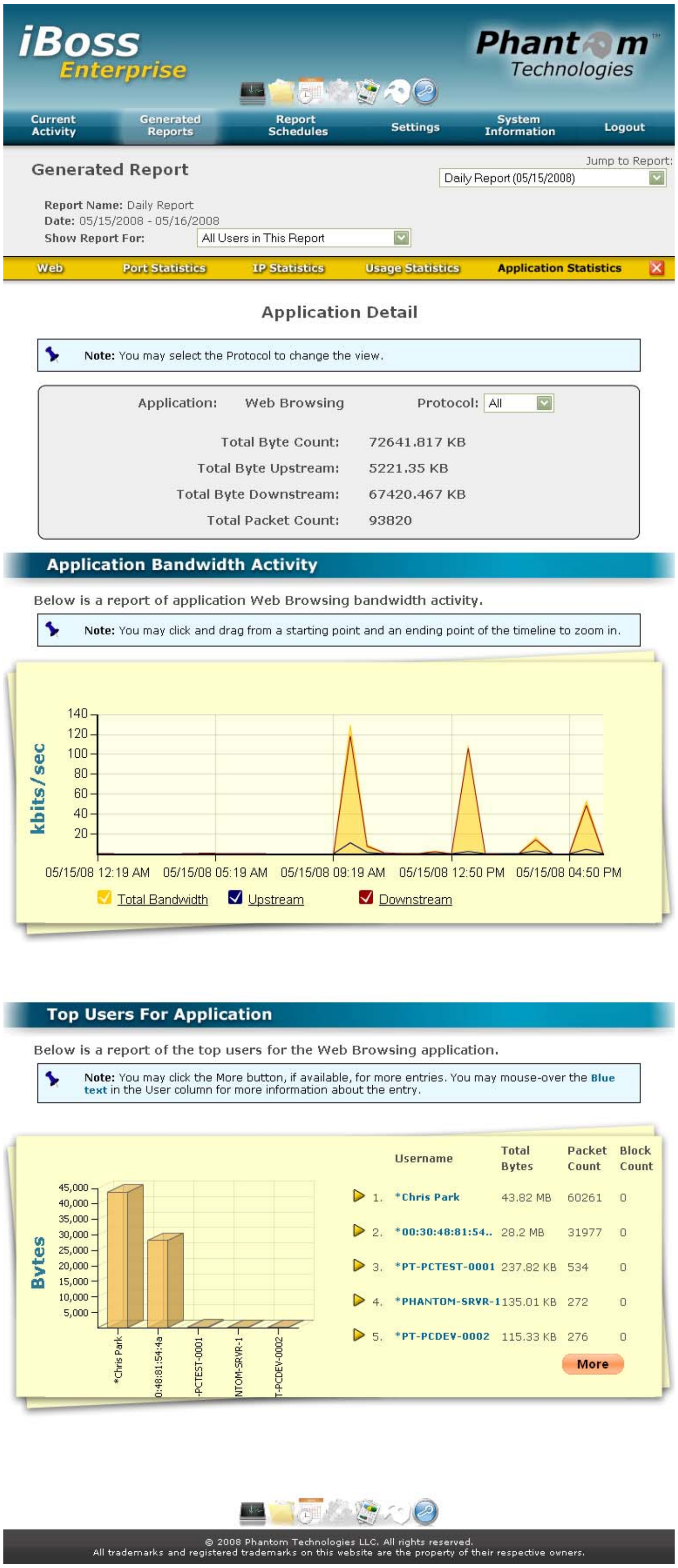
	Application	Total Bytes	Packet Count	Block Count
1.	Web Bro..	72.64 MB	93820	0
2.	Pop3	37.52 MB	55196	0
3.	Smtp	608.91 KB	1724	0
4.	Dns	75.73 KB	922	0

Figure 116 - Top Applications Usage

If you click on the “More” button in any of these sections, you will get a full list of the applications that can be sorted by a variety of criteria.

5.5.6.2.1 *Application Detail*

By clicking on any of the listed applications on this page, you will be taken to a full detail page for that application.



Generated Report

Jump to Report: Daily Report (05/15/2008)

Report Name: Daily Report
Date: 05/15/2008 - 05/16/2008
Show Report For: All Users in This Report

Application Detail

Note: You may select the Protocol to change the view.

Application: Web Browsing

Protocol: All

Total Byte Count:	72641.817 KB
Total Byte Upstream:	5221.35 KB
Total Byte Downstream:	67420.467 KB
Total Packet Count:	93820

Application Bandwidth Activity

Below is a report of application Web Browsing bandwidth activity.

Note: You may click and drag from a starting point and an ending point of the timeline to zoom in.

Top Users For Application

Below is a report of the top users for the Web Browsing application.

Note: You may click the More button, if available, for more entries. You may mouse-over the **Blue text** in the User column for more information about the entry.

	Username	Total Bytes	Packet Count	Block Count
▶ 1.	*Chris Park	43.82 MB	60261	0
▶ 2.	*00:30:48:81:54..	28.2 MB	31977	0
▶ 3.	*PT-PCTEST-0001	237.82 KB	534	0
▶ 4.	*PHANTOM-SRVR-1	135.01 KB	272	0
▶ 5.	*PT-PCDEV-0002	115.33 KB	276	0

Figure 117 - Application Detail

The application detail page contains information pertaining to a specific application.

The page also allows you to view specific details about the application such as total bandwidth used for this application, only TCP traffic for this application, or only UDP traffic for this application. To change to a particular protocol, select the protocol TCP, UDP, or All from the drop down list labeled “Protocol” near the top. All information on the page will adjust to reflect only the selected protocol.

This page also contains a graph with the bandwidth activity throughout the report period for this particular application. You can use this to determine when and how the particular application is being utilized.

Toward the bottom, a list of top users utilizing the application is listed. The list is sorted from highest use to lowest. This allows you to determine which user is utilizing the application the most. You can get a full list of these users by clicking on the “More” button.

6 REMOTE MANAGEMENT

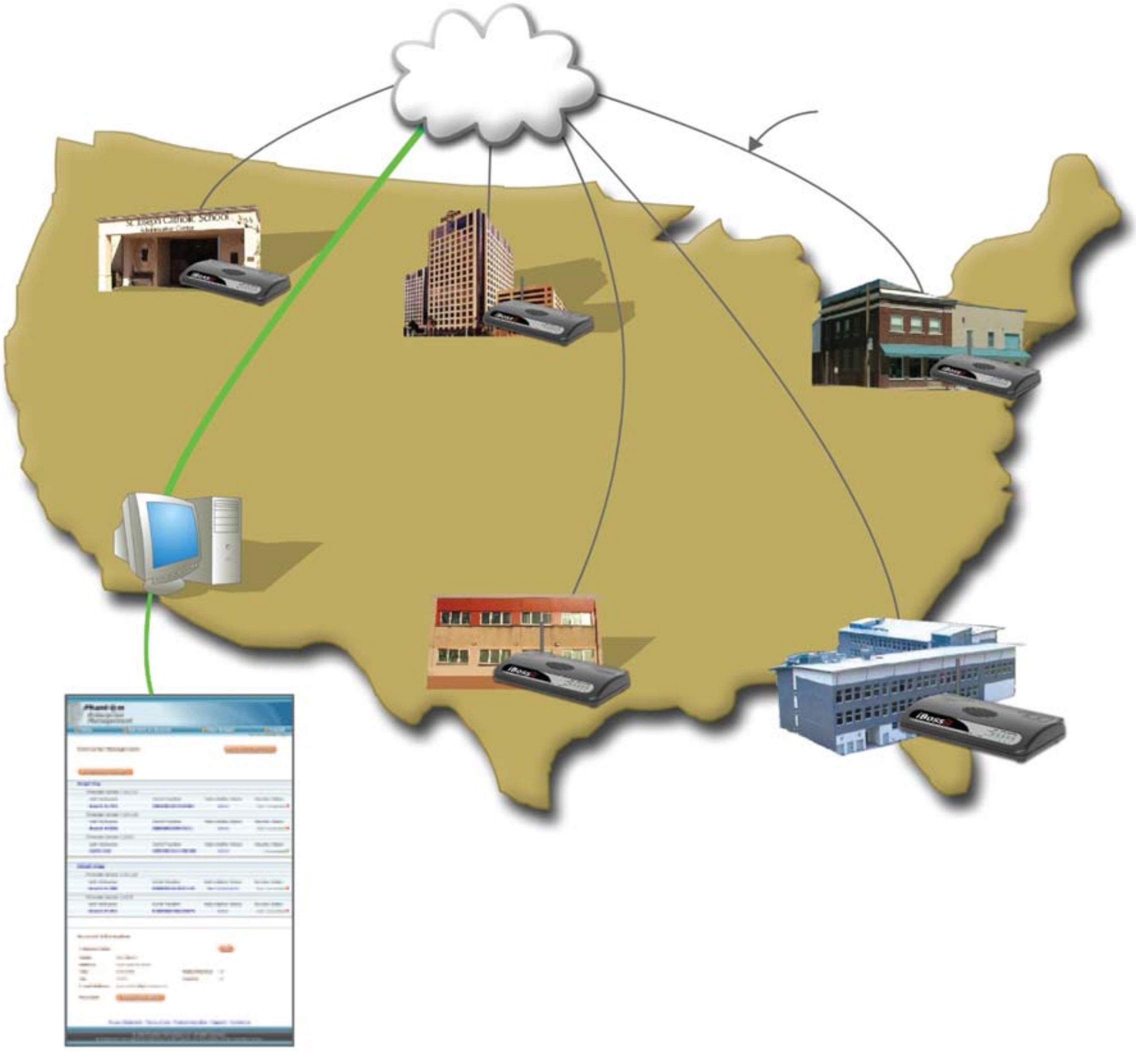


Figure 118 - Remote Management

The Remote Management portal will allow you to remotely manage all of your iBoss units from anywhere in the world. You may send the daily email report remotely, configure settings, upgrade firmware, upload or download settings, and set groups for units. Easily connect and configure settings without needing to know your IP address. Connect to all your devices securely using SSL and AES encryption without needing to set up a VPN. No static IP address required! The Remote Management can securely connect to your iBoss units even through firewalls!

The Remote Management portal will allow you to manage multiple locations that have the iBoss installed through one managed account. You or the iBoss units may be set up anywhere in the world with and Internet connection.

6.1 Set Up Account

You may create a Remote Management account through https://www.iphantom.com/enterprisemanagement/main.html. This will allow you to manage all of your iBoss units remotely. This one account can manage multiple iBoss units. You can access your Remote Management account from anywhere in the world.

6.2 Adding Units to Your Account

You may add multiple iBoss units to your account for which you would like to manage. You may also give the added unit a nickname to remember where the unit is located.

6.3 Groups

You may create and edit groups to help manage your units. Using groups allows you to organize your units and manage settings together for units of the group. You may upload or sync settings for all units within a group making it easier and quicker to configure multiple units.

6.4 Management

Easily connect and configure settings without needing to know your IP address of where your iBoss units are connected. The management portal automatically connects to your device using SSL and AES encryption without needing to set up a VPN. A static IP address is not required for the management portal to connect to your devices. It will even be able to connect to the devices through a secure firewall without having to hassle with any further configuration of the firewall.

6.5 Settings

Settings for your iBoss units may be managed individually or grouped together. You may download a unit's settings or upload them to multiple units.

6.6 Logs

You may set a report to be generated and emailed to you remotely. This allows you to send the daily report log to any email address you wish.

6.7 Firmware

Firmware updates can become available from time to time. These firmware updates have new features and updates. You may remotely update your iBoss unit with the latest firmware version without having direct access to it using the management portal.

7 SUBSCRIPTION MANAGEMENT

The iBoss requires an active subscription to function. The unit may already be pre-activated when you receive it, or you may need to obtain and/or activate a subscription key and register the active subscription key with your iBoss.

To view and manage your subscription information, login to the iBoss interface home page and click the “**Manage Subscription**” button.

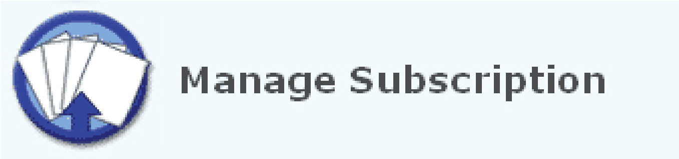


Figure 119 - Manage Subscription

This page will allow you to view your current subscription status. The following are values that may appear in the “**Status**” field:

Active – The iBoss has an active subscription.
Must Activate – An active subscription key has not been registered with the iBoss.
Not Available – The iBoss is not connected to the Internet.
Expired – The iBoss subscription has expired and is no longer active.
Cancelled – The iBoss subscription has been cancelled and is no longer active.

7.1 Adding a Subscription Key

The iBoss needs an active Subscription Key entered into the device before it can start functioning.

1. Confirm that your Subscription Key has been activated.
2. Enter the active Subscription Key for the iBoss.
· Log into your iBoss and click on "**Manage Subscription**" button on the main page. (Please refer to the User Interface section on how to log into the iBoss)
· Enter in the active Subscription Key in the boxes provided.

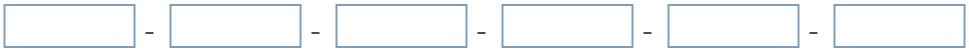


Figure 120 - Enter Subscription Key

· Click on "**Apply**" and "**Confirm**" on the next page.
3. If you do not have a Subscription Key, you may press the “**Purchase Subscription Key Now**” button to purchase one. This will guide you through the process of activating and registering your Subscription Key with your iBoss.

8 TROUBLESHOOTING

8.1 Password Recovery

In the event that the iBoss administration password becomes lost, there is a way by which it can be recovered. If you checked the "**Password Recovery**" option on the iBoss when the password was initially setup, you will be prompted to have the password E-mailed to you upon a failed login attempt. Follow the link provided on the login page to have your password E-mailed to the address specified during the "**Password Recovery**" setup.
If you did not enable the password recovery option, you can contact the Phantom Technologies support department to have the password E-mailed to a specific address. Note that you will be prompted for account authentication information before a password recovery request is fulfilled.

The password may be reset by performing a factory reset on the iBoss, however this action is typically reserved as a last resort due to the fact that ALL of your settings will be erased back to factory defaults.

8.2 Resetting to Factory Defaults

The iBoss can be reset back to factory default settings through two different methods. After performing the factory reset, all of the iBoss settings will be set back to default values (including Internet connection, Internet filtering and password settings.

Note: The tamper log cannot be erased by a factory reset. This is by design for security reasons.

8.2.1 Through the iBoss User Interface

- Login to iBoss Interface (http://myiboss.com).
- From the "**Home**" page, go to "**My Preferences**" and "**System Settings**".
- Click the "**Restore Factory Defaults**" button. You will be prompted to confirm before continuing.

8.2.2 Using the iBoss Console Port

- Connect your computer to the console port of the iBoss. (Please see console setup in this manual for more information on connecting the iBoss to the console port).
- Choose the option Restore Factory Defaults
- Confirm that you would like to reset the factory defaults.

8.3 Technical Support

Phantom Technologies Inc prides itself on supporting our products and services. Please use the information below if you are in need of assistance.

Website Support: http://www.iPhantom.com/troubleshooting.html
Telephone Support: 1.877.PHANTECH (742.6832)
E-mail Support: support@iPhantom.com

9 APPENDIX

9.1 Warranty Information

For warranty information please visit:
https://www.iPhantom.com/warranty.html

BY PROCEEDING TO USE THE PRODUCTS AND SERVICES PROVIDED BY PHANTOM TECHNOLOGIES INC, YOU ACKNOWLEDGE YOUR AGREEMENT TO BE BOUND BY THE FOLLOWING TERMS AND CONDITIONS AVAILABLE AT:
http://www.iPhantom.com/productAndServiceAgreement.html

IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE PRODUCTS AND SERVICES PROVIDED BY PHANTOM TECHNOLOGIES INC.

For the latest news, features, documentation and other information regarding the iBoss please visit:
http://www.PhantomTechnologies.com

10 GLOSSARY

Default Gateway: Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.iPhantom.com) and one or more IP addresses (such as 208.70.74.14). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "iphantom.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier. The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1. A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's. When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID. For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000, it means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

11 REGULATORY STATEMENT

FCC
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC rules.

CE
This equipment has been tested and found to comply with the limits of the European Council Directive on the approximation of the law of the member states relating to electromagnetic compatibility (89/336/EEC) according to EN 55022 Class B.

FCC and CE Compliance Statement
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Safety
This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment.