iBoss Enterprise SWG Web Filter

User Manual

Phantom™
Technologies
www.iboss.com

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

www.iboss.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 SWG 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 & onboard report settings:

Model	Recommended Concurrent Users	Identifiable Computers	Identifiable Users	Filtering Groups	Reports Database Size	Generated Reports	Report Schedules
1550	50-100	120	120	25	25 GB	50	5
1750	101-200	240	240	50	25 GB	75	10
2150	201-300	360	360	60	25 GB	75	10
2550	301-400	480	480	75	25 GB	100	15
3550	401-600	720	720	100	25 GB	100	20
4550	601-1000	1200	1200	125	25 GB	125	25
5550	1001-1500	1800	1800	200	25 GB	250	30
6550	1501-2000	2400	2400	300	25 GB	300	35
7550	2001-2500	3600	3600	100	25 GB	300	35
8550	2501-4000	4800	4800	300	25 GB	300	35
9550	4001-6000	7200	7200	300	25 GB	300	35
10500	6001-12,000	7200	7200	300	25 GB	300	35
14500	12,001-50,000	7200	7200	300	25 GB	300	35
14500x	50,000-100,000	7200	7200	300	25 GB	300	35
16500	12,001-50,000	7200	7200	1000	25 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

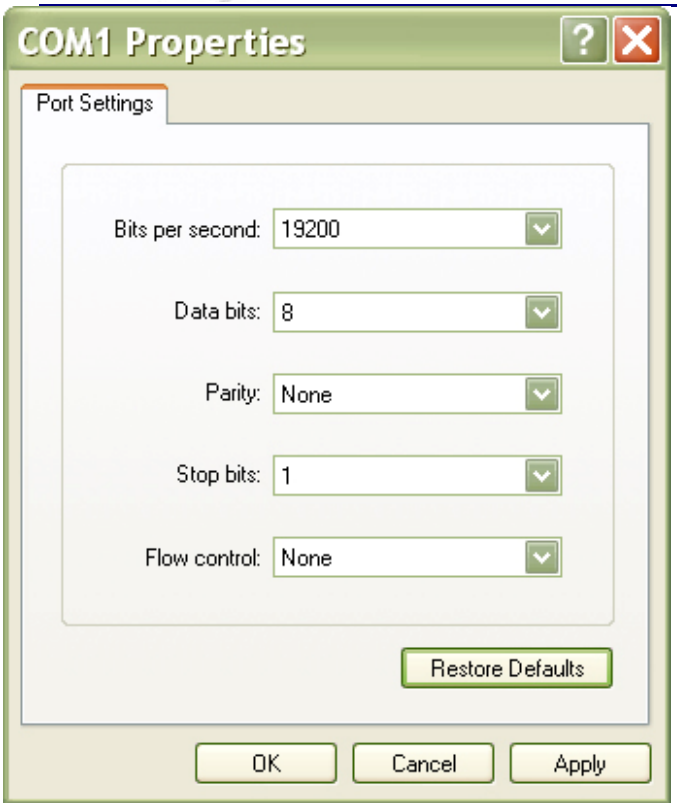

Figure 1 - COM Properties

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.

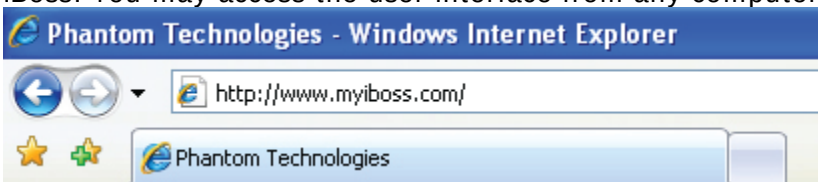

Figure 2 - iBoss User Interface

3.2.3 Setup Network Connection

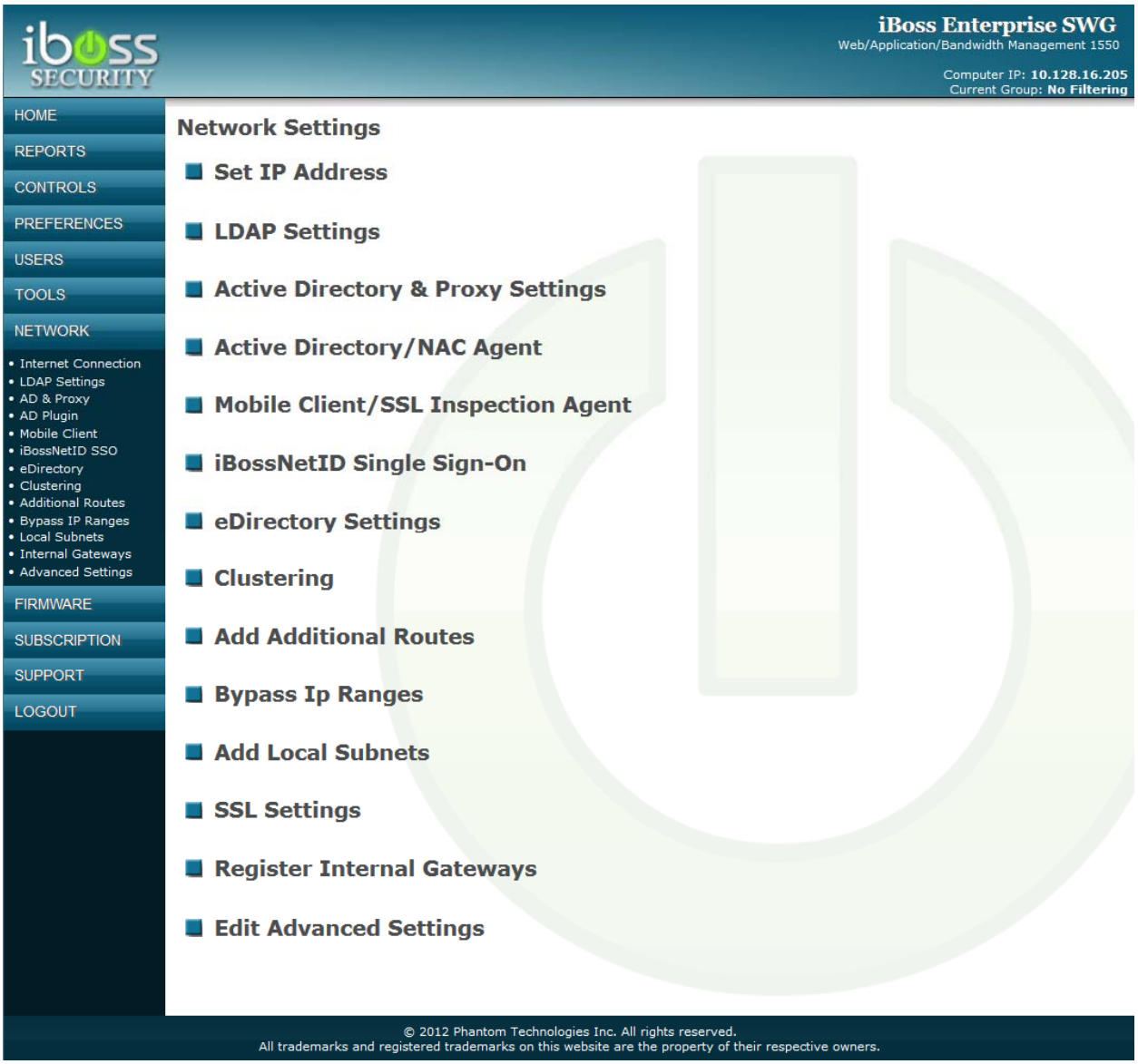

Figure 3 - Setup Network Connection

The "Setup Network Connection" menu lets you choose options for configuring the current iBoss connection settings. There are eleven 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.

Setup IP Address - 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 typically used with the Internet Access Window.

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 / NAC Agent - 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. This section also allows you to setup integration with Network Access Controllers for user authentication.

Mobile Client / SSL Inspection Agent - This option allows you to setup the iBoss mobile client for Windows, MAC and the iPad/iPod browser. This will allow you to also use the local SSL Inspection Agent.

iBossNetID Single Sign-On - This option allows you to setup the iBossNetID Single Sign-On Agent that installs on the computer as an agent to authenticate usernames for Windows. This section also allows you to setup the Apple Logon Hooks for user authentication with MACs.

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.

SSL Settings - This option allows you to configure a SSL Certificate to allow https access to the iBoss interface.

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

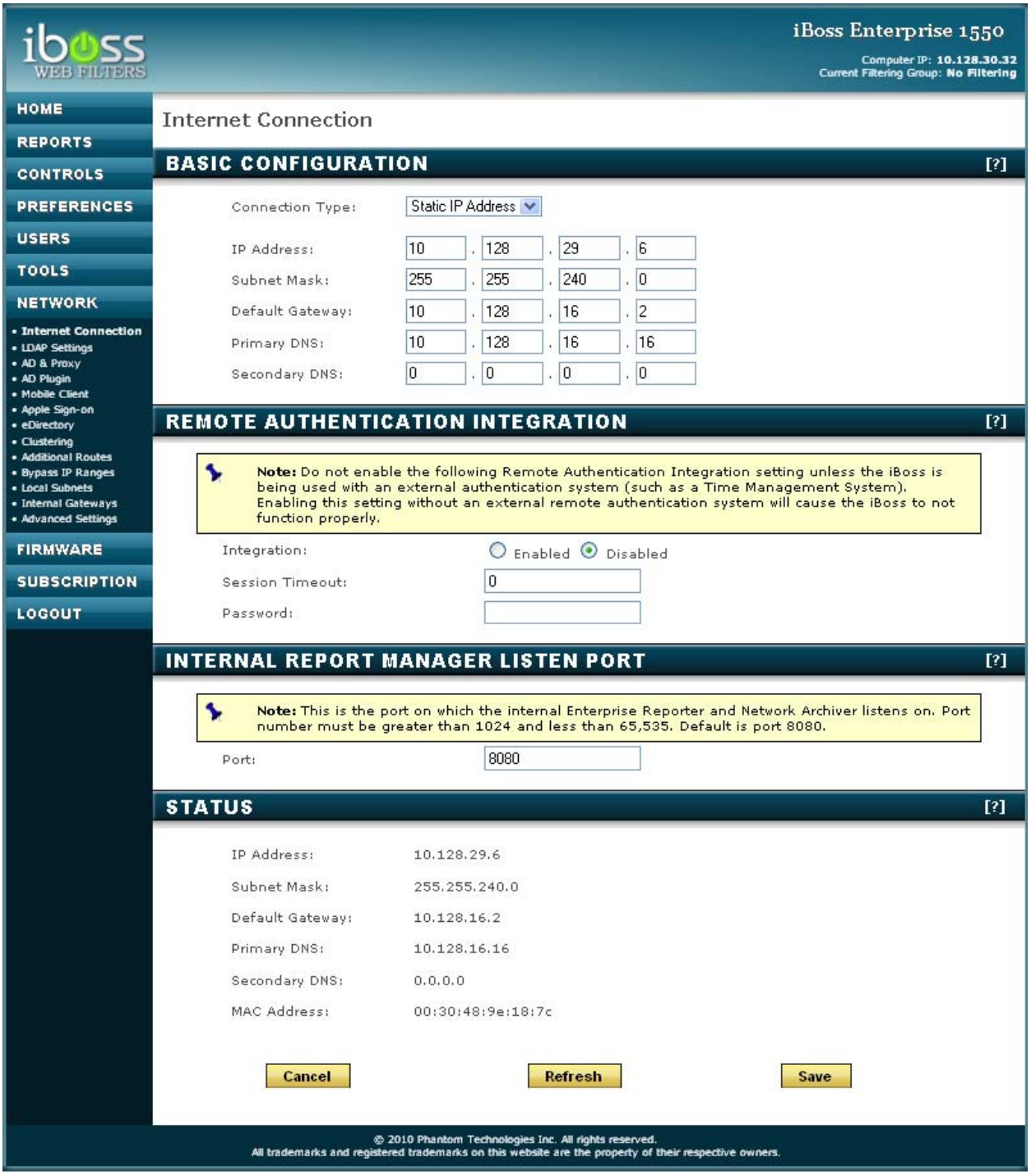

Figure 4 - Configure Internet Connection

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

This feature allows Remote Authentication Integration. This is an OEM feature that is only used for third party applications. Typically this is not used unless specifically needed by third party applications.

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

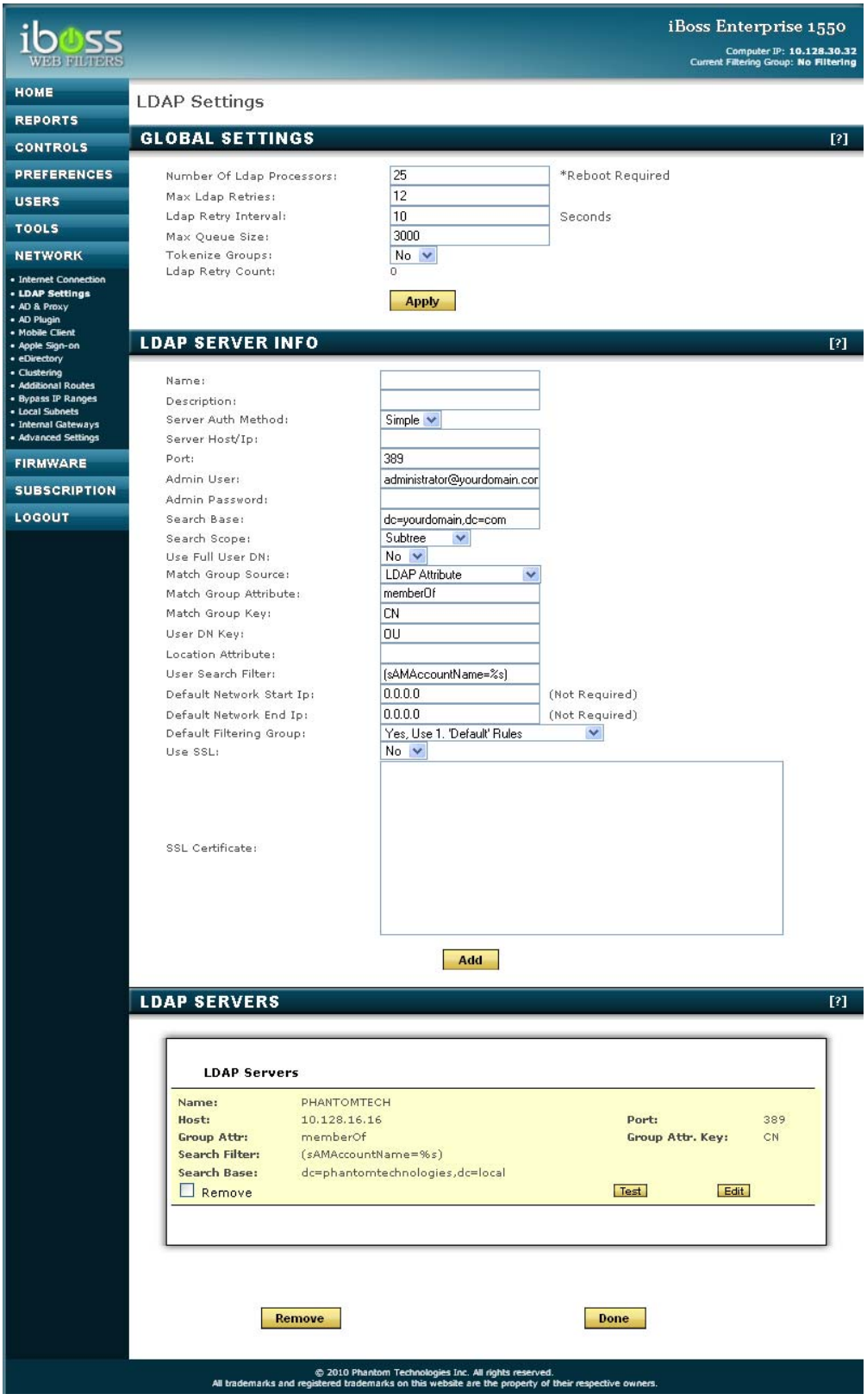

Figure 5 - LDAP Settings

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 Type - This option allows you change the server type from General LDAP/Active Directory to Open Directory and Open LDAP.

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: dc=iphantom,dc=com

Match Group source – You may select to look for group matches within an LDAP attribute specified by 'Match Group Attribute' or the 'User DN' or both.

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

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. Active Directory Example: CN

User DN Key- If 'User DN' is included within the 'Match Group Source' option then this key is used to parse the User DN. Active Directory Example: OU

Location Attribute - Deprecated

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. Active Directory Example: (sAMAccountName=%s)

Active Directory Overview: An LDAP query is made for the sAMAccountName attribute containing the username and the memberOf attribute is requested. The value of the memberOf attribute will be the DN of each group that the user belongs to. The Group Key of CN is used to search the returned DN values for the group names. These names are compared to your iBoss filtering groups. If there is a match that filtering group is used. If there are multiple matches, the filtering group configured with the highest priority is used.

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

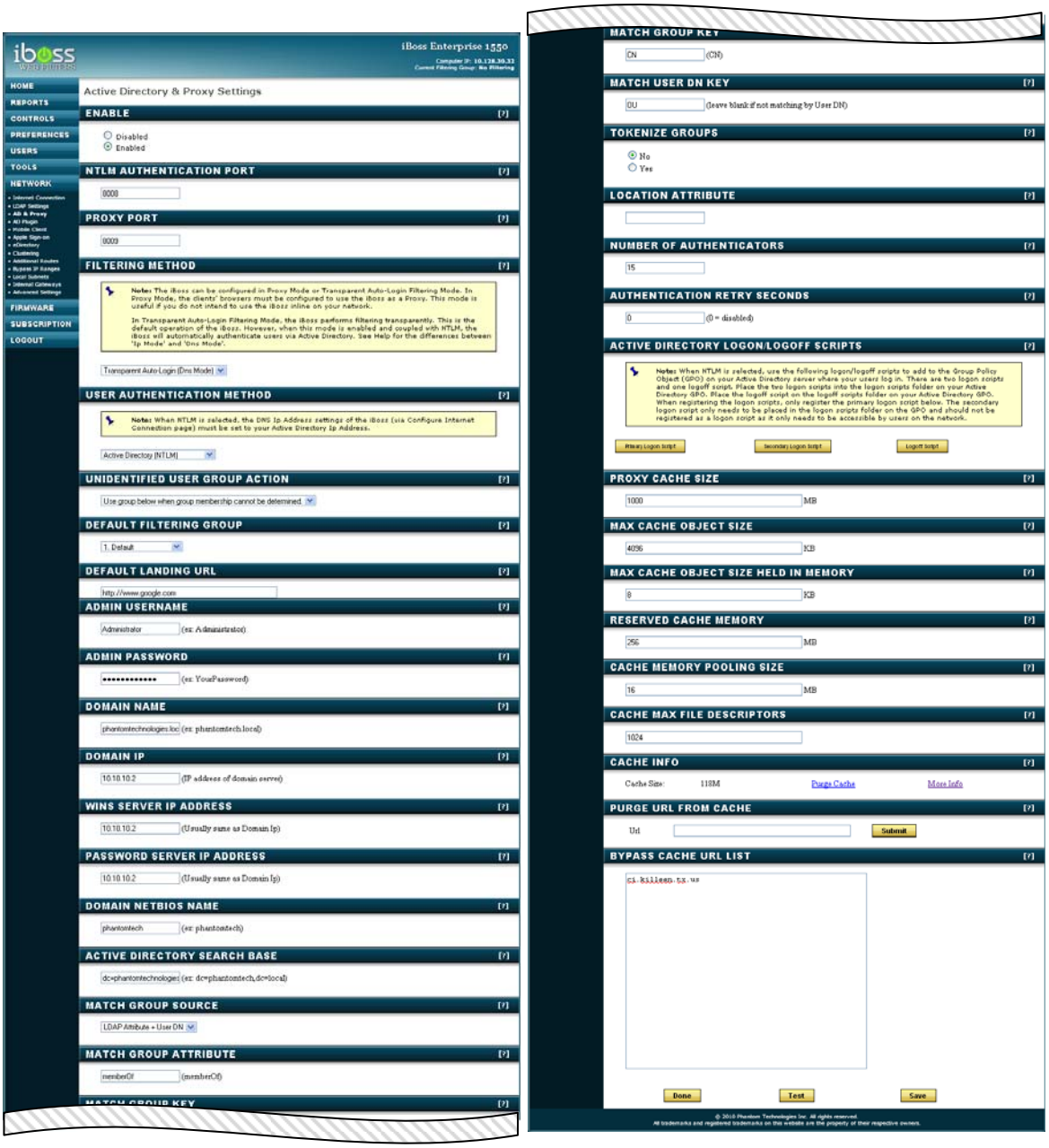

Figure 6 - Active Directory & Proxy Settings

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 (NTLM)**, **Local iBoss User Credentials**, **Active Computer Policy** or **Mobile Devices (Source IP Address Based)**.

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.

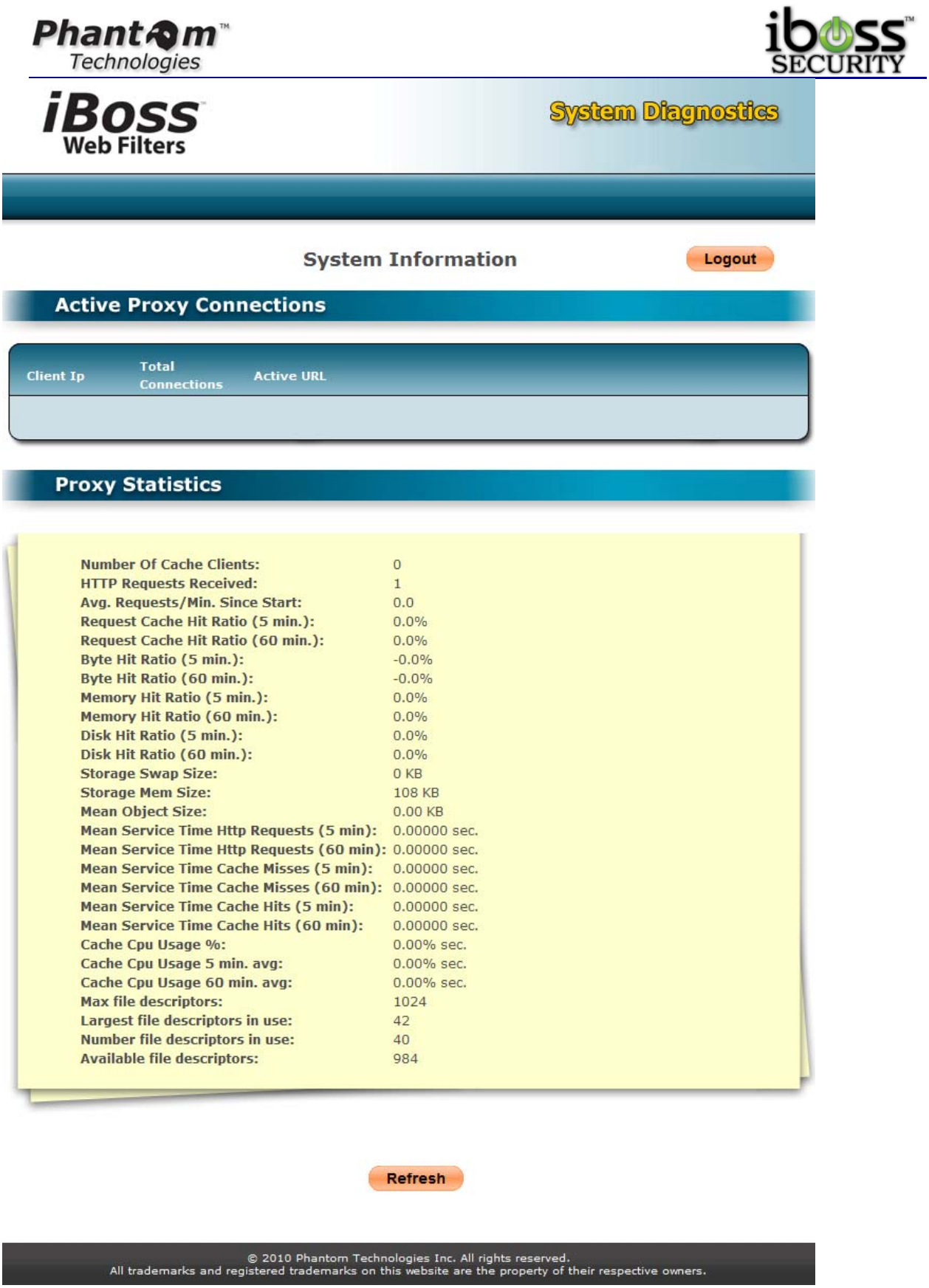

Figure 7 - Proxy Cache System Information

3.2.3.3.1 *Proxy Mobile Devices (Source IP)*

Mobile Devices (Source IP Based) option under User Authentication Method on the AD & Proxy settings page is an authentication method that allows the proxy to authenticate users based on their source IP. When a new client hits the proxy and this authentication method is enabled, the client is redirected to an https page where they can enter their credentials (local or ldap). Once the user authenticates, the username is associated with that source IP and the user can surf through the proxy (logs are associated with username).

Now, if the client is mobile, the source IP is still added to the computers list and marked **(Mobile).** This allows this method to be used for mobile filtering (especially in cases where they are not using MDM or are using Apple Configurator or something other than MobileEther).

The new feature works by programming the device with a pac script which is hosted on the iboss (link shown on proxy page authentication drop down list) or downloaded and placed on external webserver if additional proxy pac configuration is necessary.

The address is based on the hostname and domain that is setup for the iBoss under Home → Preferences → System Settings.

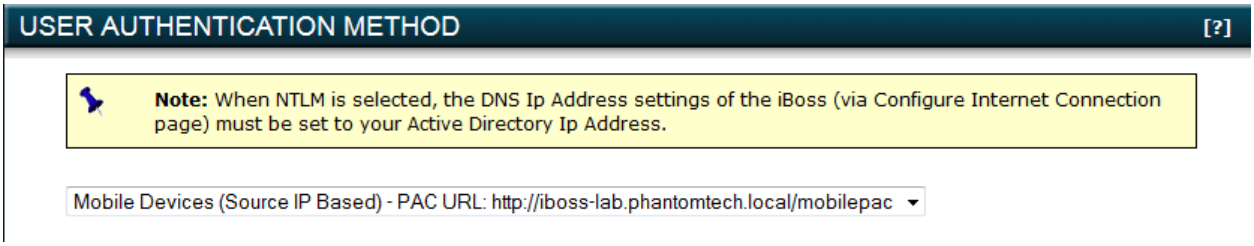

Figure 8 - Proxy Mobile Devices (Source IP)

function FindProxyForURL(url,host) { if(localHostOrDomainIs(host,"iboss-lab.phantomtech.local")) {return "DIRECT"; } else{ return "PROXY iboss-lab.phantomtech.local:8009"; } }

3.2.3.3.2 *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.

3.2.3.3.3 *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.

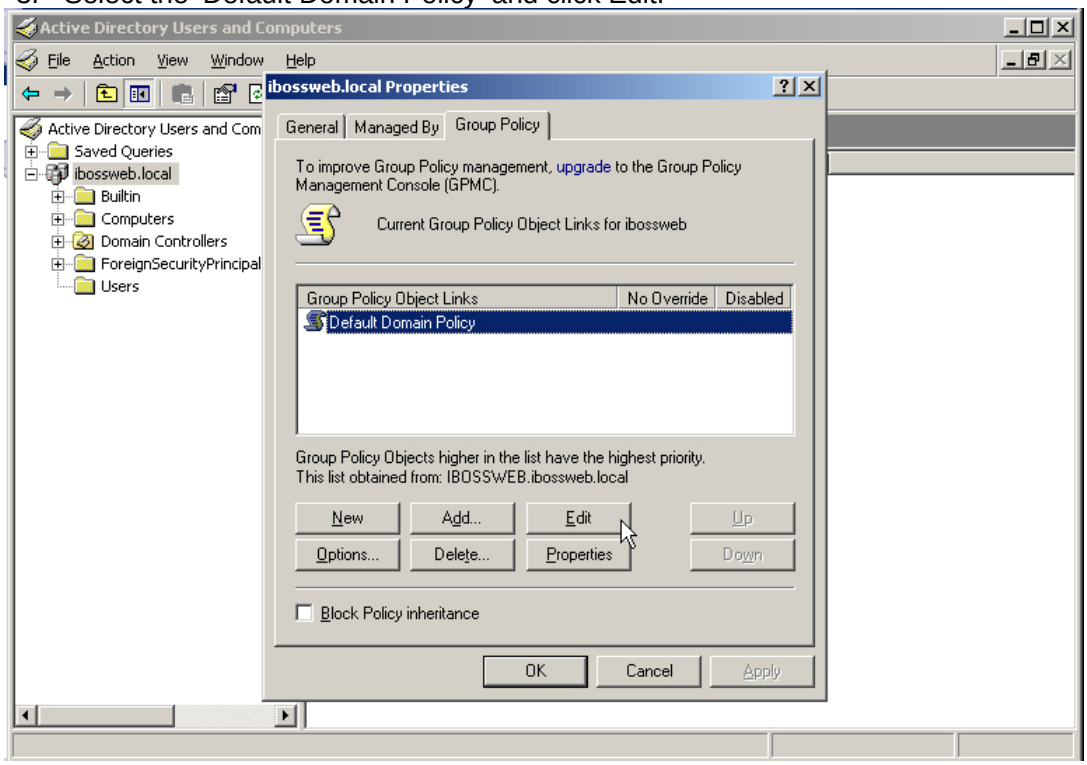

Figure 9 - GPO Default Domain Policy

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

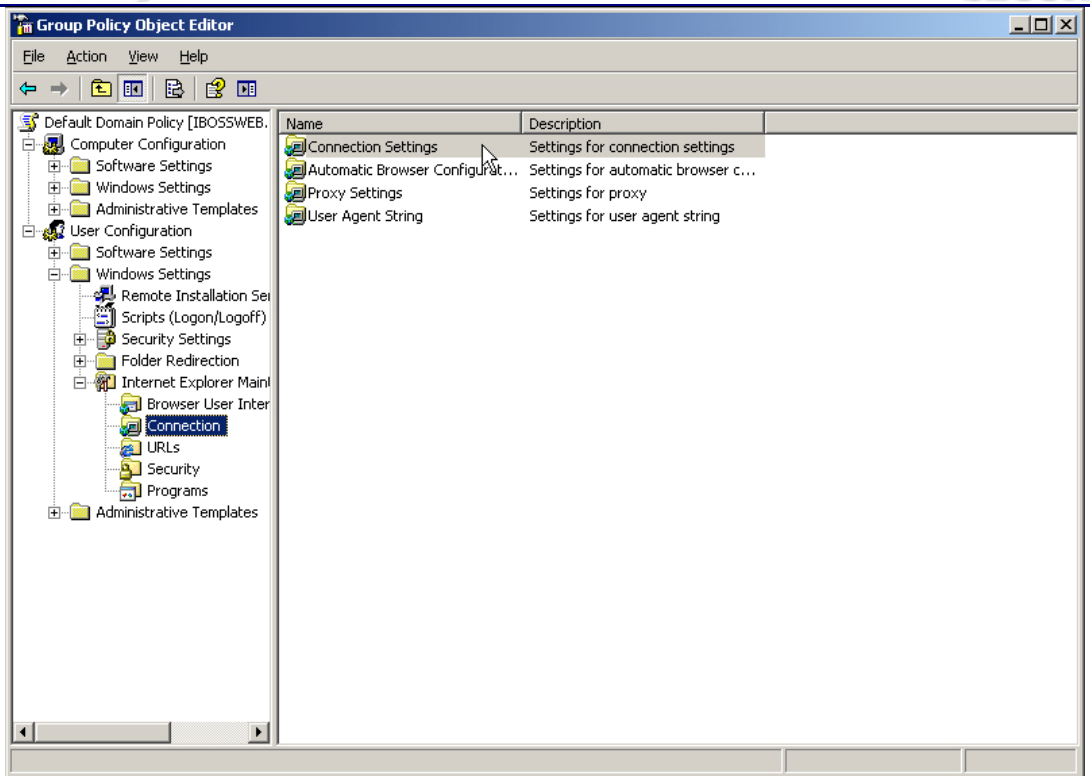

Figure 10 - GPO Connection Settings

6. Select the option 'Import the Connection Settings' and click Modify Settings.

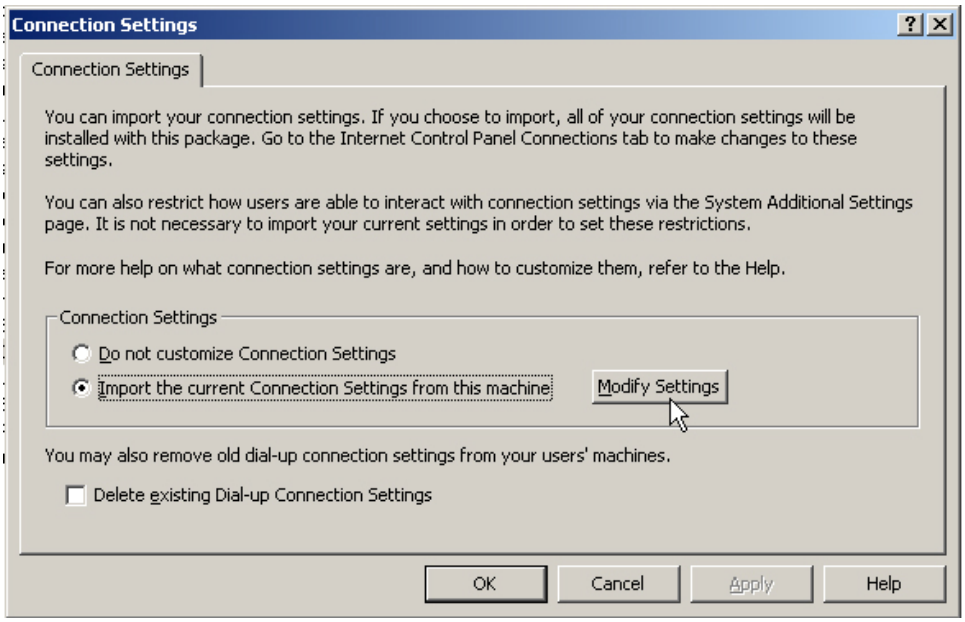

Figure 11 - GPO Import the Connection Settings

7. Click 'LAN Settings' and check 'Use a proxy server'.

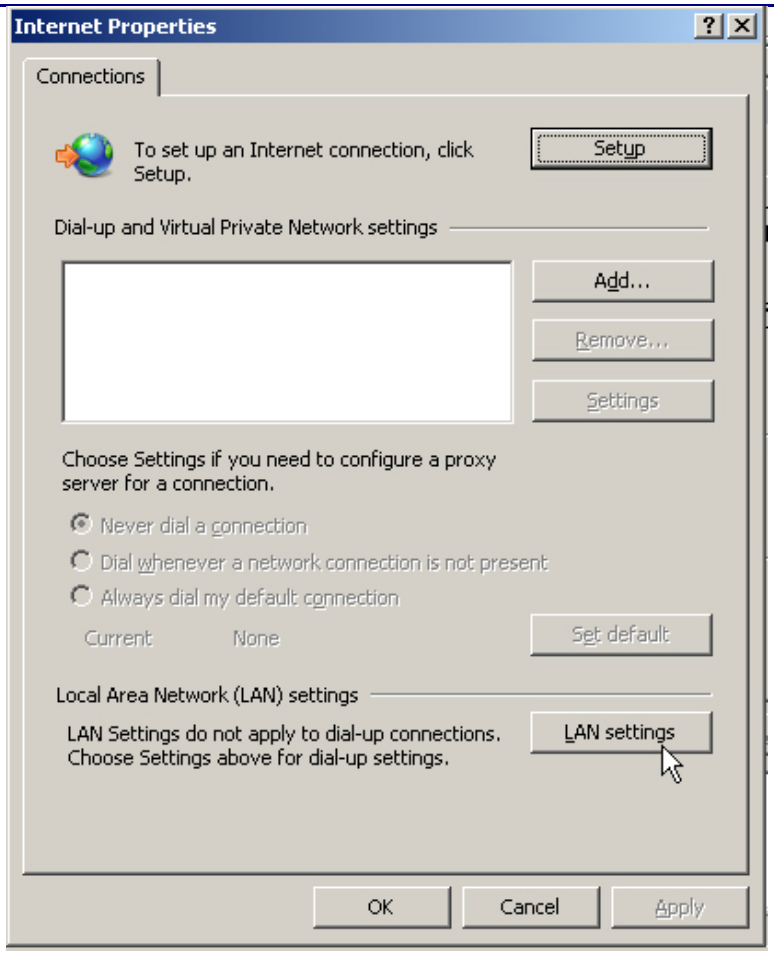

Figure 12 - GPO Use Proxy Server

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

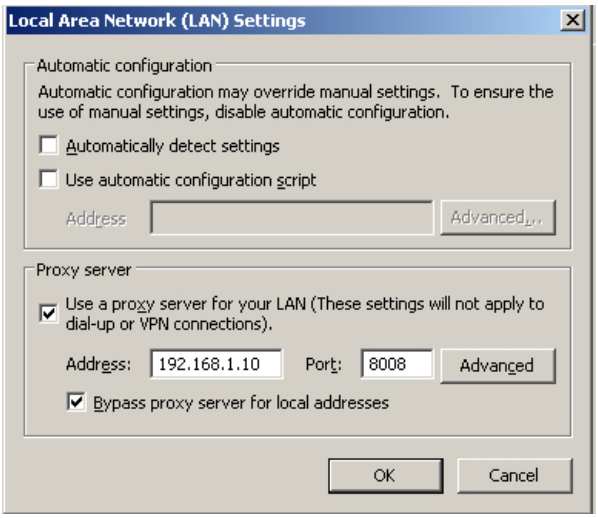

Figure 13 - GPO Local Area Network Settings

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

3.2.3.3.3.1 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.

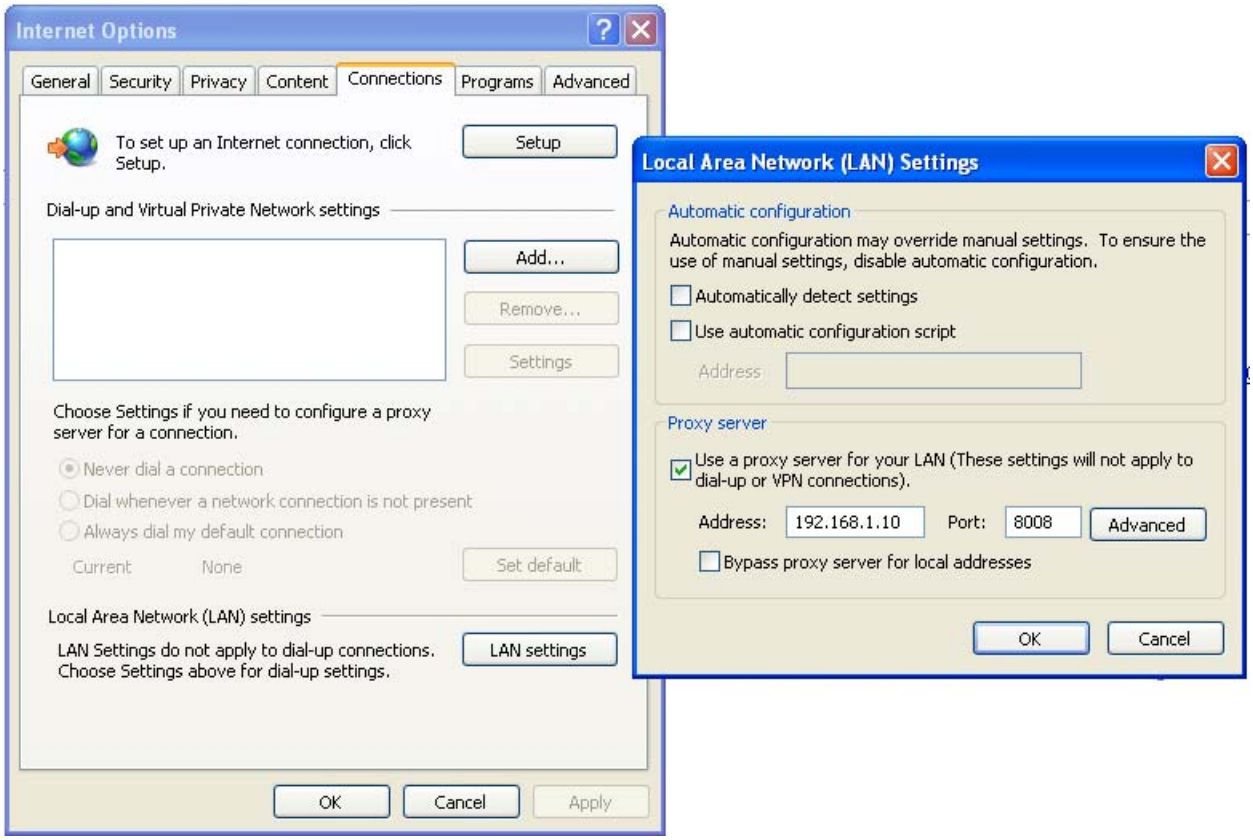

Figure 14 - Manual Proxy with Internet Explorer

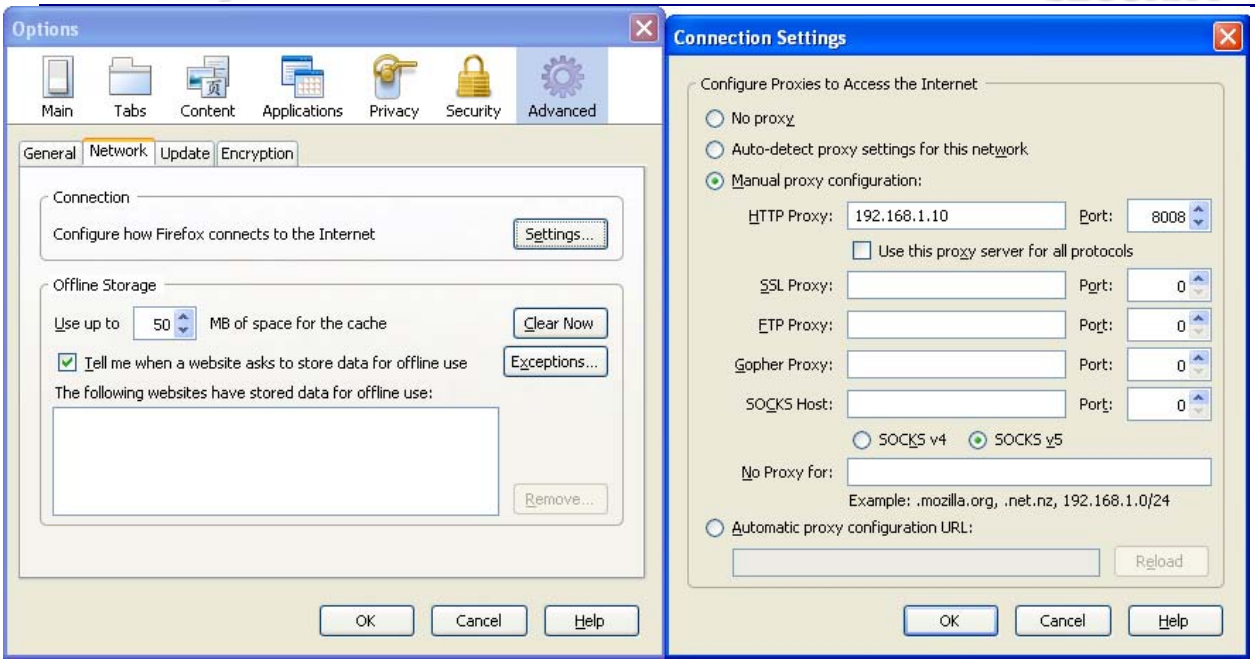

Figure 15 - Manual Proxy with Mozilla Firefox

3.2.3.3.3.2 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.

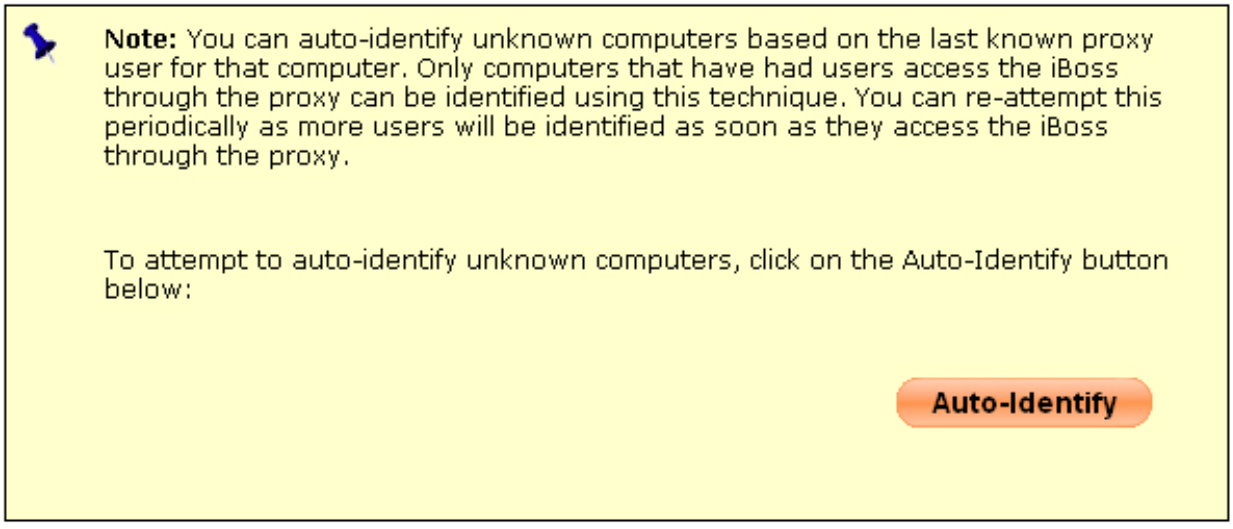

Figure 16 - Automatic Identify of Unknown Computers

3.2.3.4 Active Directory Plugin

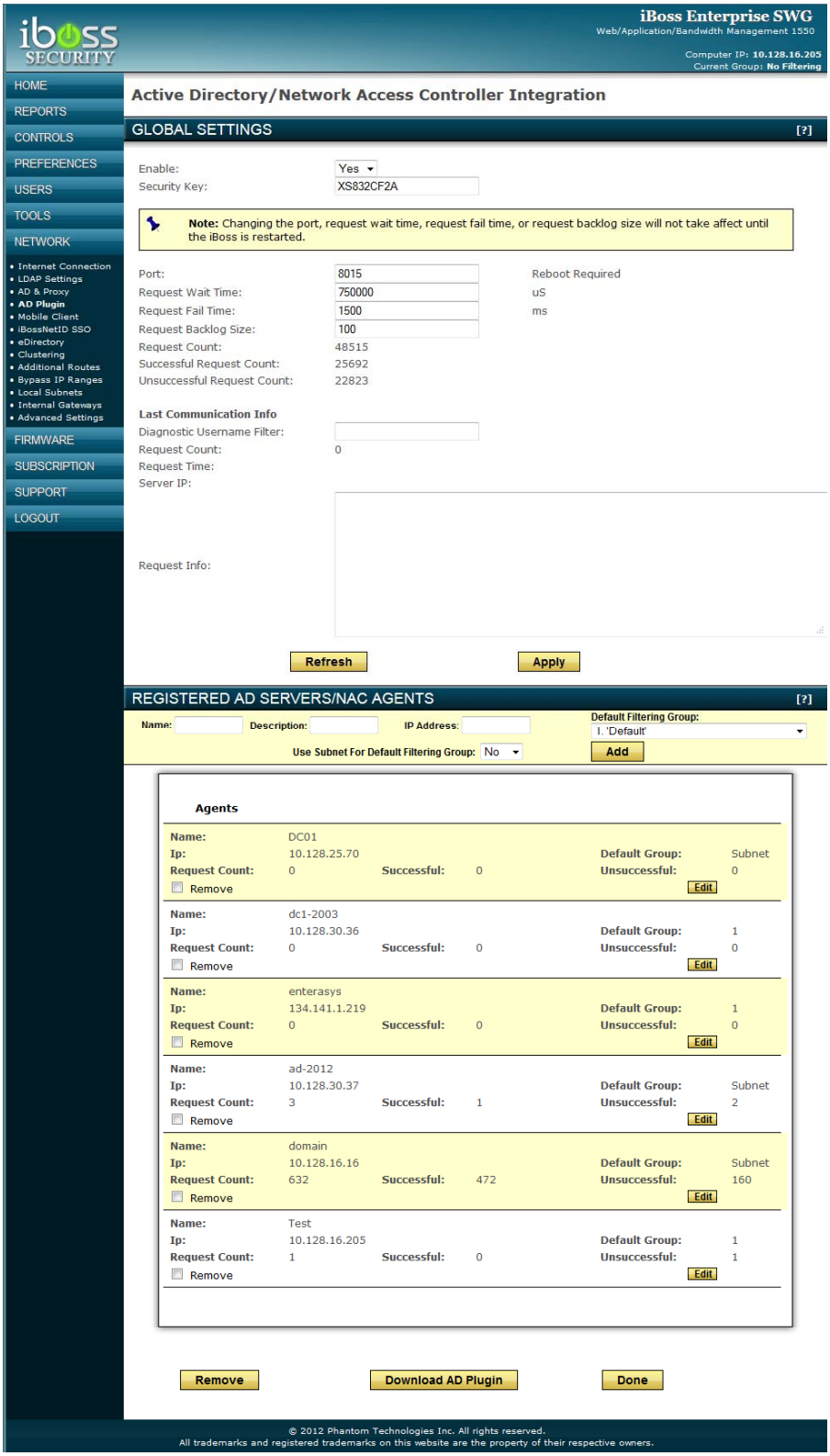

Figure 17 - AD Plugin / NAC Integration

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.

Use Subnet For Default Filtering Group – This will either default to the group chosen above or the subnet default filtering group if chosen to yes.
Once finished, click "Add" to add the Active Directory server.

3.2.3.4.1.1 iBoss Active Directory Plugin Configuration

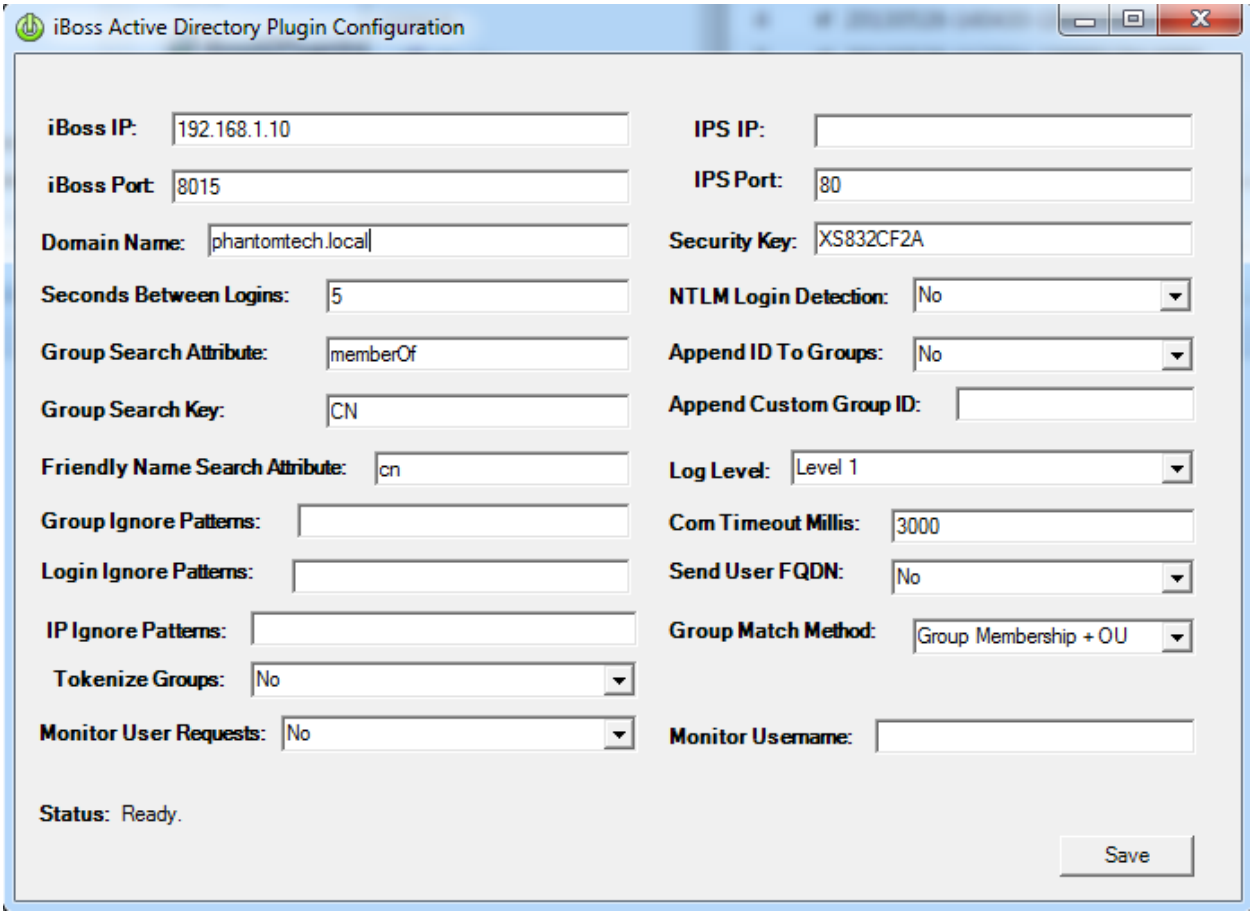

Figure 18 - iBoss Active Directory Plugin Configuration

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.
IPS IP – This is the IP address of the iBoss IPS/IDS device if you have it also.
IPS Port – This is the port number of the IPS/IDS device.
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.

Append ID To Groups – This is the field that allows you to set No or Append Domain Name for student@domain1.local or a custom Group ID.
Append Custom Group ID – This is the field for above if Custom Group ID is chosen to enter a custom Group ID to append to the group name.
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.
Group Ignore Patterns – These are ignore patterns within the group names that shouldn't match users filtering groups with.
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
Group Match Method – This is the method of how the groups are matched by Security Group or Organizational Unit (OU)
Tokenize Groups – This is the setting that allows you to set wildcard group names like Student for Groups called Students 2013 & Students 2014 to tokenize the group names to just match Student.
Monitor User Requests – This option allows you to monitor a specific username in the event viewer.
Monitor Username – This is the field for the feature above for monitoring their username.

NOTE: You may need to Right-click the program under Start and Run as Administrator.

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

3.2.3.4.1.2 Edit AD Plugin Orca

Orca is a Microsoft program that allows you to edit the .msi installer of the AD Plugin before installing. This is beneficial to configure the settings prior to installing the AD Plugin on multiple servers.

First, install the Orca.msi program. Once installed, you can right-click the AD Plugin .msi file and click Edit with Orca.

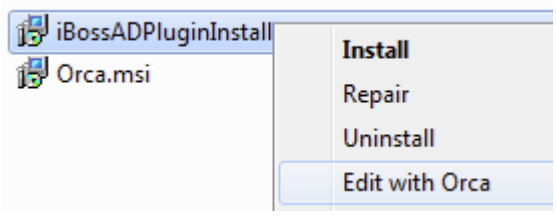

Figure 19 - Edit with Orca option

When it opens in Orca, click on **Property** on the left side and then click on **Property** at the top to sort the options by name.

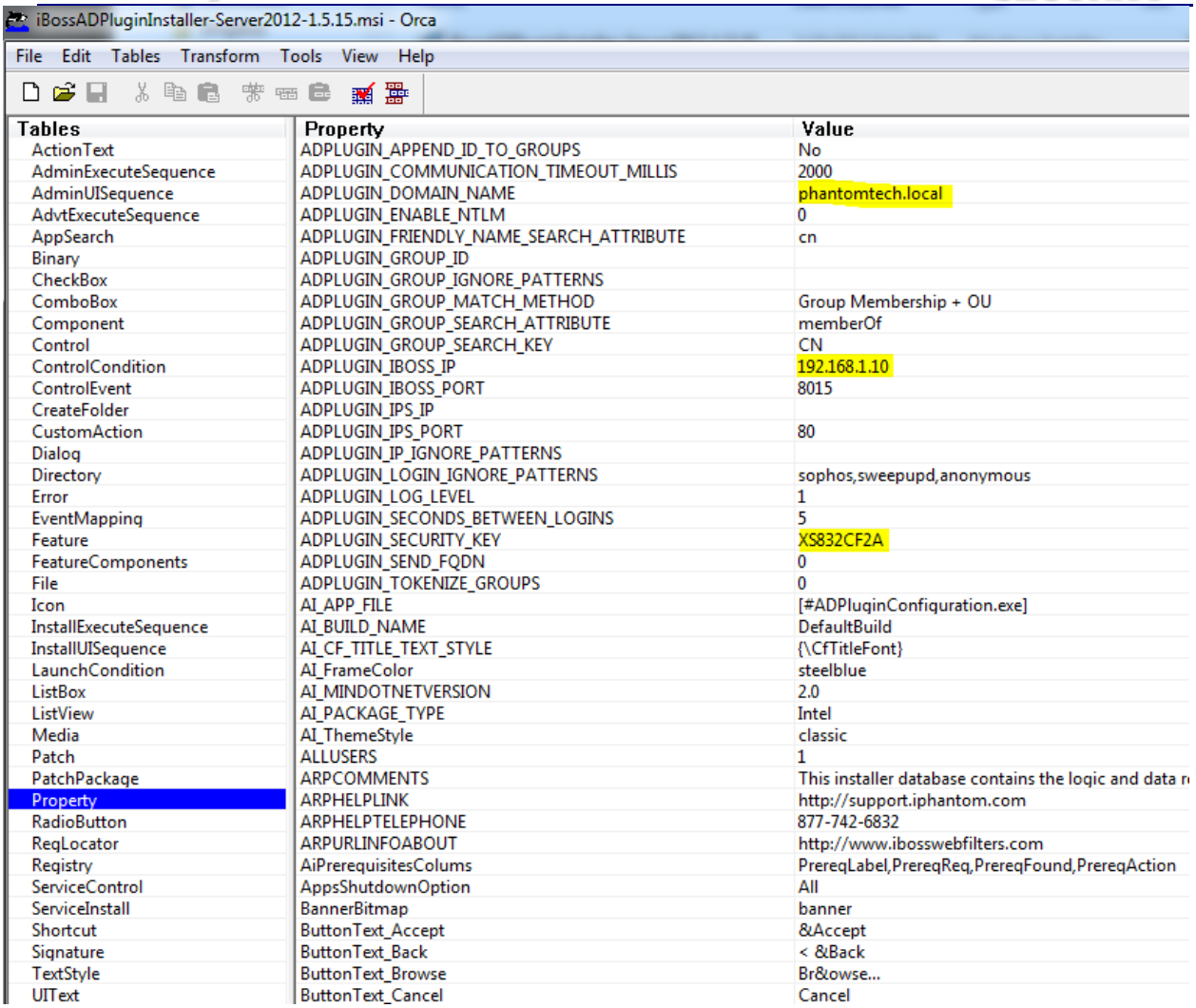

Figure 20 - AD Plugin Properties with Orca

Edit the highlighted fields for the Security Key, IP address of the iBoss and the domain.

Once finished, click the **Save** icon or close the program and it will prompt you to Save and click **Yes**. **Do not** click **File** and then **Save As**, as this will only save the select property that you have selected.

3.2.3.4.1.3 Ad Plugin Radius Audit Log

The iBoss AD Plugin has the ability to audit logs for Radius Authentication. In the parameters of the AD Plugin installation, there are additional features to modify for the Radius Audit Log. The default Radius Audit Path is at C:\Windows\System32\LogFiles.

ADPLUGIN_RADIUS_AUDIT_LOG_ENABLED	1
ADPLUGIN_RADIUS_AUDIT_LOG_FILE_PATTERN	IN*
ADPLUGIN_RADIUS_AUDIT_LOG_MONITOR_INTERVAL_SECONDS	2
ADPLUGIN_RADIUS_AUDIT_LOG_PATH	C:\Windows\System32\LogFiles

Figure 21 - AD Plugin Radius Audit Log Config

3.2.3.4.1.4 Active Directory Audit Logon Events

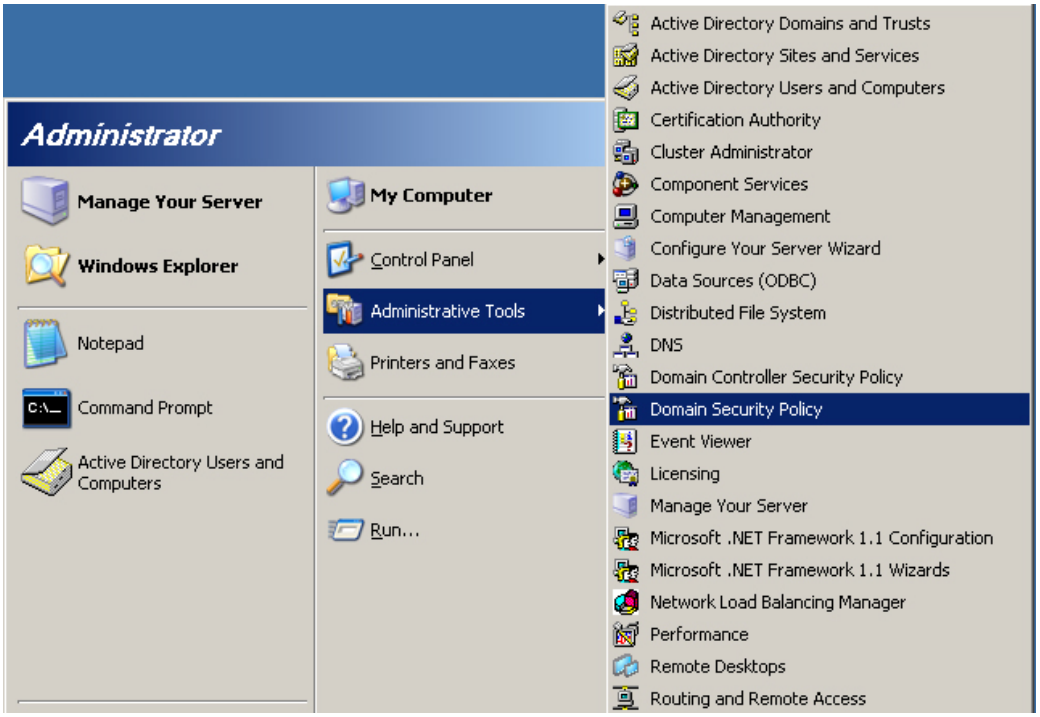

Figure 22 - Domain Security Policy

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.

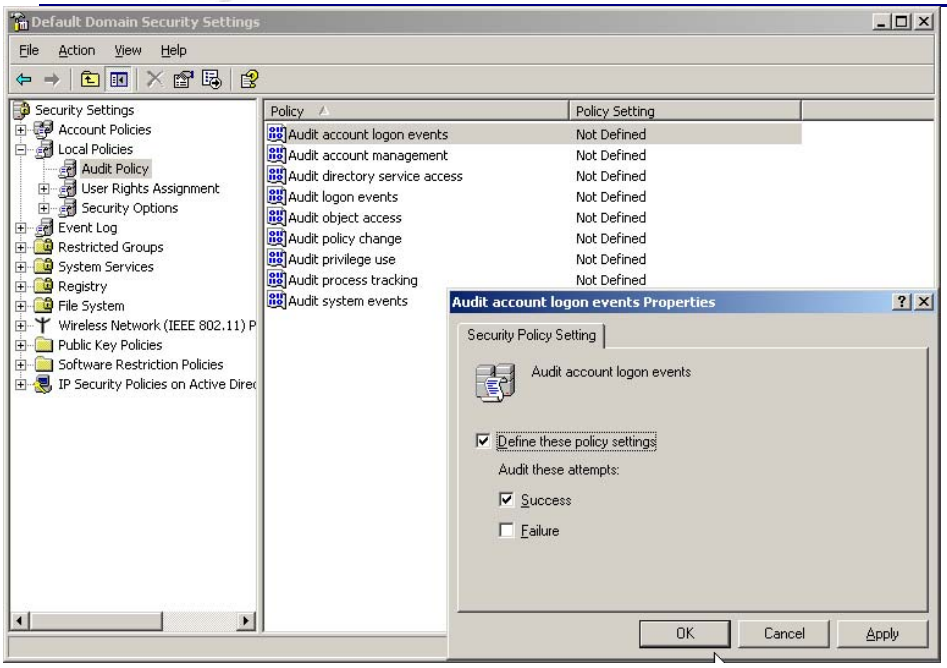

Figure 23 - Audit Account Logon Events

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**.

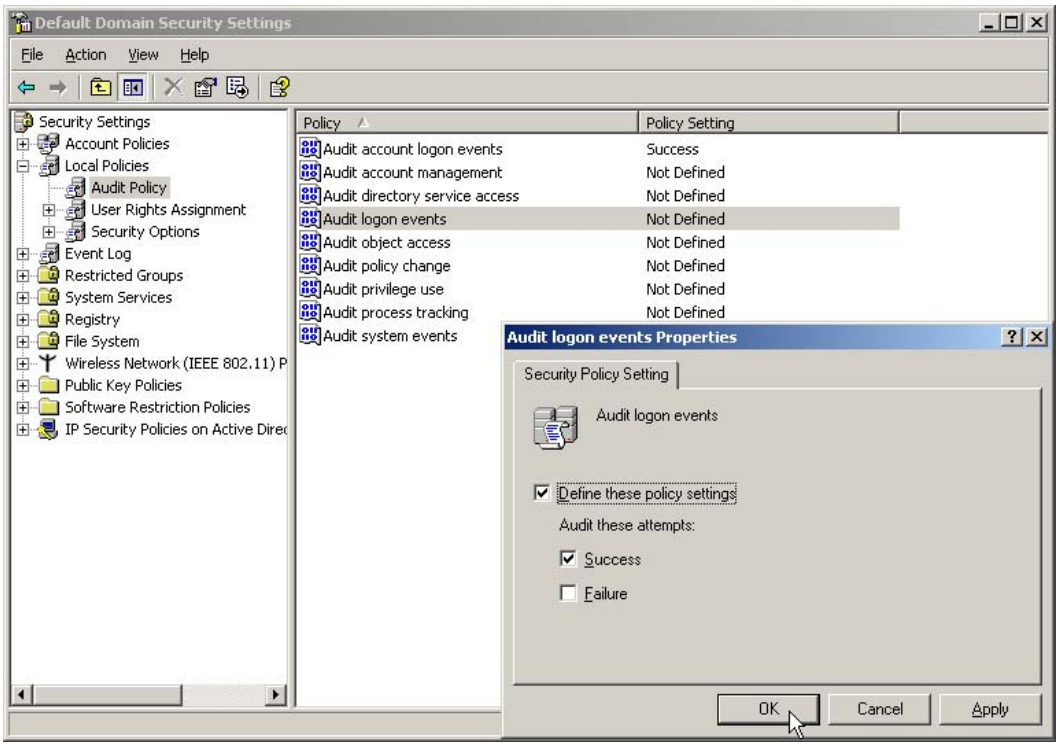

Figure 24 - Audit Logon Events

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 NAC Integration

Please see Enterasys Mobile IAM iBoss Integration Guide for details on integrating with the Enterasys NAC. You can obtain this from iBoss Support.

3.2.3.6 Mobile Client/Local SSL Inspection Agent

Please see iBoss Security Agents guide for more details in the iBoss Security Agent mobile client install and local SSL Inspection Agent

3.2.3.7 iBossNetID Single Sign-On Agent

Please see iBossNetID Install Guide for more details on installing this. The latest document can be obtained for the download link within the iBoss interface.

3.2.3.8 eDirectory Settings

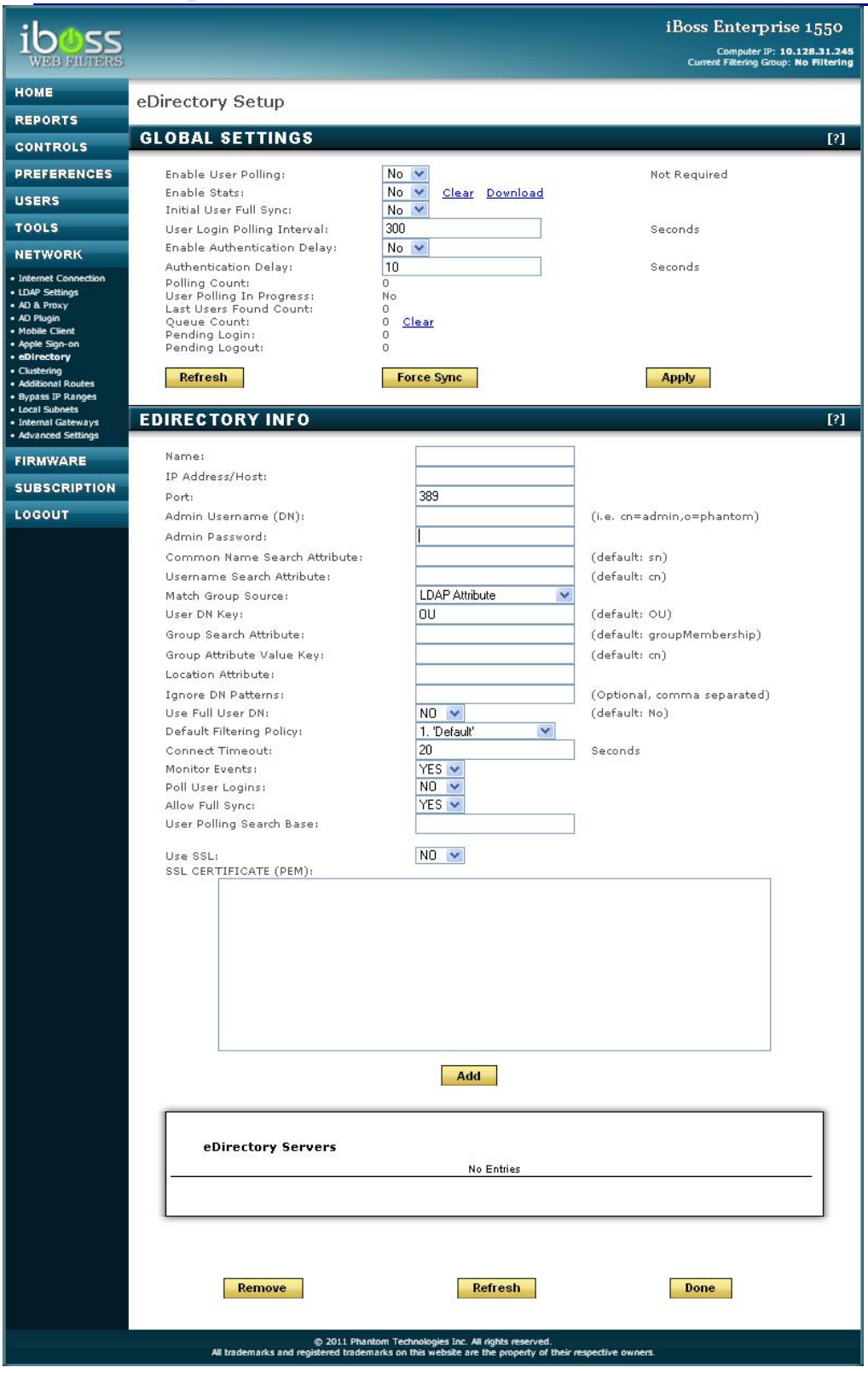

Figure 25 - eDirectory Settings

3.2.3.9 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.

3.2.3.9.1.1 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 eDirectory 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.

3.2.3.10 Clustering

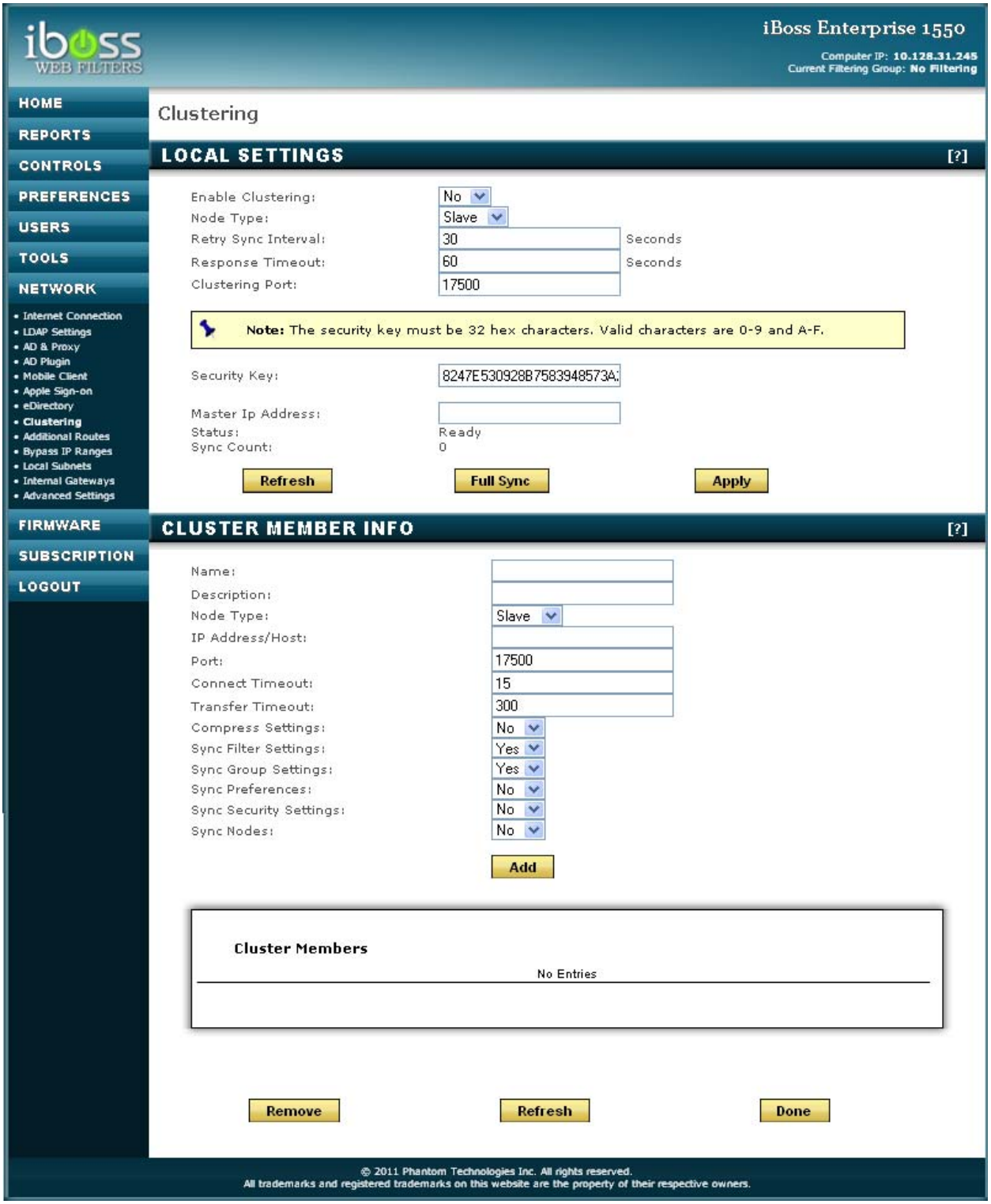

Figure 26 - Clustering

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.

3.2.3.11 Add Additional Routes

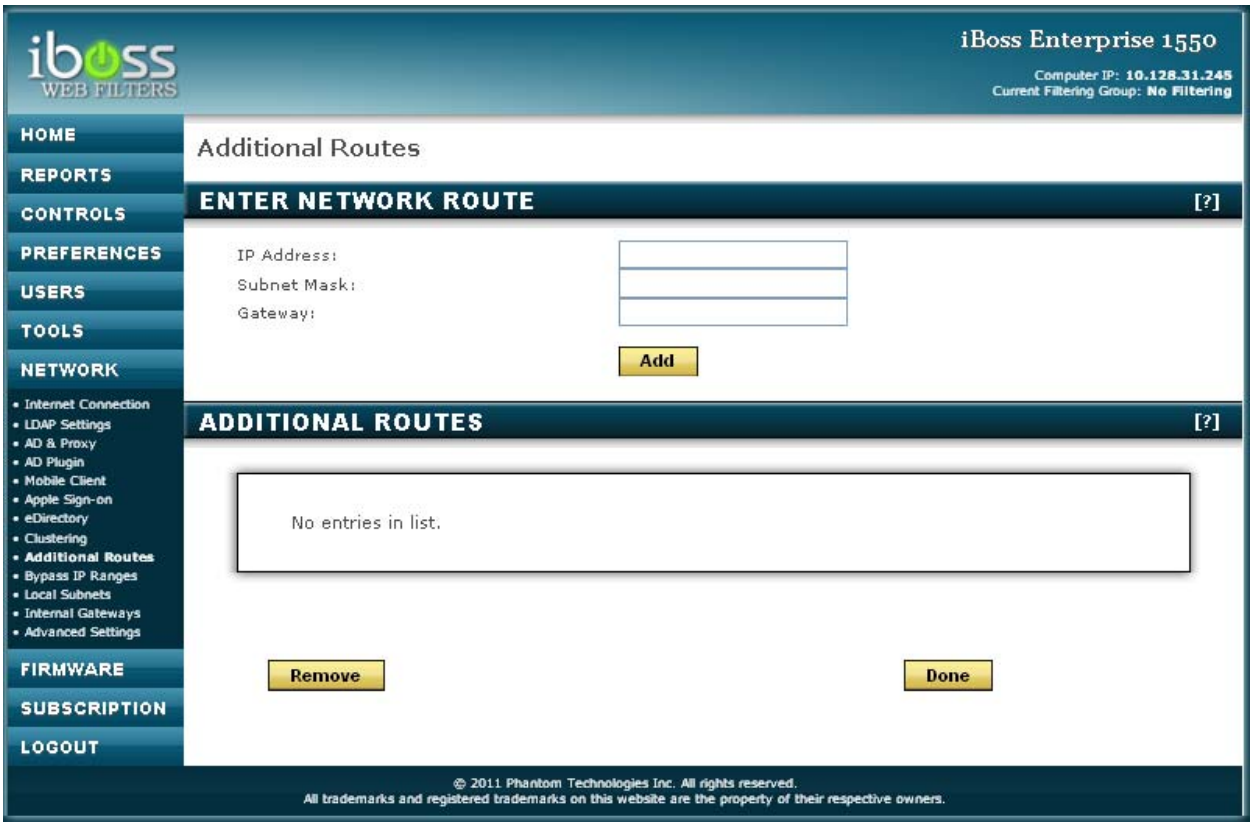

Figure 27 - Add Additional Routes

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.

3.2.3.12 Bypass IP Ranges

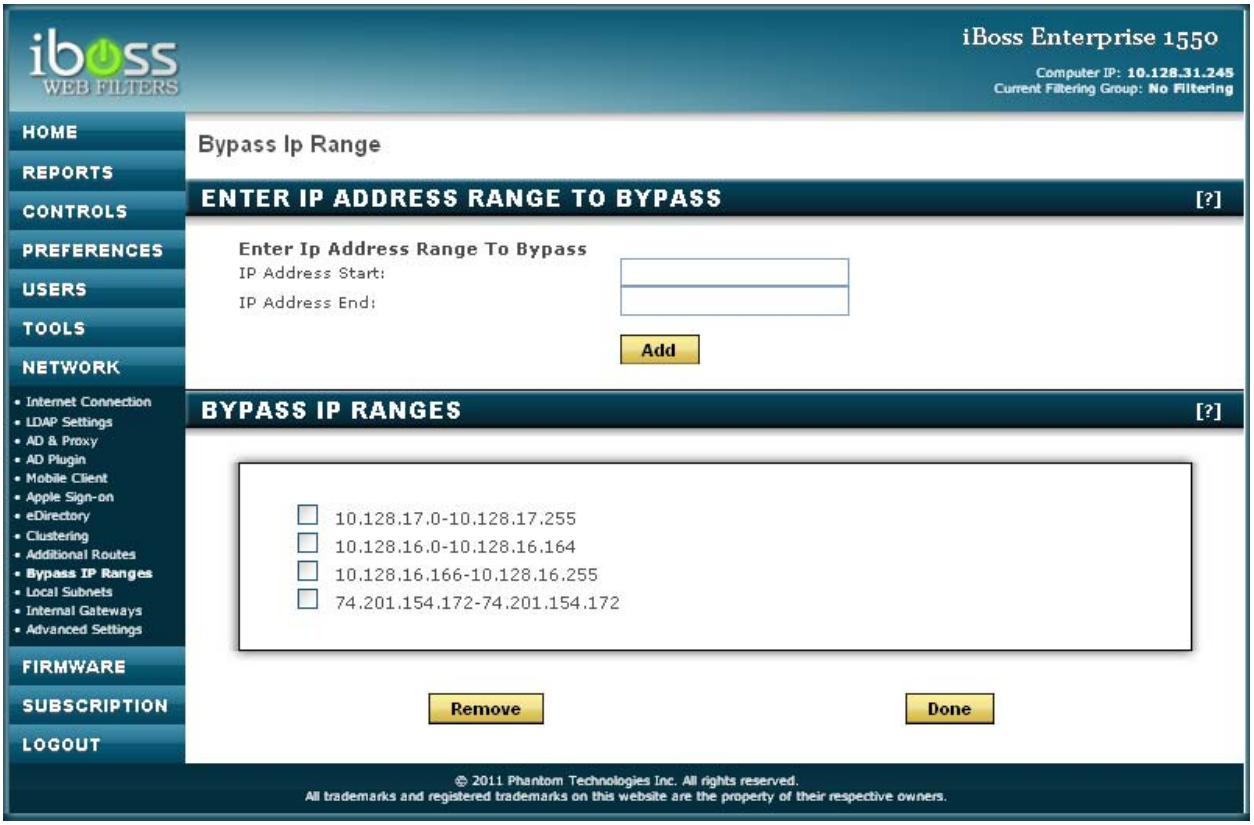

Figure 28 - Bypass IP Range

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.

3.2.3.13 Add Additional Local Subnets

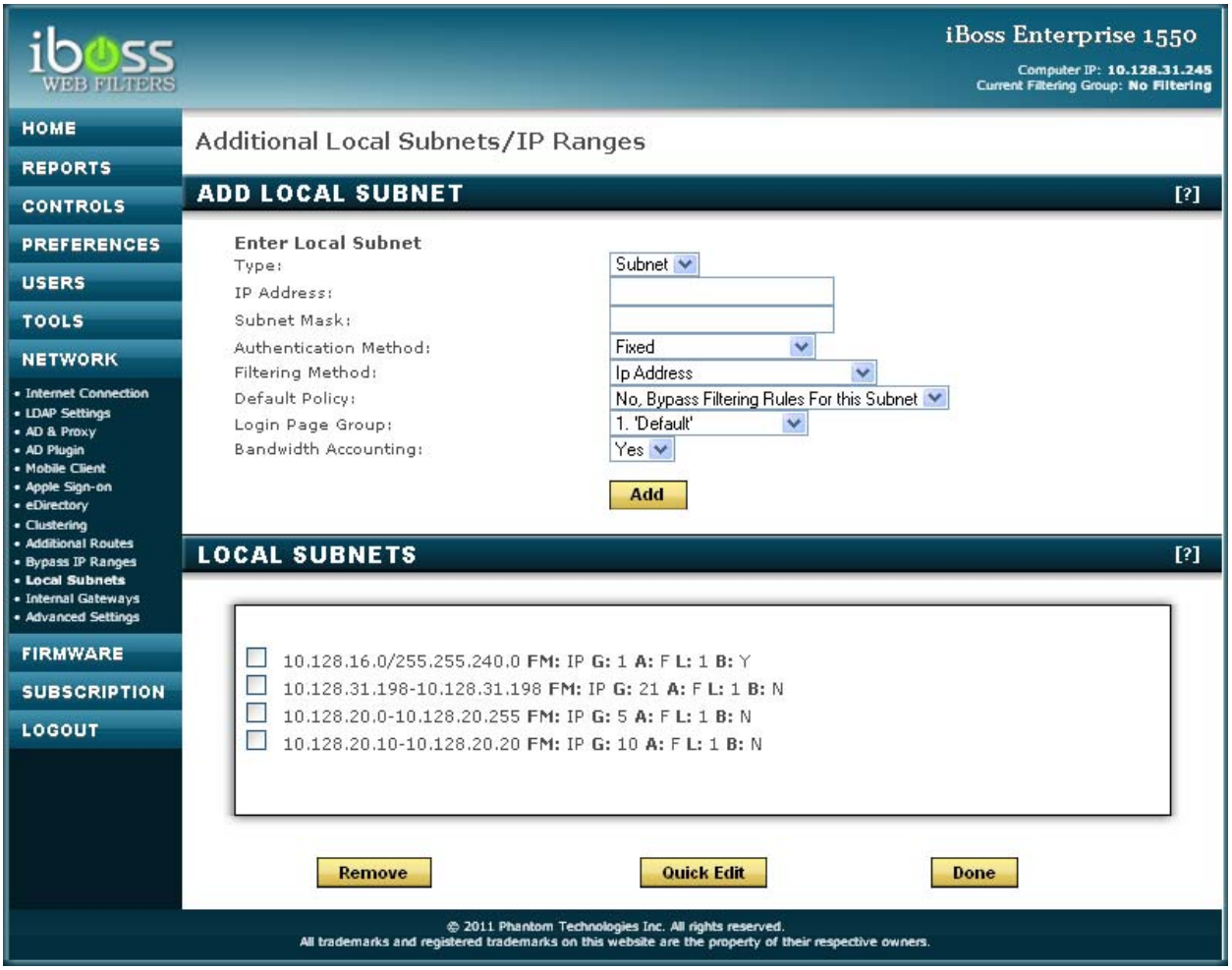

Figure 29 - Add Additional Local Subnets

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.

Authentication Method - The recommended option is "**Fixed**". With this option the iBoss presents the user with the iBoss login page if "**Require User Login**" is selected as the default policy and the user has not been authenticated (transparently or by other methods). The iBoss login page will NOT be presented if the user was authenticated transparently or the default policy is not "**Require User Login**". Selecting "**Active Directory/NTLM"** will cause the iBoss to attempt single sign-on/NTLM if the user was not authenticated transparently.

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.

3.2.3.14 SSL Settings

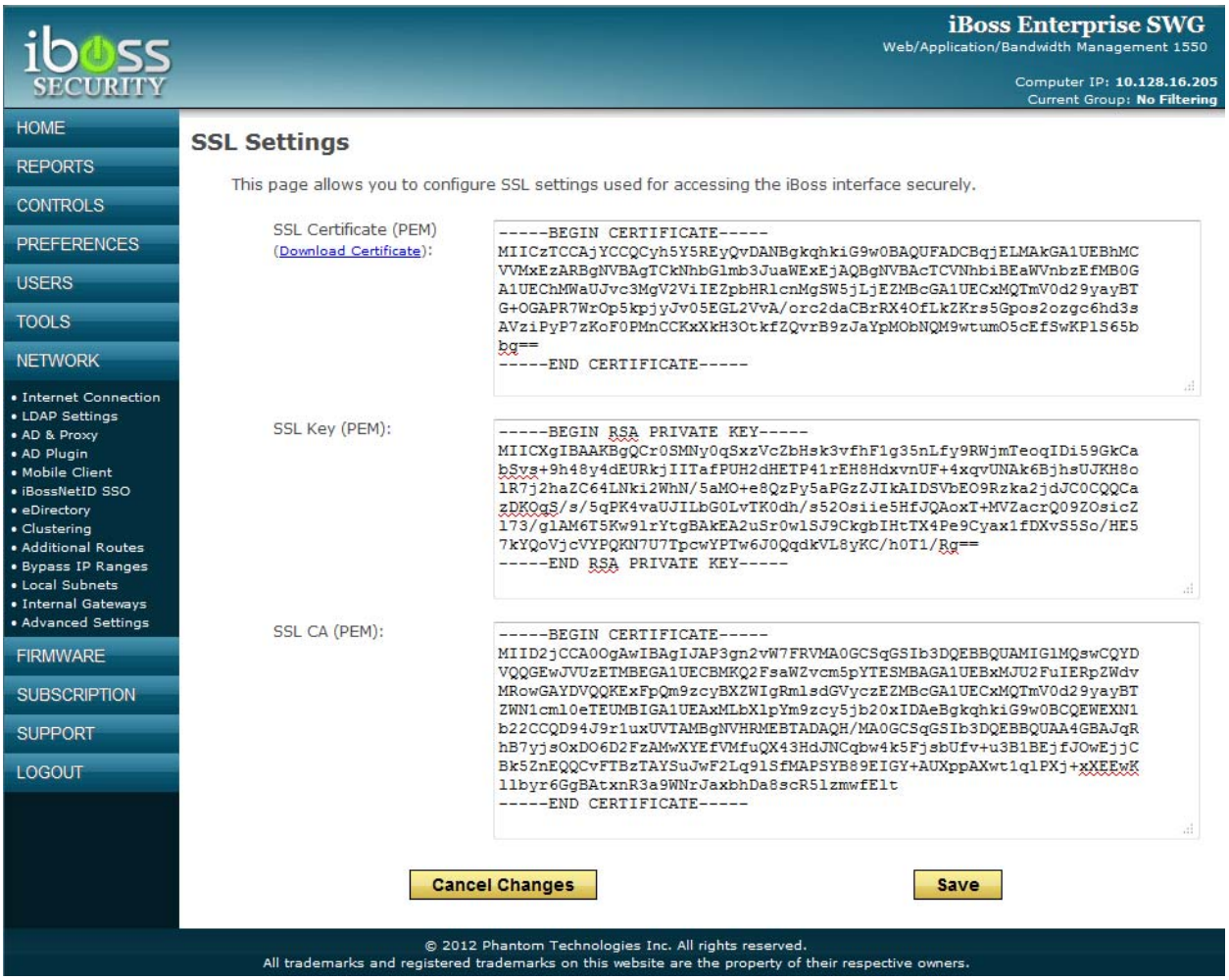

Figure 30 - SSL Settings

This page allows you to configure SSL settings used for accessing the iBoss interface securely. There is an SSL certificate in there by default to use but you can create your own SSL certificate to access the iboss via https.

3.2.3.15 Register Internal Gateways

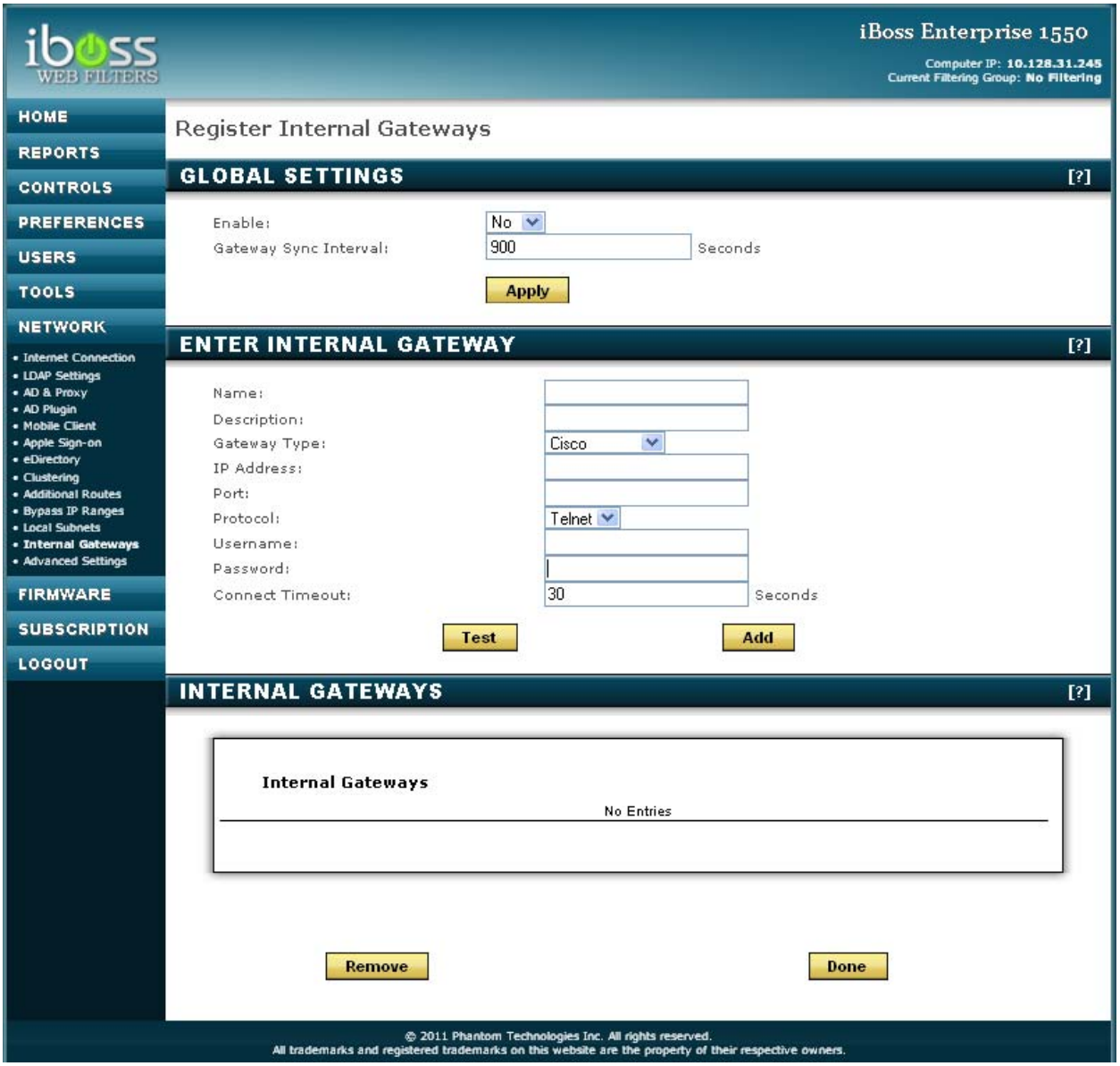

Figure 31 - Register Internal Gateways

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.

3.2.3.16 Edit Advanced Network Settings

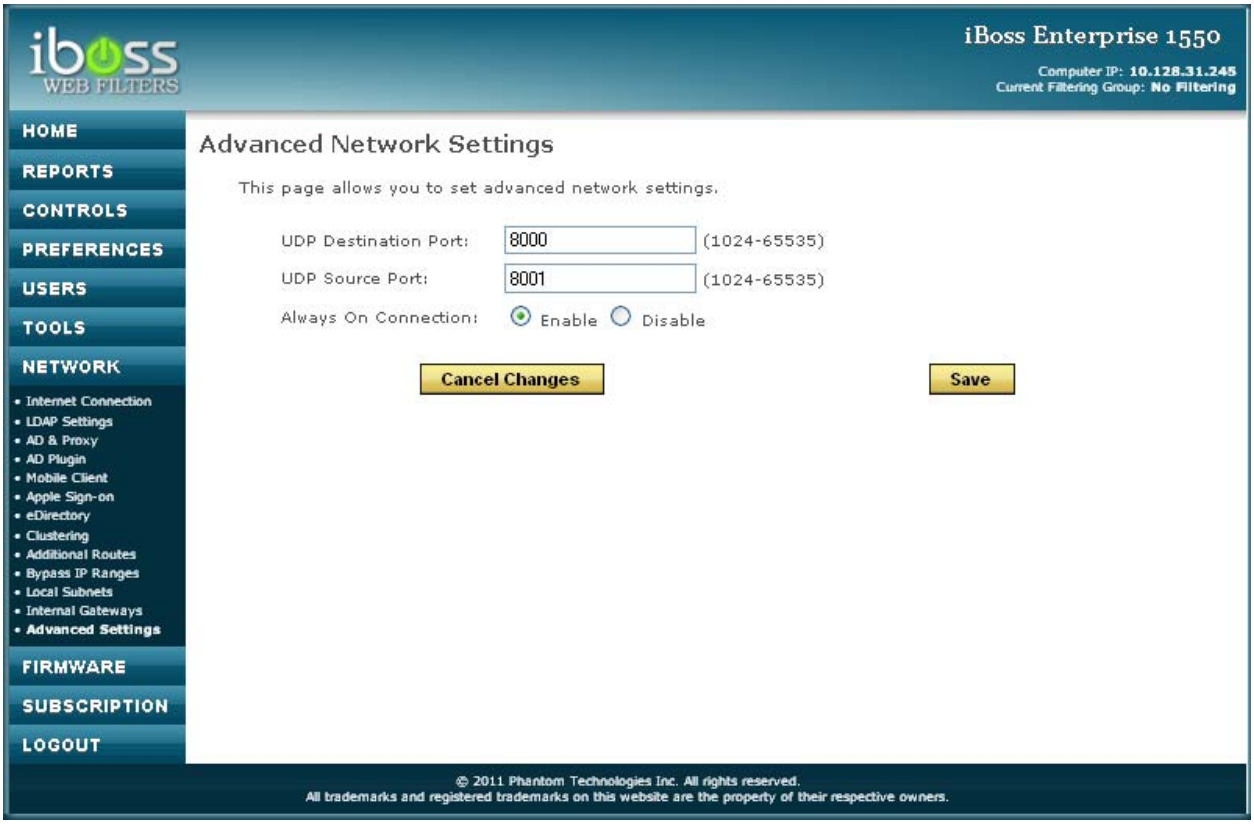

Figure 32 - Edit Advanced Network Settings

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.

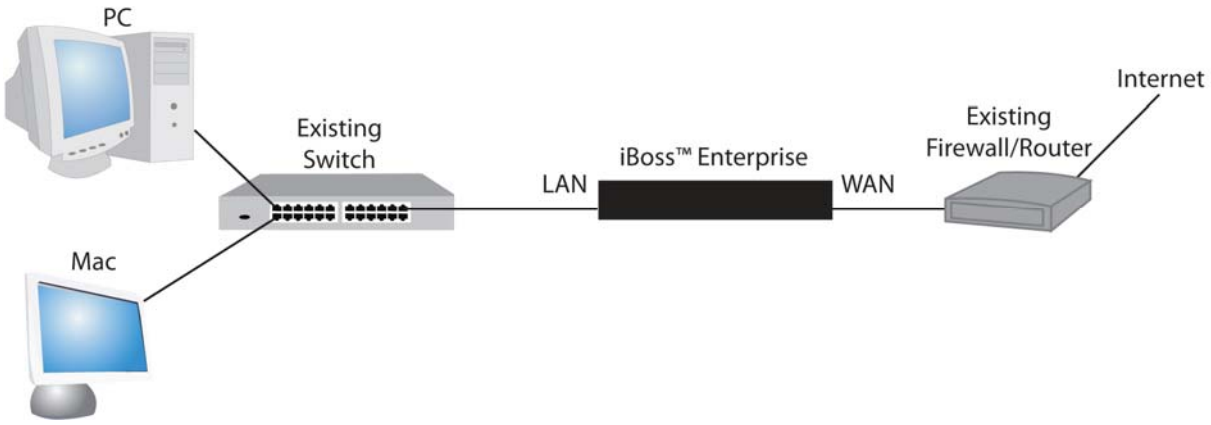

Figure 33 - iBoss Hardware Installation

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

Figure 34 - 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

The "**Configure Internet Controls**" menu lets you choose options for configuring the current iBoss Internet controls.

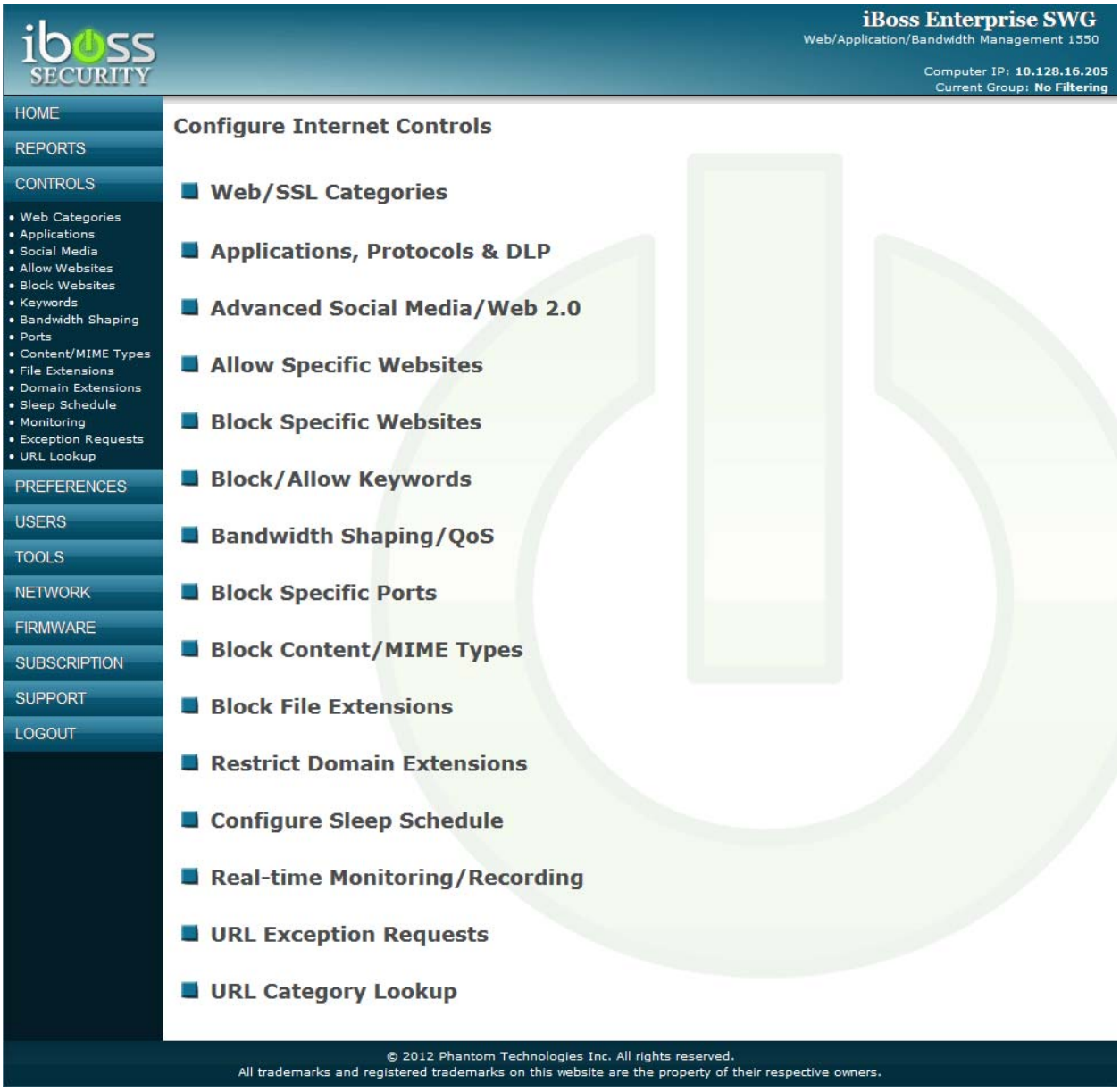

Figure 35 - Configure Internet Controls

Web/SSL Categories - This option allows you to block or allow website content based on categories.

Applications, 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).

Advanced Social Media / Web 2.0. - This option allows you to configure some of the social media sites and other web 2.0 sites like advanced Google and YouTube features. Some other features include Pinterest Controls. In addition, using the Local SSL Inspection Agent, other controls appear that can be used for social media sites such as Facebook, Twitter, and LinkedIn as well as more advanced Google controls.

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

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

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

Bandwidth Shaping/QoS - This option allows you to set bandwidth throttles & reservations on users, groups, domains, or web categories. Additional modules allow you to setup bandwidth pools for parent and child rules.

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

Block Content/MIME Types - This option allows you to block specific content types and MIME types from being downloaded through the web.

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.

URL Exception Requests - If enabled, a link on the block page will allow users to request the page be allowed. The requests are managed from this page.

URL Category Lookup - URLs can be looked up here to determine the assigned categories and if needed, submitted for recategorization.

4.2.1 Web / SSL Categories

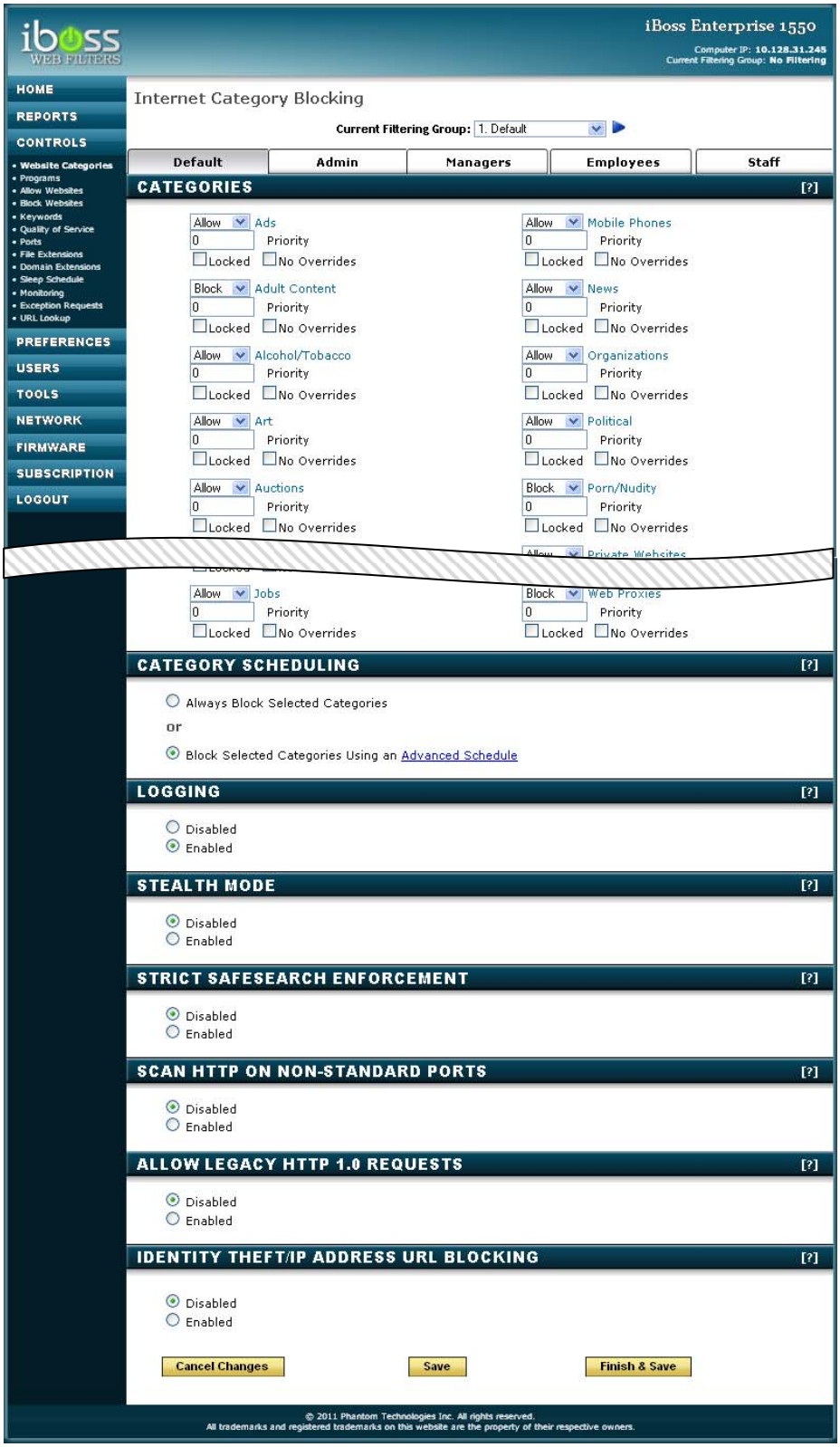

Figure 36 - Block Specific Website Categories

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

Block / Allow / Stealth - Specifies whether the category is blocked or allowed for this filtering group. Designating 'Stealth' will flag as a violation but will not actually block.

Priority - By default 'Block' has priority over 'Allow'. A site belonging to multiple categories will be blocked if ANY of those categories are blocked unless a category with a higher priority is allowed. For example: A site belonging to both 'Education' and 'Gaming' would be blocked if the policy is to block all gaming. If 'Education' priority is bumped to 1 or more then the site is allowed.

Locked - A Delegated Administrator will not be able to alter the category settings of those flagged as 'Locked'.

No Override - A Delegated Administrator will not be able to add URLs to the Allowlist if they belong to a banned category marked as 'No Override'.

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

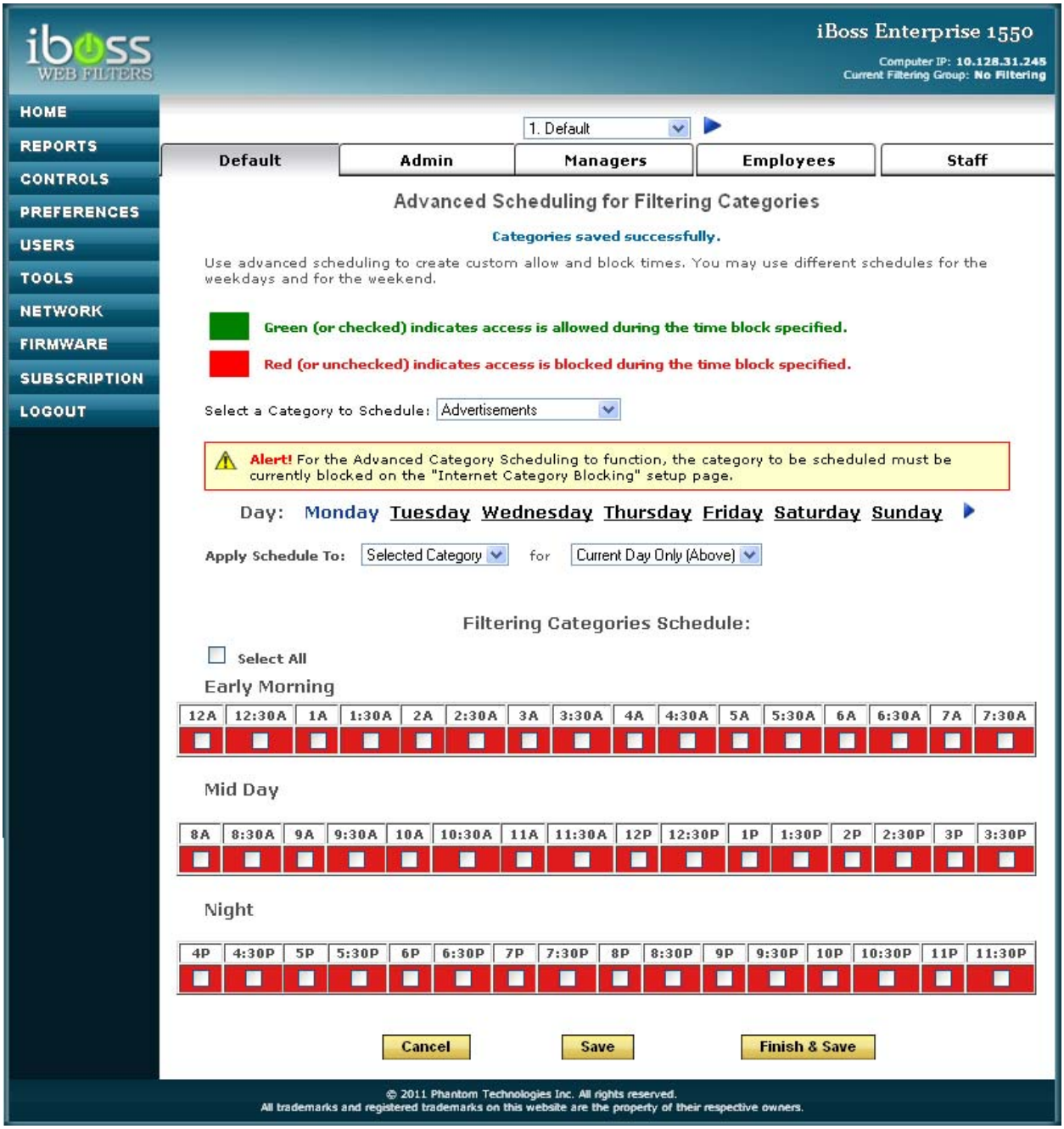

Figure 37 - Advanced Scheduling

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

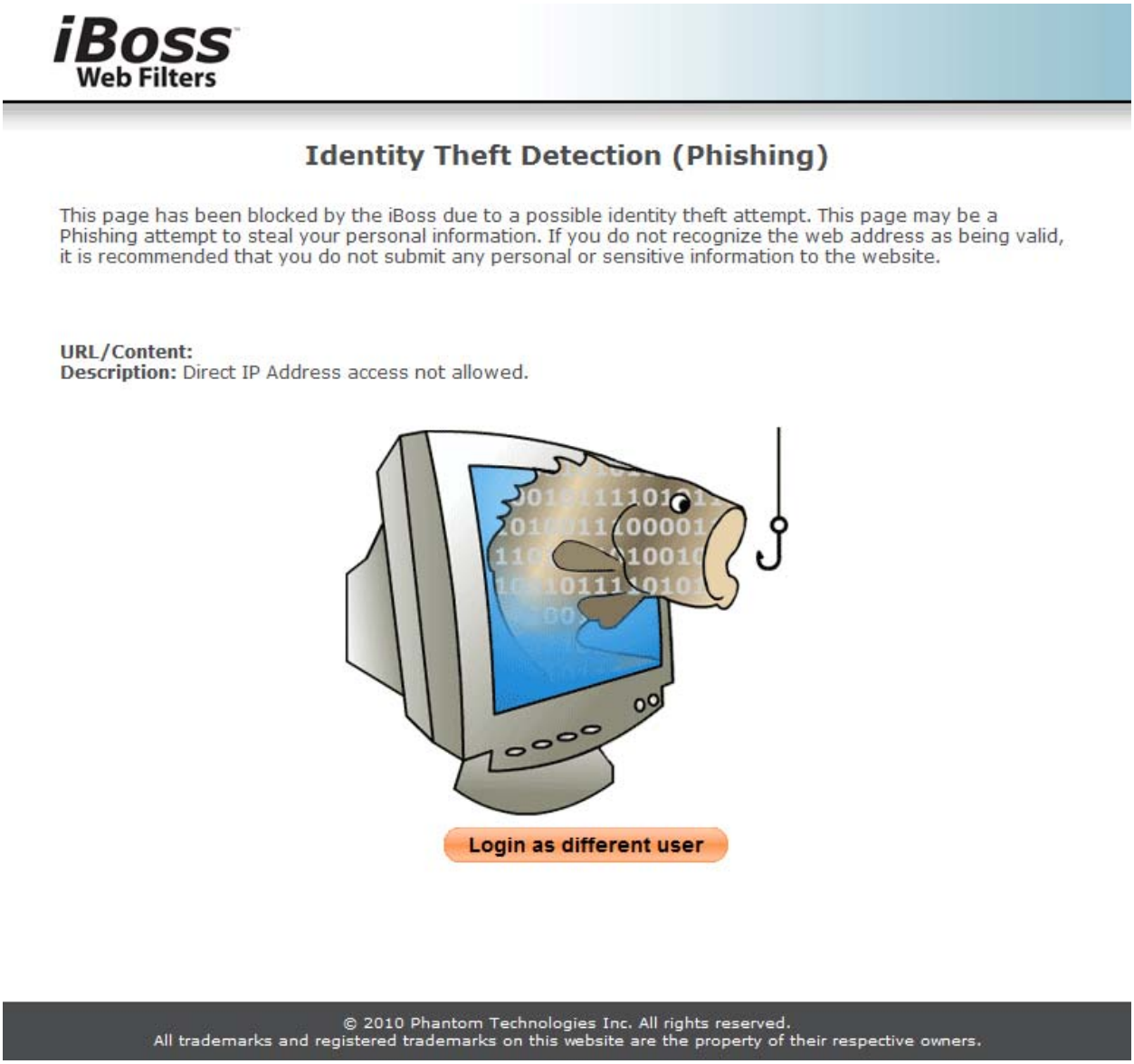

Figure 38 - Identity Theft Detection Page

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 Application Management

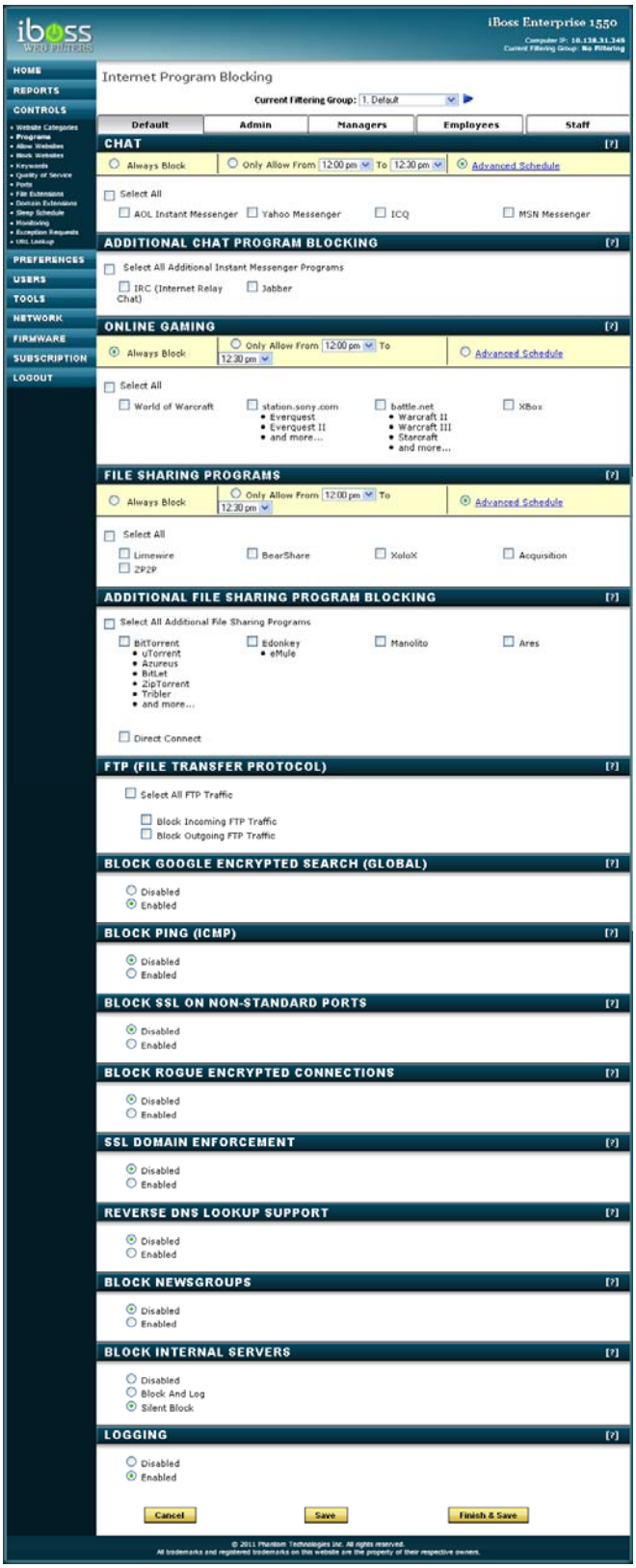

Figure 39 - Block Specific Web Programs

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.

Ultrasurf / Tor / High-Risk Activity Device Lock - This feature allows you to lock the Internet for the user if the activity of Ultrasurf/Tor Proxies is detected. This blocks all Internet access so that when the user opens a web browser, they will be informed that the detection has occurred and that they must disable the program. The Internet will be blocked for the specified time. To enable this feature, check **Enable Ultrasurf/High-Risk activity lock**.

Send Real-time email when activity is detected and computer is locked option will inform the iBoss administrator that the detection has occurred when the event is detected. By default, it will email the Email setup for the User Alerts. The individual filtering group can have a group email contact under Controls --> Monitoring. This will then email the group email contact when the activity lock is detected.

Lock computer for __ minutes when Ultrasurf/high-risk activity is detected allows you to specify a specified time of minutes that the user would be locked for. This will lock the computer from going to the Internet from the time it has detected this event for the amount of minutes that you specify. The suggested setting for this value is 5 minutes, but you can set a lower or higher value.

You can unlock a computer manually by finding the computer under the Users --> Computer tab and click Unlock.

WARNING! These features should NOT be enabled if the iBoss SWG is OUTSIDE of a NAT firewall. If they are enabled and the iBoss is on the WAN side of a NAT firewall, any user on the network that triggers the lock due to high risk programs/activities will lock Internet activity for all other users on the same network. If you are not sure of your network topology, please contact your network administrator or iBoss support.

Block SSH/Secure Shell Access - You may choose to enable blocking for incoming and outgoing SSH Shell Access.

Block RDP/Remote Desktop Access - You may choose to enable blocking for incoming and outgoing Remote Desktop Access.

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.

Dynamic Proxy Blocking (Glype) - You may chose to enable blocking for dynamic Glype themed proxy sites. These are proxy sites setup using the Glype Proxy script which the iBoss can detect and block dynamically regardless of the domain.

Block Hotspot Shield - You may chose to enable blocking for Hot Spot Sheild program. Hot Spot Shield is a program used to proxy to Hot Spot Sheilds servers. Enabling this feature will block the program from being used as a proxy.

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 Advanced Social Media & Web 2.0 Controls

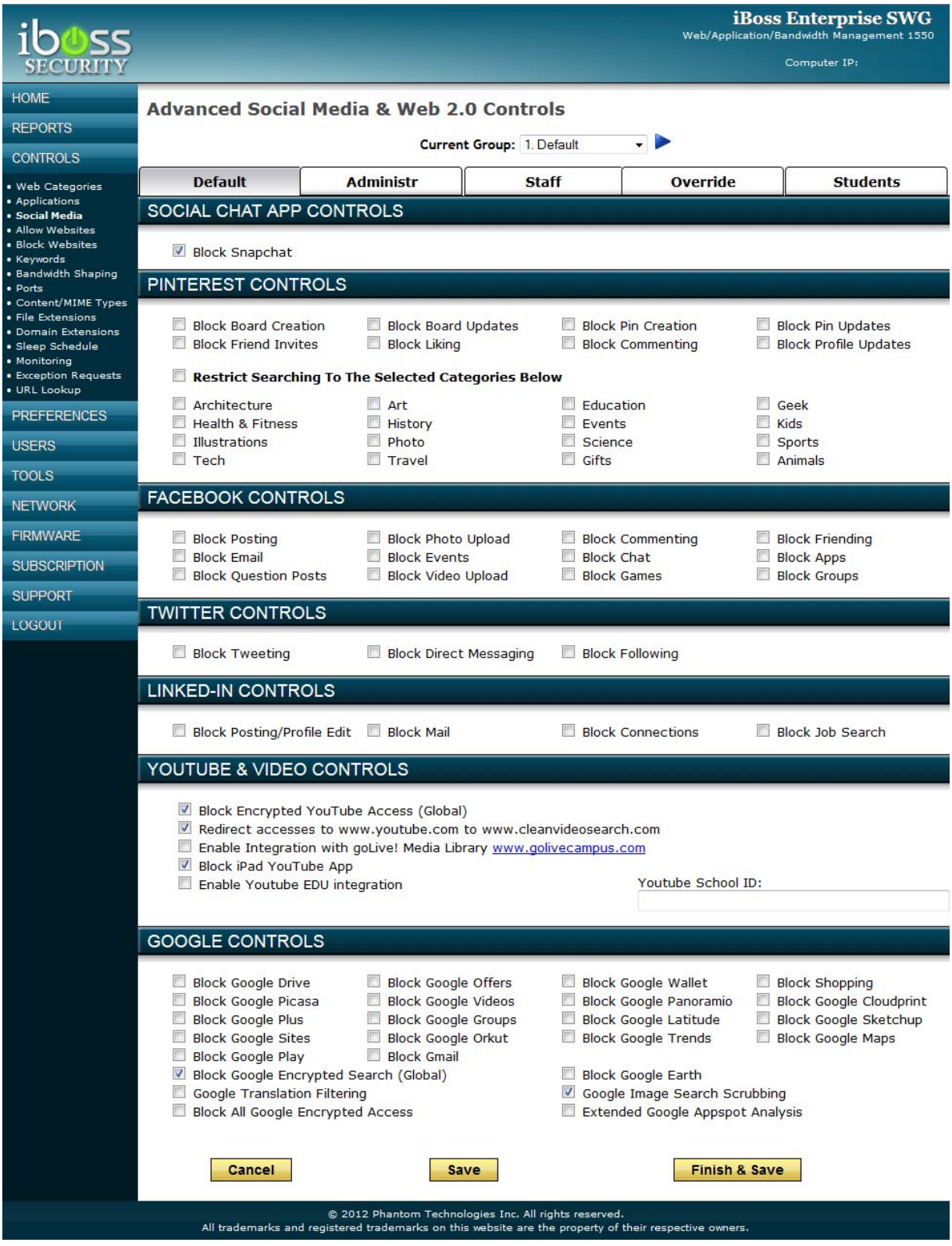

Figure 40 - Advanced Social Media & Web 2.0 Controls

Social Chat App Controls – This feature allows you to configure blocking for the SnapChat application on mobile devices.

Pinterest Controls – These features allow you configure particular sections of Pinterest websites. The following options are available to choose to block:

- Block Board Creation
- Block Board Updates
- Block Pin Creation
- Block Pin Updates
- Block Friend Invites
- Block Liking
- Block Commenting
- Block Profile Updates
- Restrict Searching to selected categories
  - Architecture
  - Art
  - Education
  - Geek
  - Health & Fitness
  - History
  - Events
  - Kids
  - Illustrations
  - Photo
  - Science
  - Sports
  - Tech
  - Travel Gifts
  - Animals

Facebook Controls (SSL Inspection Agent needed) – These features allow you to block specific features and sections for facebook.com. The following options are available to choose to block:

- Block Posting
- Block Photo Upload
- Block Commenting
- Block Friending
- Block Email
- Block Events
- Block Chat
- Block Apps
- Block Question Posts
- Block Video Upload
- Block Games
- Block Groups

Twitter Controls (SSL Inspection Agent needed) - These features allow you to block specific features and sections for twitter.com. The following options are available to choose to block:

- Block Tweeting
- Block Direct Messaging
- Block Following

Linked-in Controls (SSL Inspection Agent needed) - These features allow you to block specific features and sections for linkedin.com. The following options are available to choose to block:

- Block Posting/Profile Edit
- Block Mail
- Block Connections
- Block Job Search

YouTube & Video Controls – These features allow you to controls certain features of YouTube as well as handle requests to YouTube differently for specific filtering groups.

- **Block Encrypted YouTube Access (Global)** – This option will block encrypted https access to YouTube. This is a global feature since the method used to do this is DNS based. If your DNS server has direct access to the Internet without going to through the iBoss or you have the iBoss in tap mode, you would want to setup a DNS Conditional Forwarder for youtube.com to point to the iBoss. You can get these instructions from iBoss support.
- **Redirect accesses to www.youtube.com to www.cleanvideosearch.com** – This redirects any request to youtube.com to cleanvideosearch.com. Cleanvideosearch.com is a site that provides searching for videos from YouTube.com while enforcing Strict Safety Mode and stripping out all comments and related videos. You can set this option on a per group basis.
- **Enable Integration with goLive! Media Library www.golivecampus.com** – This feature allows you to block YouTube.com but allow videos to be played from golivecampus.com. Golivecampus.com is a site that allows you to granularly choose which videos are allowed to be viewed with channels that can have videos linked on them.
- **Block iPad YouTube App** – This option allows you to block the YouTube App on mobile devices.
- **Enable Youtube EDU integration** – This feature integrates with YouTube for Schools. This allows you to enter your **Youtube School ID** and this will be appended to each request to YouTube allowing only educational videos from YouTube to be allowed to play.

Google Controls (Some features need the SSL Inspection Agent) – These features allow you to controls specific sections of Google.

- **Block Google Encrypted Search** – This feature turns https searches on Google to and http search to be able to log and block keywords. This is DNS based.
- **Block Google Earth**
- **Google Translation Filtering –** This feature blocks violation sites from being translated on Google Translation.
- **Google Image Search Scrubbing –** This feature strips out images on Google Image Search that come from violation sites that are block by the categories.
- **Block All Google Encrypted Access -** This feature blocks all encrypted Google services.

- **Extended Google Appspot Analysis –** This feature allows you to give access to appspot.com but it will support adding subdomains to the blocklist to block based on DNS for other hosted sites on AppSpot.

Other features that are available when enabling the SSL inspection Agent are:

- Block Google Drive
- Block Google Offers
- Block Google Wallet
- Block Shopping
- Block Google Picasa
- Block Google Videos
- Block Google Panoramio
- Block Google Cloudprint
- Block Google Plus
- Block Google Groups
- Block Google Latitude
- Block Google Sketchup
- Block Google Sites
- Block Google Okrut
- Block Google Trends
- Block Google Maps
- Block Google Play
- Block Gmail

4.2.4 Allow Specific Websites

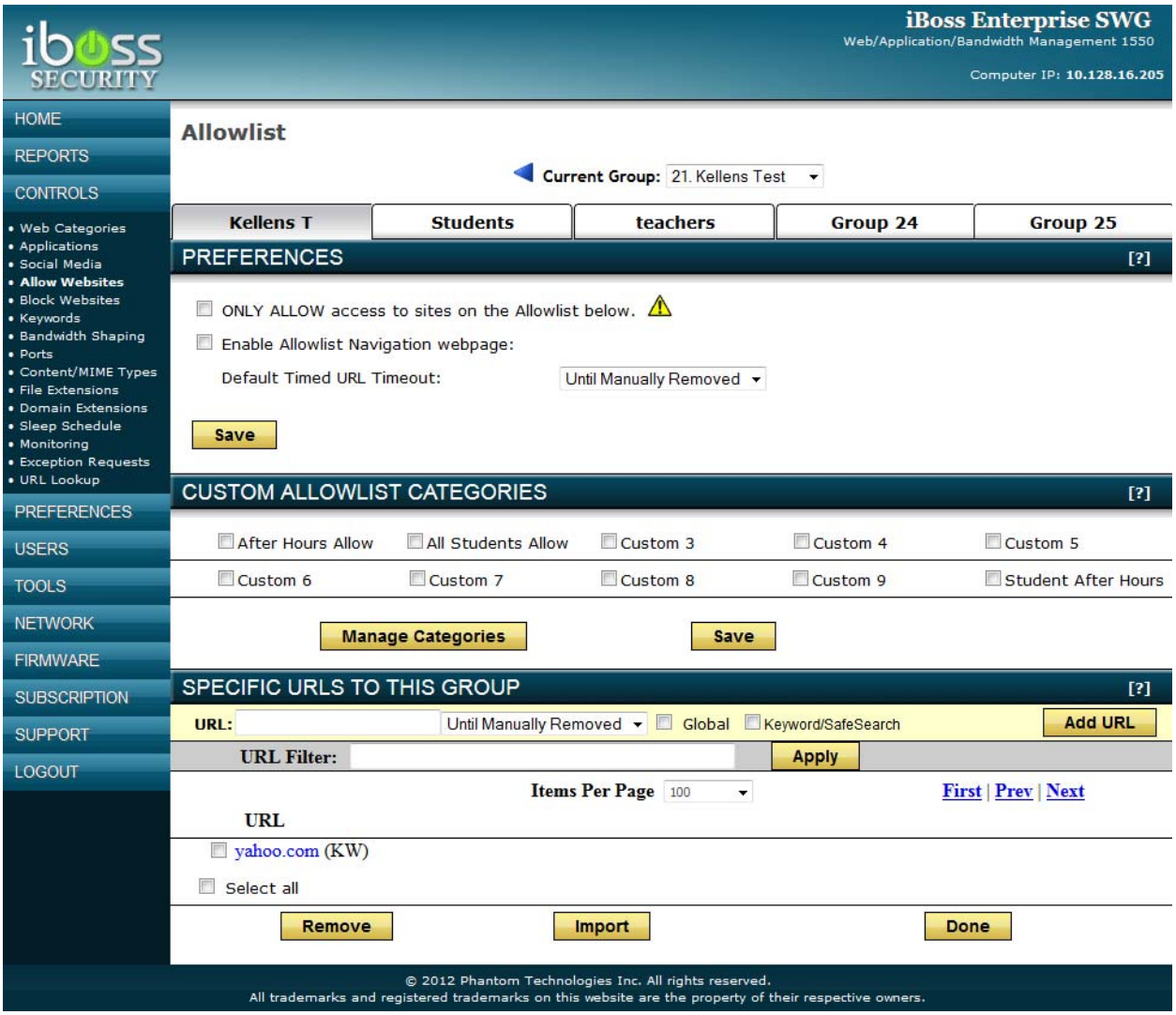

Figure 41 - Allow Specific Websites

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.

Allow ONLY access to sites on the Allowlist – Checking this option will only allow sites in list.
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.

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. 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.

Default Timed URL Timeout – This is the default setting for when adding sites on this list. By default, sites added to this list will remain until removed. There are options to choose a time limit as a default for removing it after the specified time.

Once you have changed any of these settings, click the "**Save**" 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.

Enter URL (ex: domain.com) – field to enter the domain or URL to allow.
URL Timeout – choose a time to have the URL removed after a specified time.
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. Select "**Apply Keyword/Safe Search**" if you would still like to have keyword and safe search enforcement applied to the domain being bypassed.

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

URL Filter – This feature allows you to search through the list. You can enter part of the domain like google to see any URLs that are in this list with that word in it. You can click Apply to view entries in this list. To clear the filter, delete the entry in this field and click Apply.

Sorting – You can click on the URL word to sort the list alphabetically.

Removing – You can remove a URL by selecting the checkbox next to the URL and click the Remove button at the bottom.

4.2.4.1 Custom Allowlist Categories

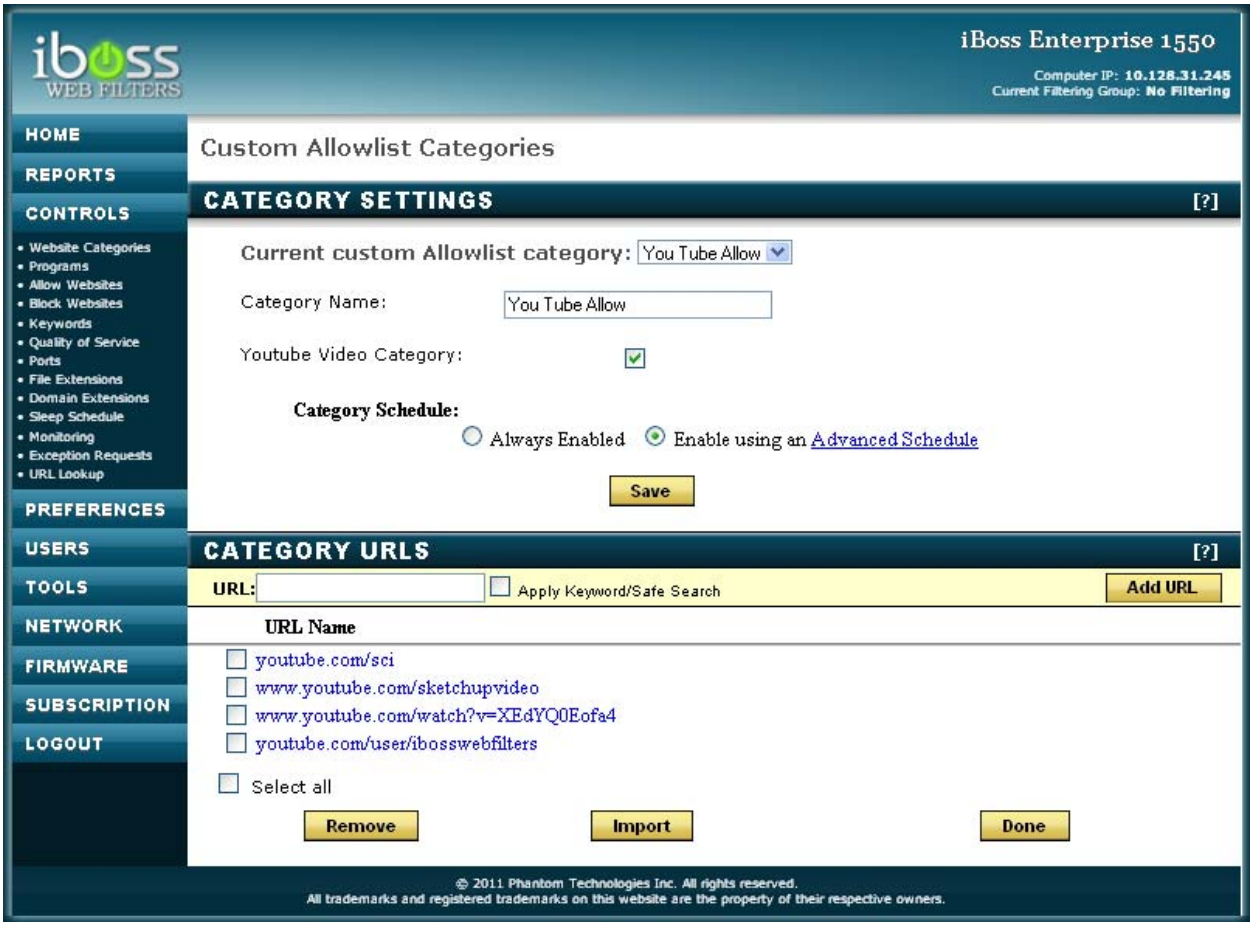

Figure 42 - Custom Allowlist Categories

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.

4.2.4.2 Allowlist Import

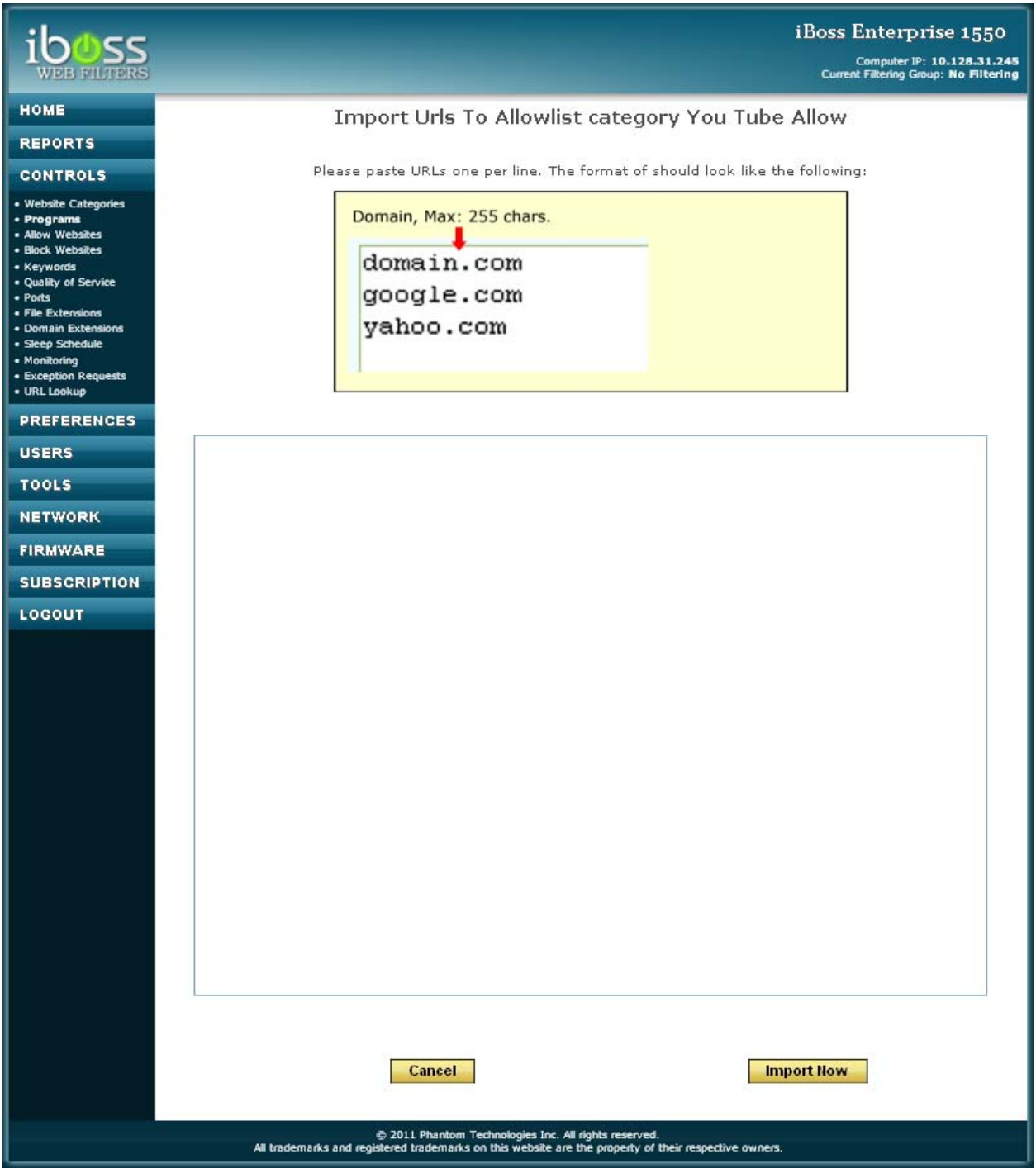

Figure 43 - Allowlist Import

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.

4.2.5 Block Specific Websites

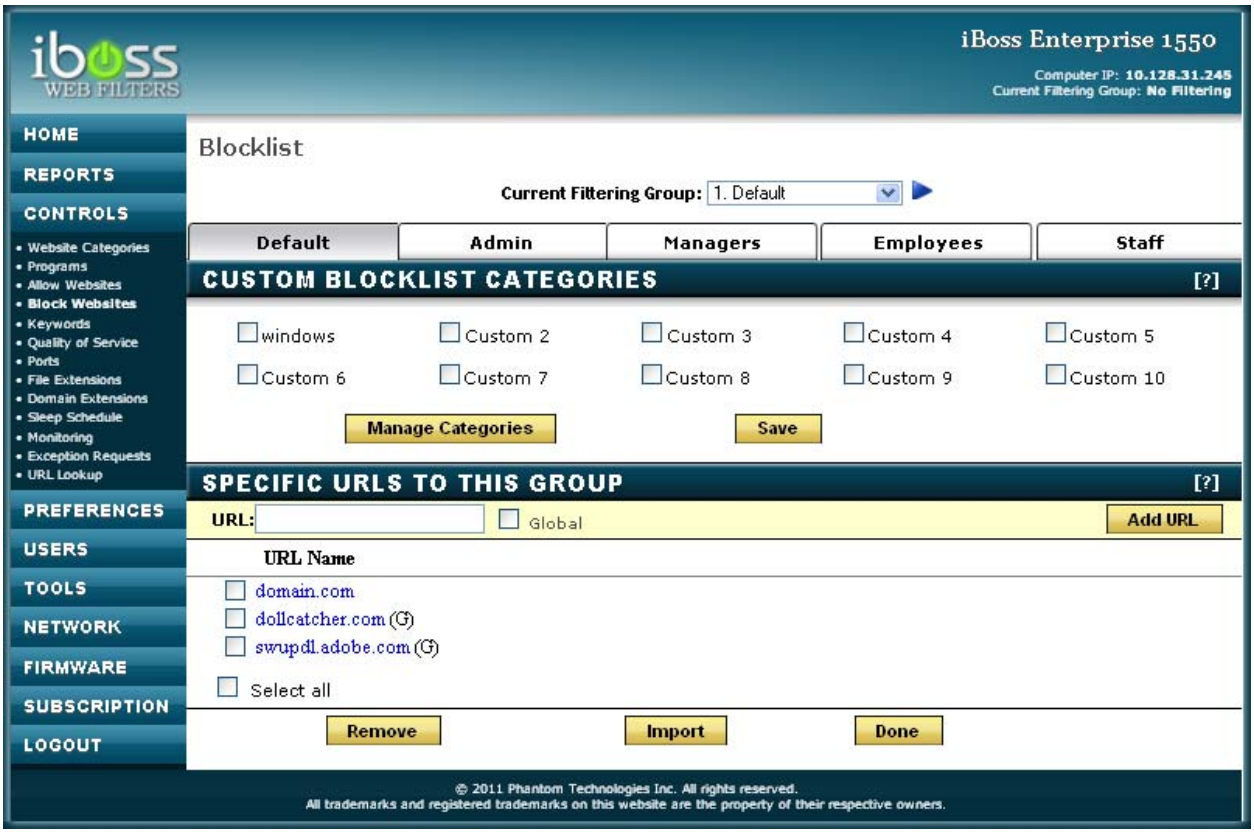

Figure 44 - Block Specific Websites

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.

4.2.5.1 Custom Blocklist Categories

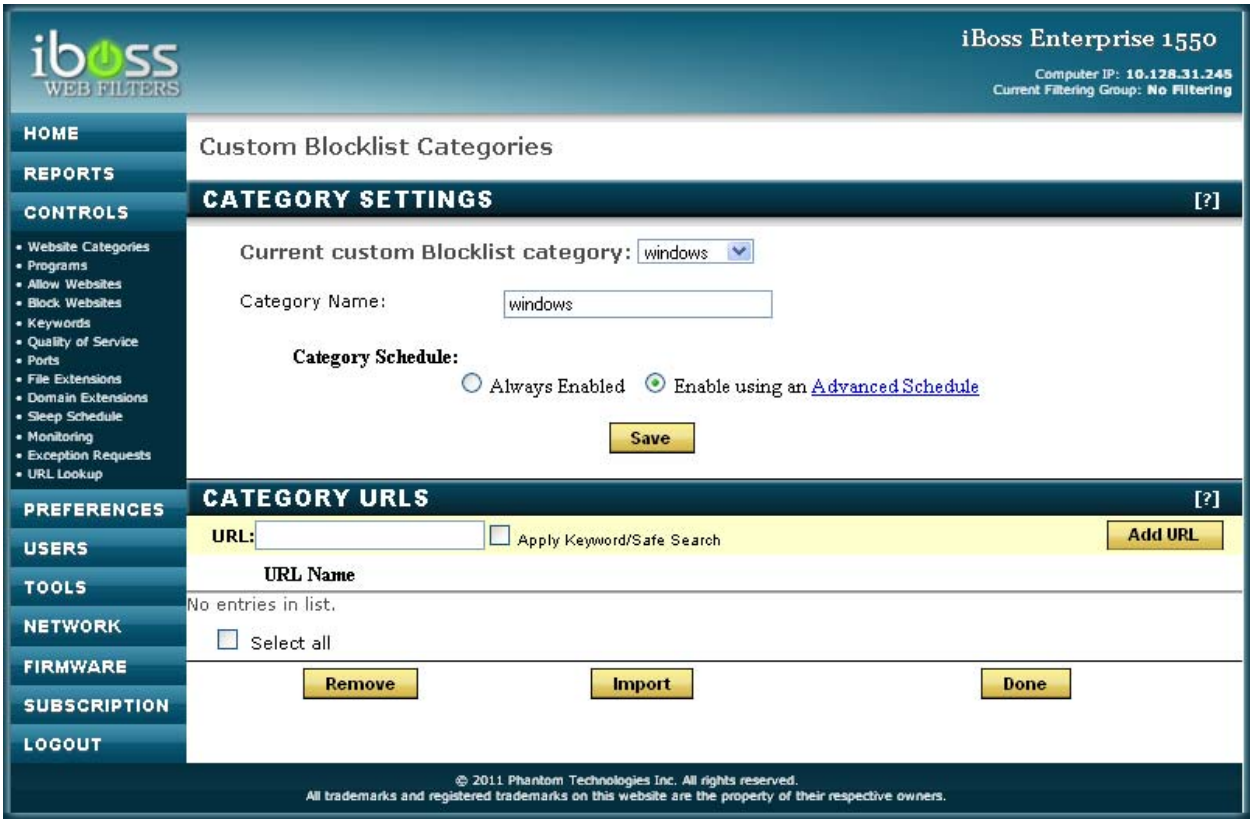

Figure 45 - Custom Blocklist Categories

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.

4.2.5.2 Blocklist Import

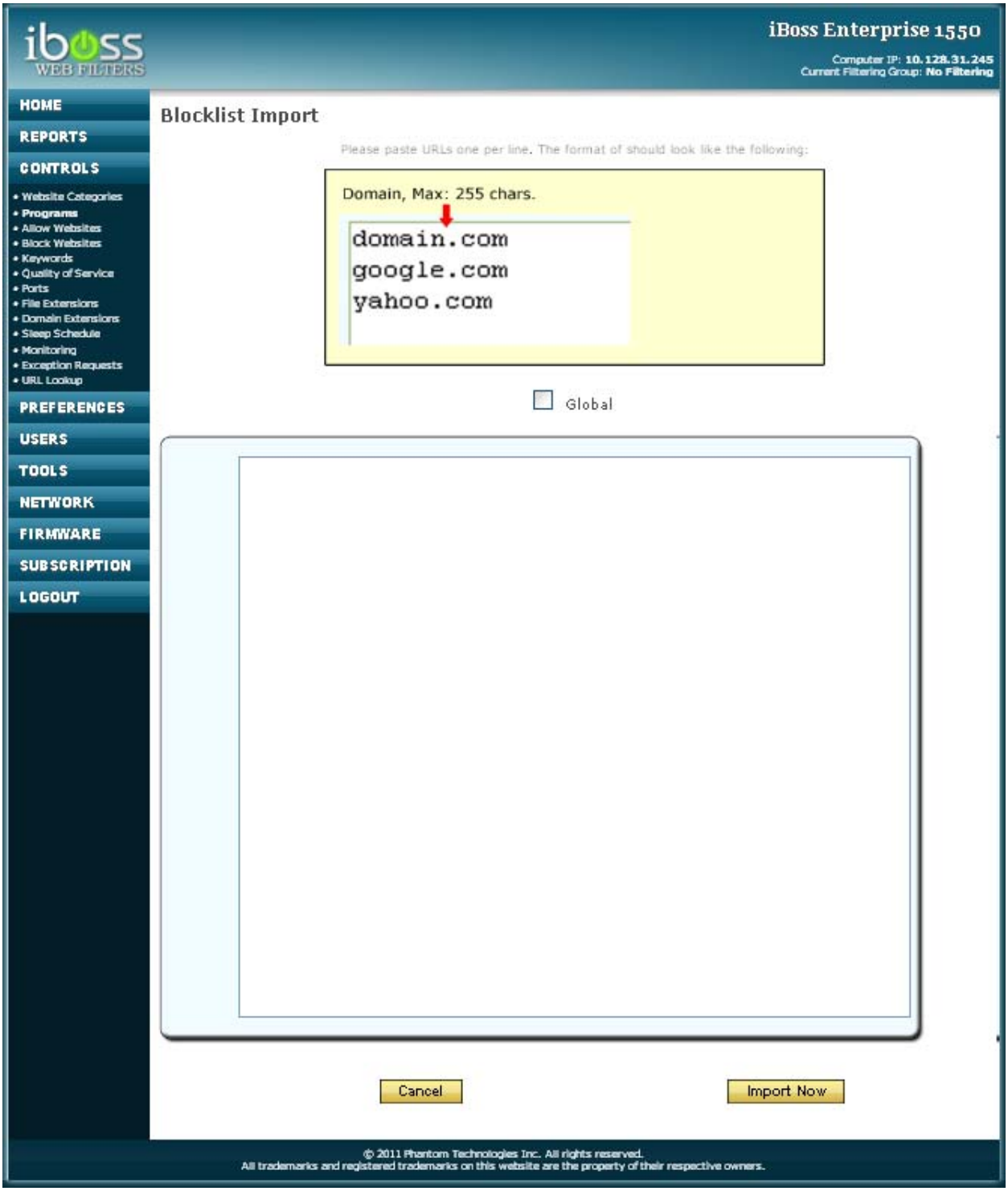

Figure 46 - Blocklist Import

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.

4.2.6 Block Specific Keywords

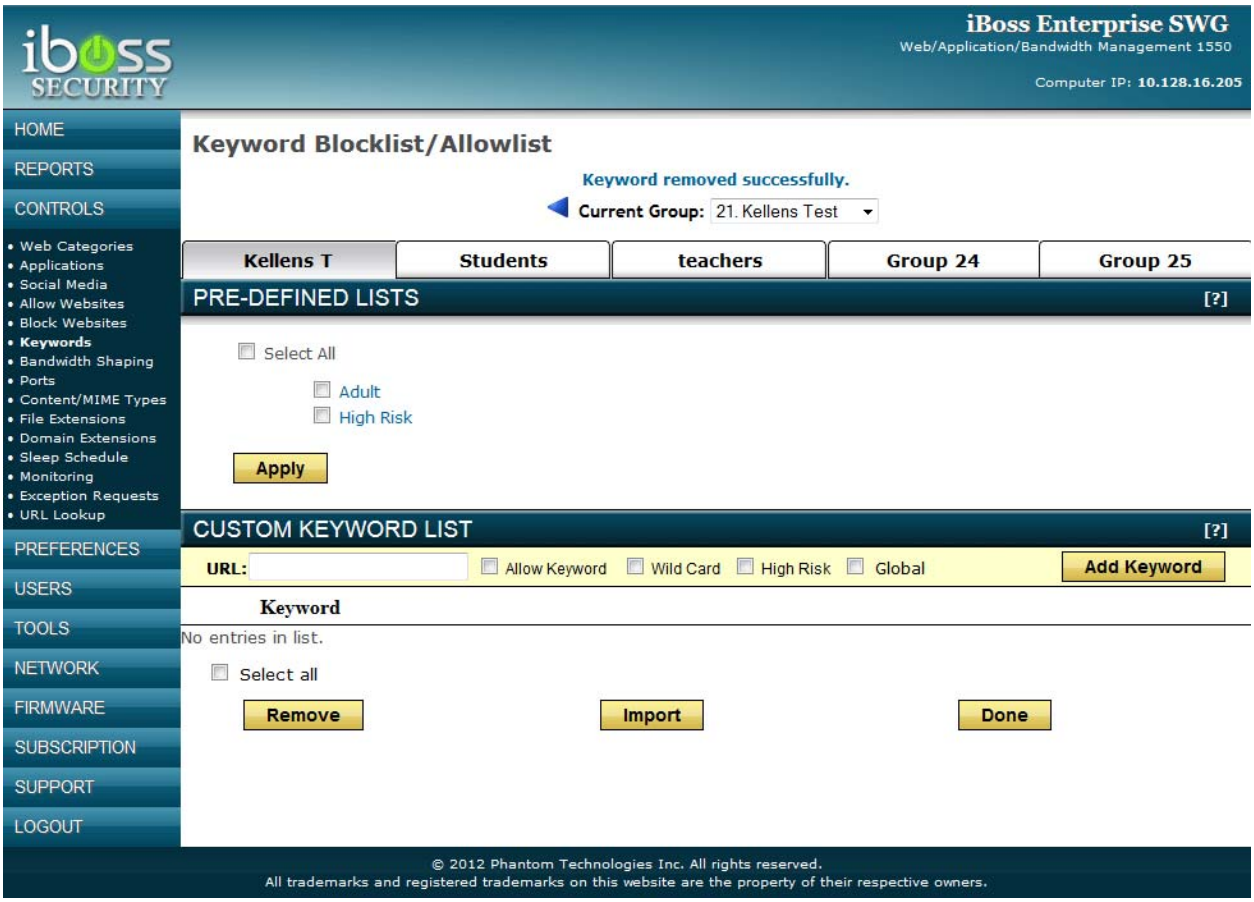

Figure 47 - Block Specific Keywords

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.

4.2.6.1 Keyword Import

Figure 48 - 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.

4.2.7 Bandwidth Shaping/QoS

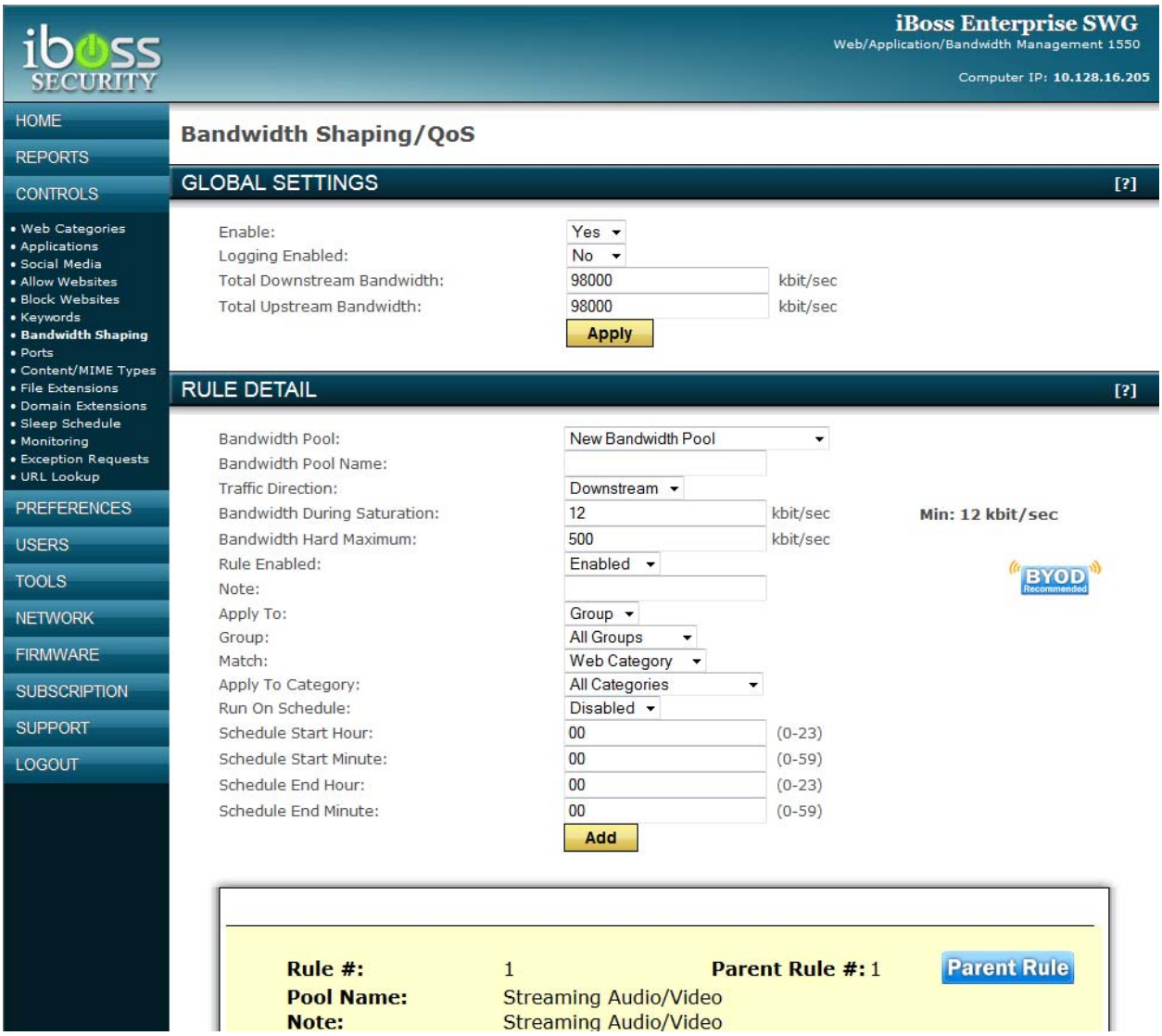

Figure 49 - Bandwidth Throttling / QoS

There is a separate, more comprehensive manual for the Bandwidth Throttling/QoS feature. Please request this from iBoss Support for the iboss Enhanced QoS & Bandwidth Shaping Datasheet.

4.2.8 Block Specific Ports

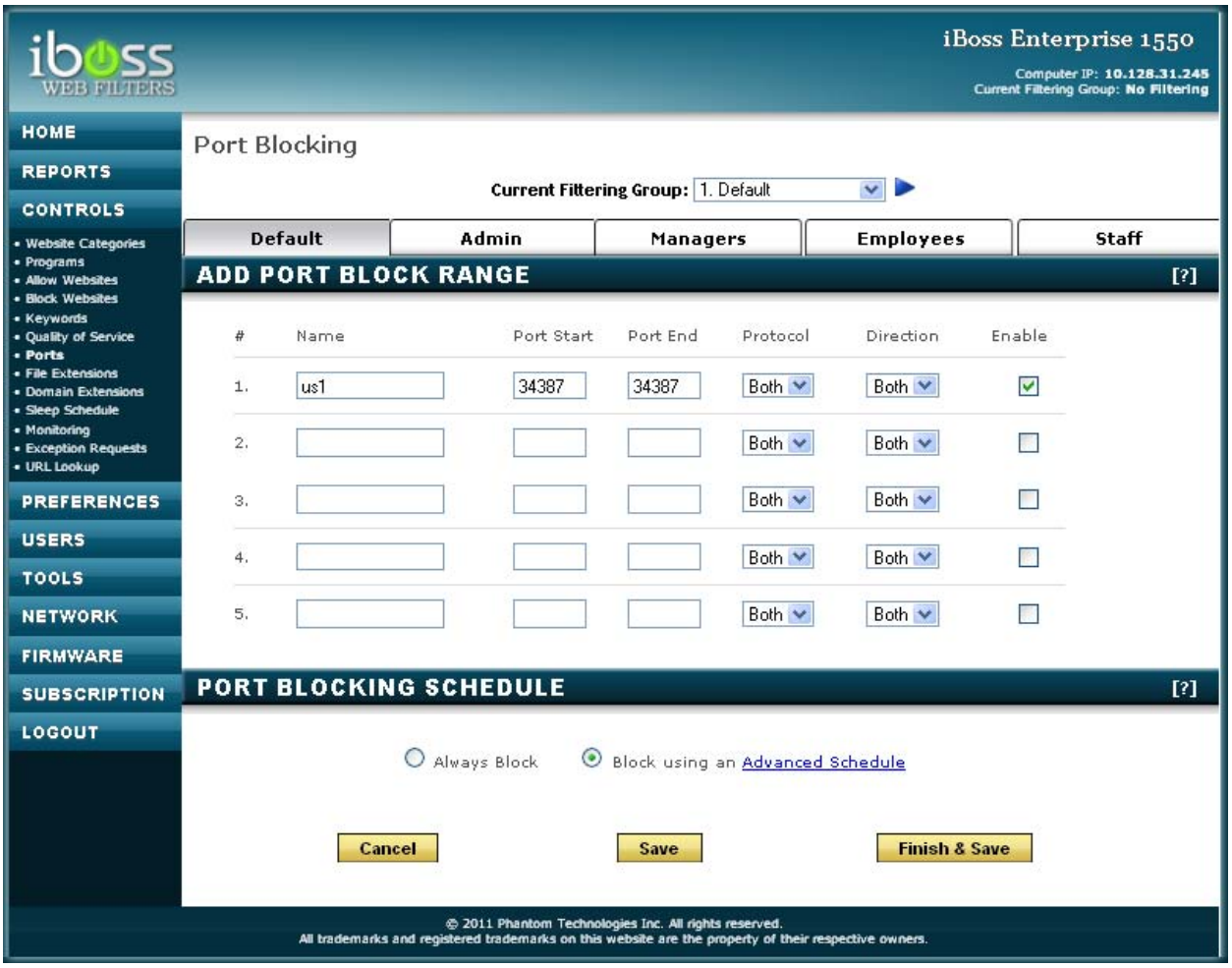

Figure 50 - Port Blocking

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.

4.2.9 Block Content/MIME Types

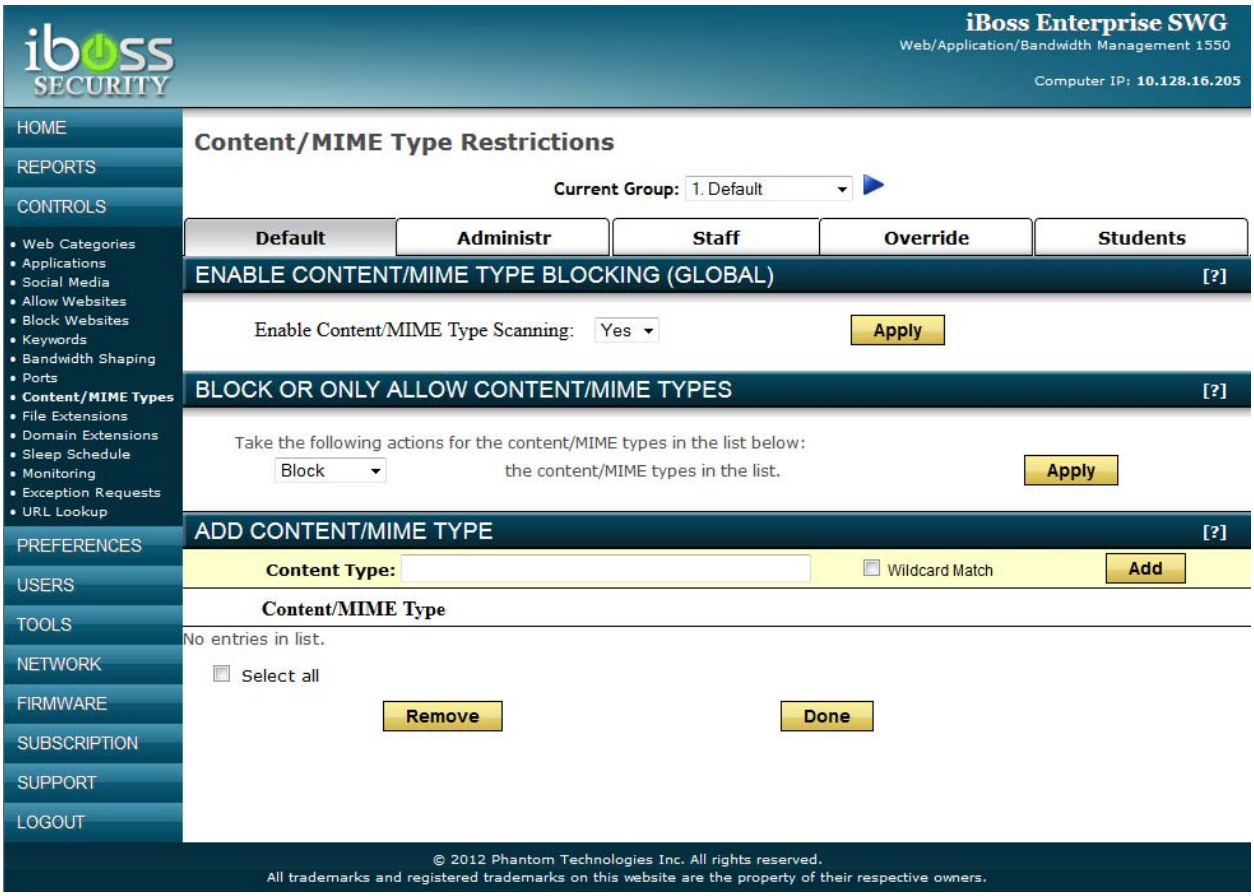

Figure 51 - Block Content/MIME Types

This page allows you to block web content based on Content Type or MIME type. You can enter a content type like audio/mp3 to block this type of content. There are MIME type lists online that can be used for reference. You can enter wildcard matches for different file types instead of using the file extensions. For example, you can type in **audio** and check the box for Wildcard Match to block all audio type files.

You also have the choice to **Block** the entries in the list or **Only Allow** the entries in the list.

After you enter a content/MIME type, click **Add** to add it to the list. To remove it, select it with the checkbox next to the entry and click the **Remove** button at the bottom.

4.2.10 Block Specific File Extensions

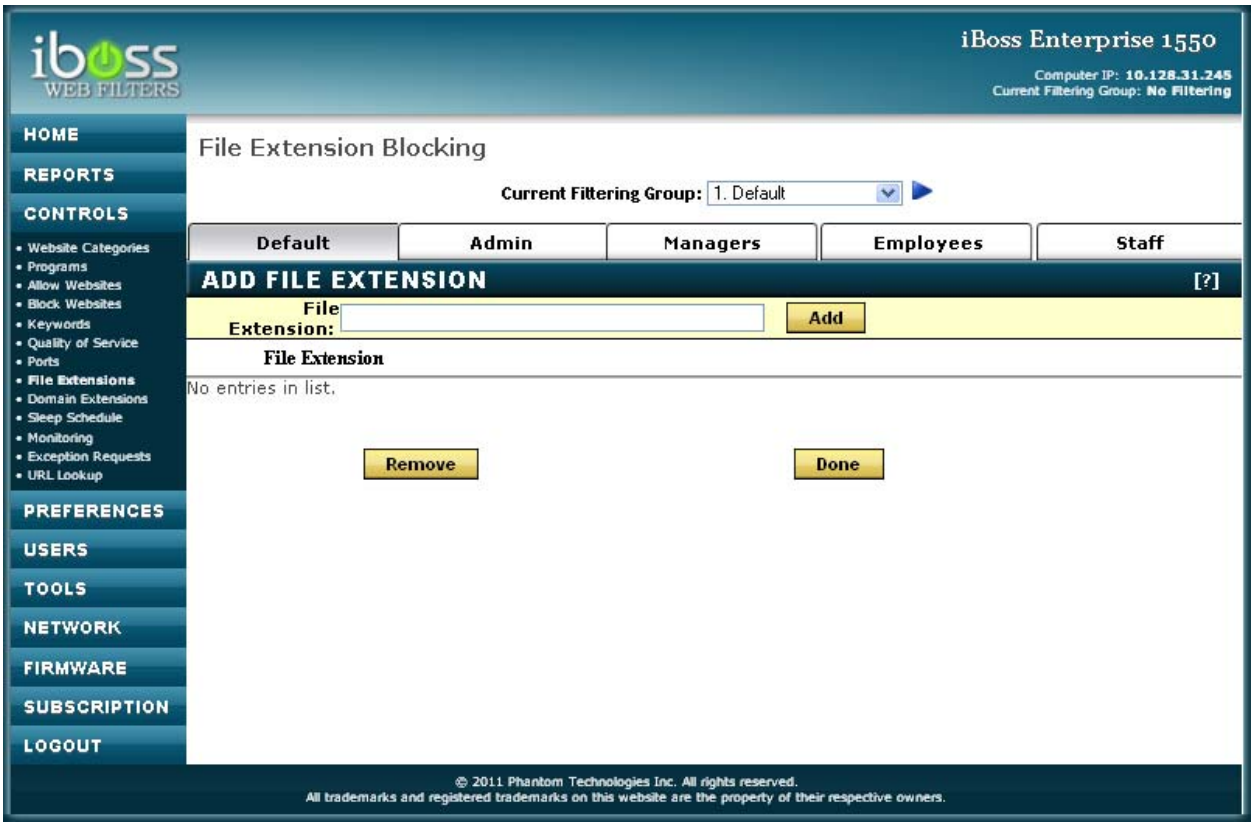

Figure 52 - Block Specific File Extensions

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.

4.2.11 Restrict Domain Extensions

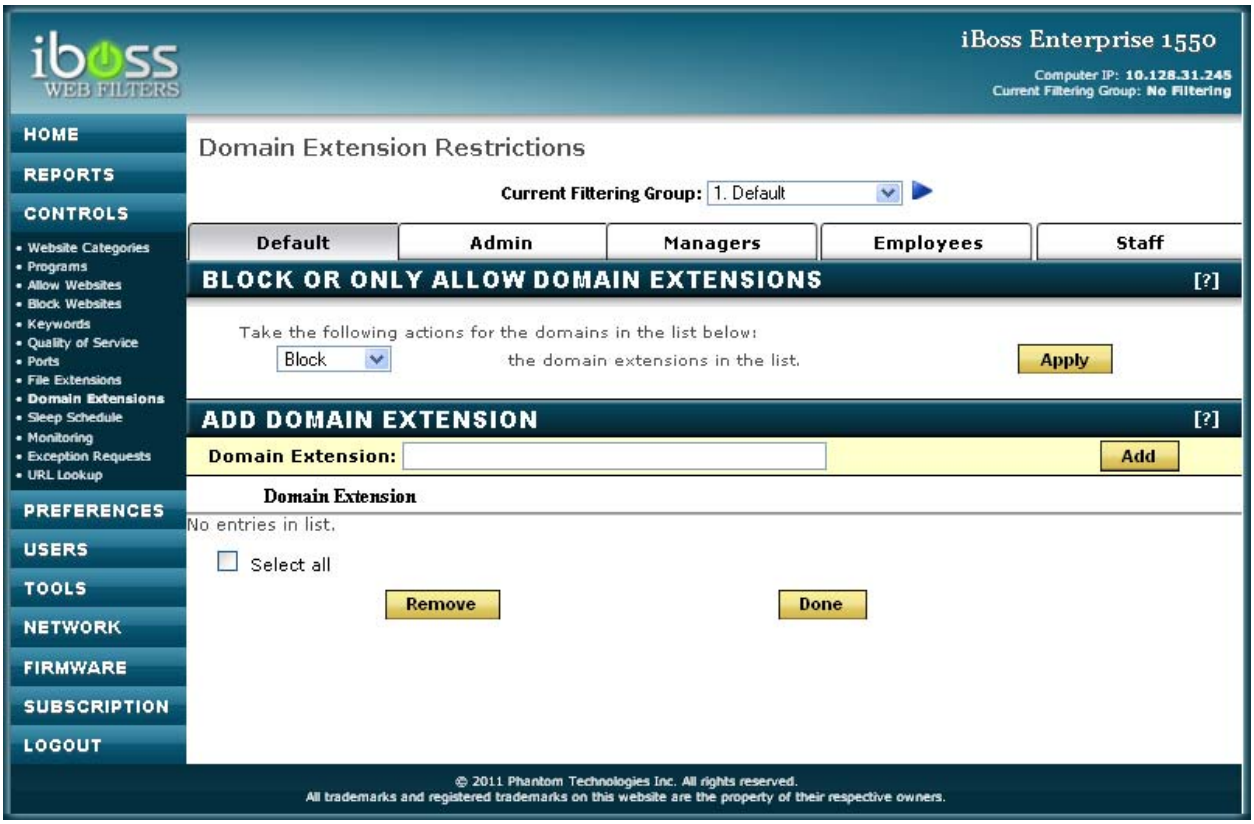

Figure 53 - Restrict Domain Extensions

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.

4.2.12 Configure Sleep Schedule

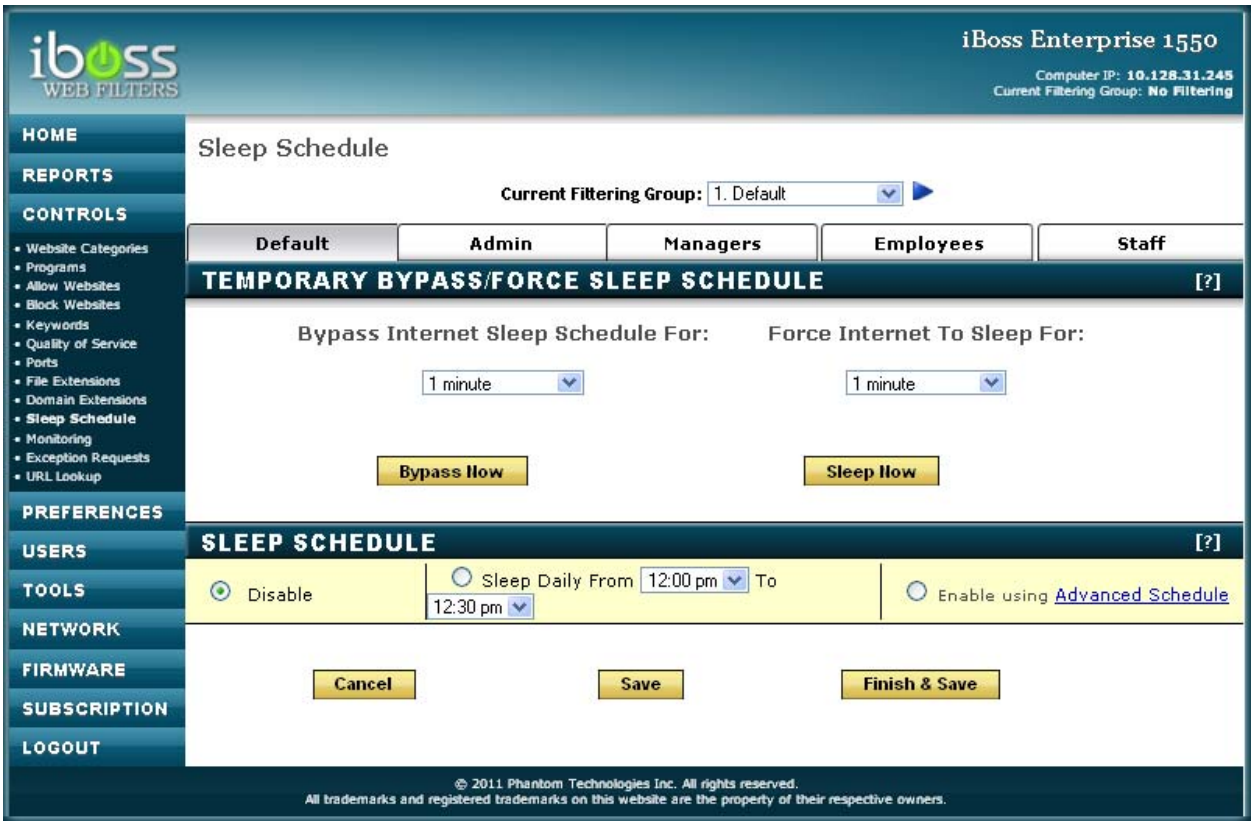

Figure 54 - Configure Sleep Schedule

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.

4.2.12.1 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.

Figure 55 - Internet Sleep Mode Page

4.2.13 Real-Time Monitoring/Recording

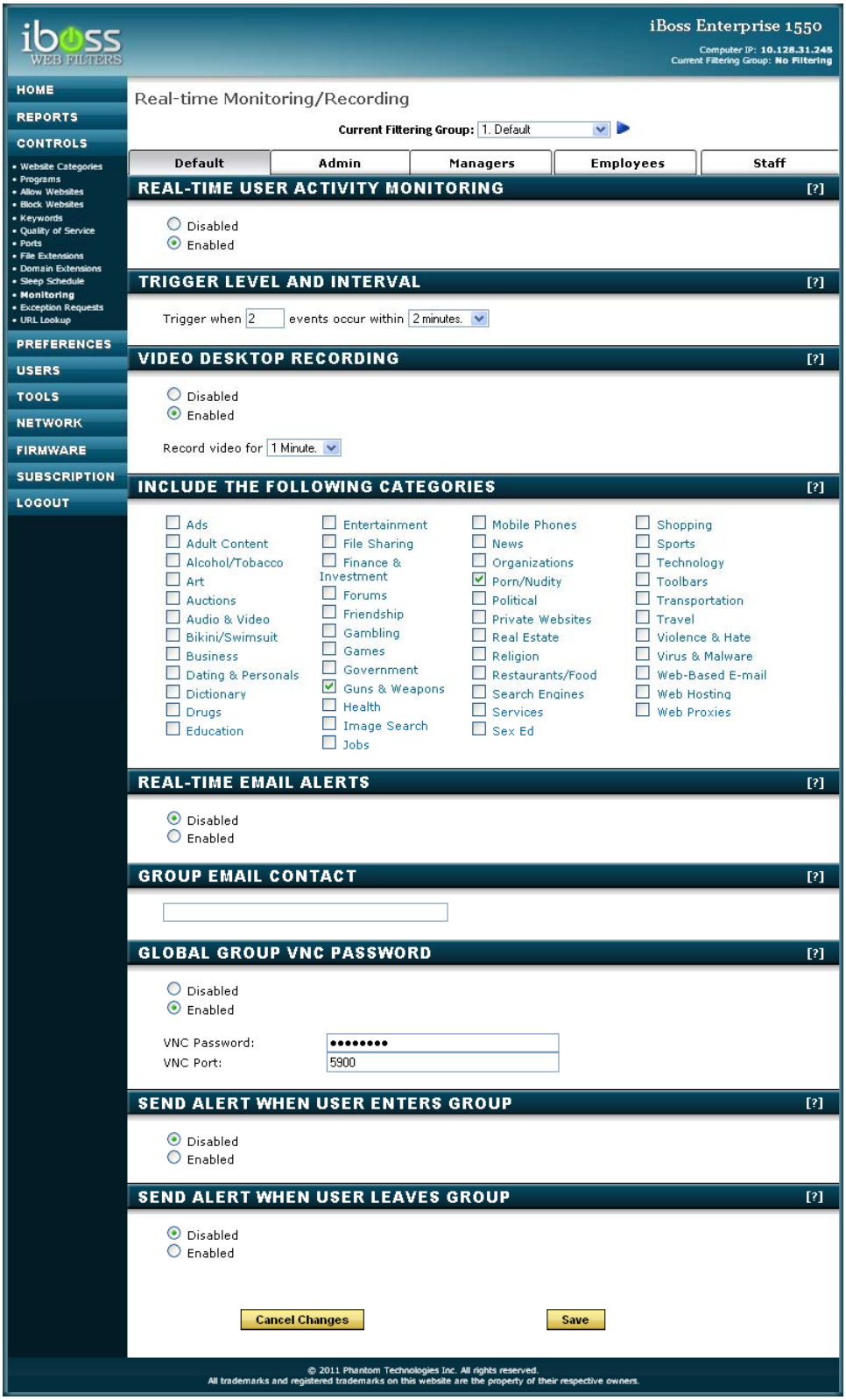

Figure 56 - Real-time Monitoring/Recording

Note: The VNC recording feature is not included by default and may not be available on all models. 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.

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.

4.2.14 URL Exception Requests

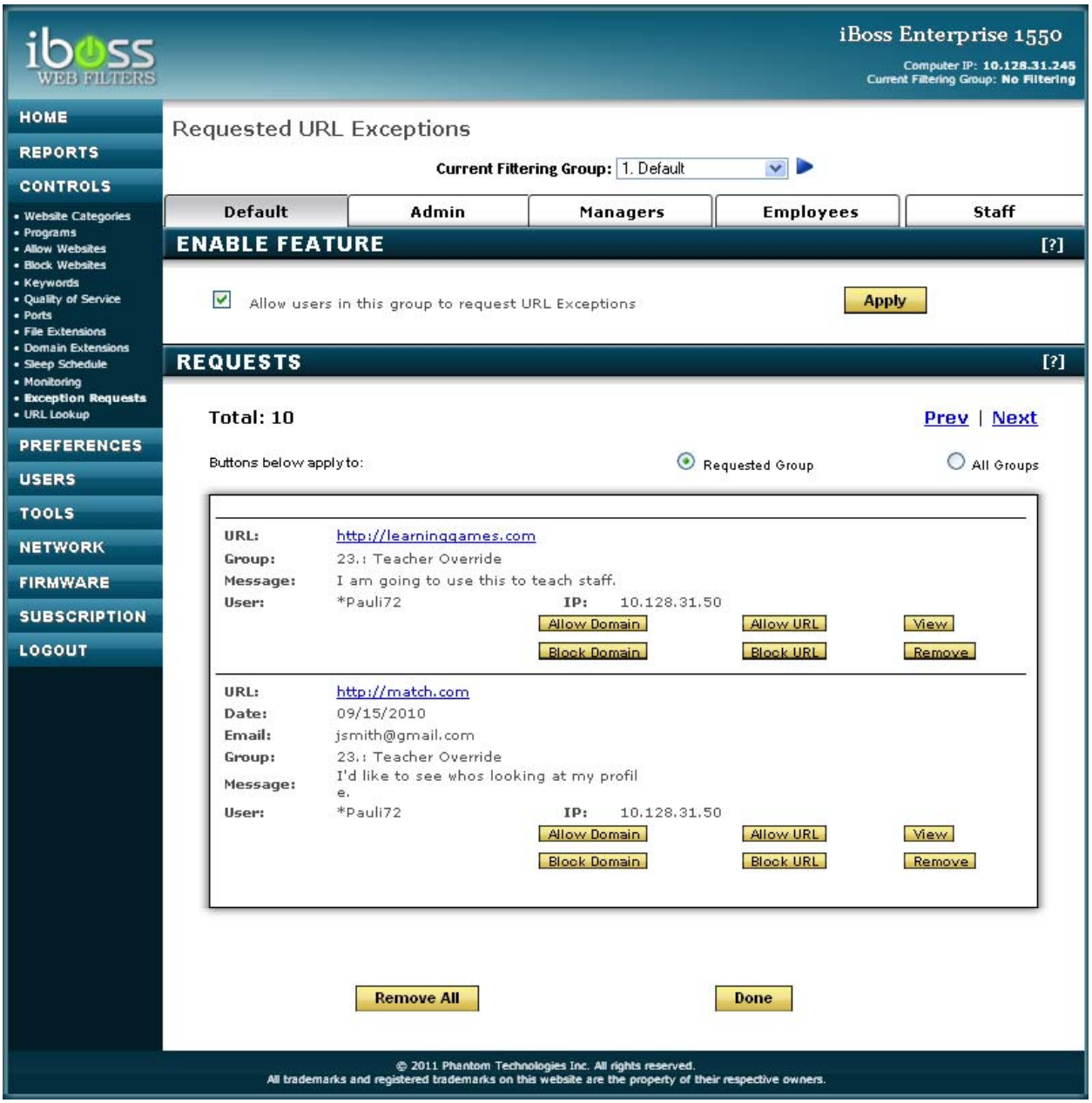

Figure 57 - URL Exception Requests

If enabled this feature adds a section to the block page allowing the user to submit a request to allow the page. Notes and the user's email may be included. The request will be delivered to the email address(es) specified at Controls→Monitoring in the section 'Group Email Contact' if one is specified for the group; otherwise it will be delivered to the email specified in the settings of the reporter.

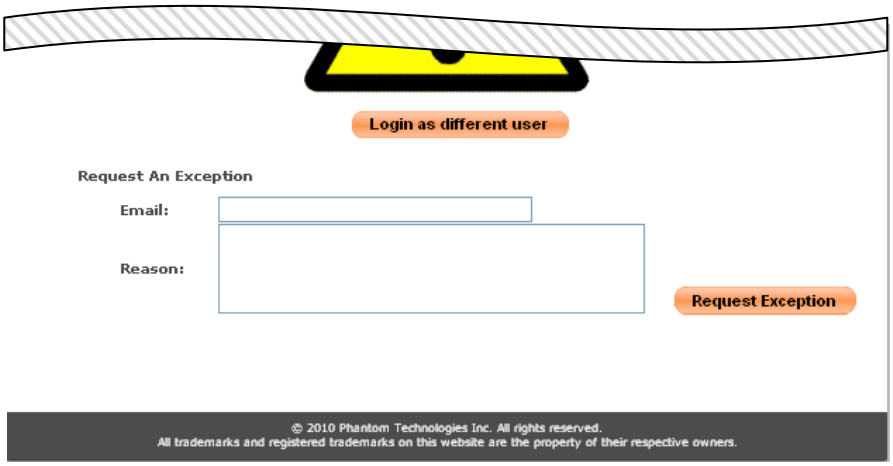

Figure 58 - URL Exception Request - Block Page

4.2.15 URL Category Lookup

This provides a utility to query a URL to see how it has been categorized. Once a URL has been entered and the 'Lookup' button clicked there will be a message at the top of the screen indicating the database status of the URL. The section below will indicate which categories it is assigned.

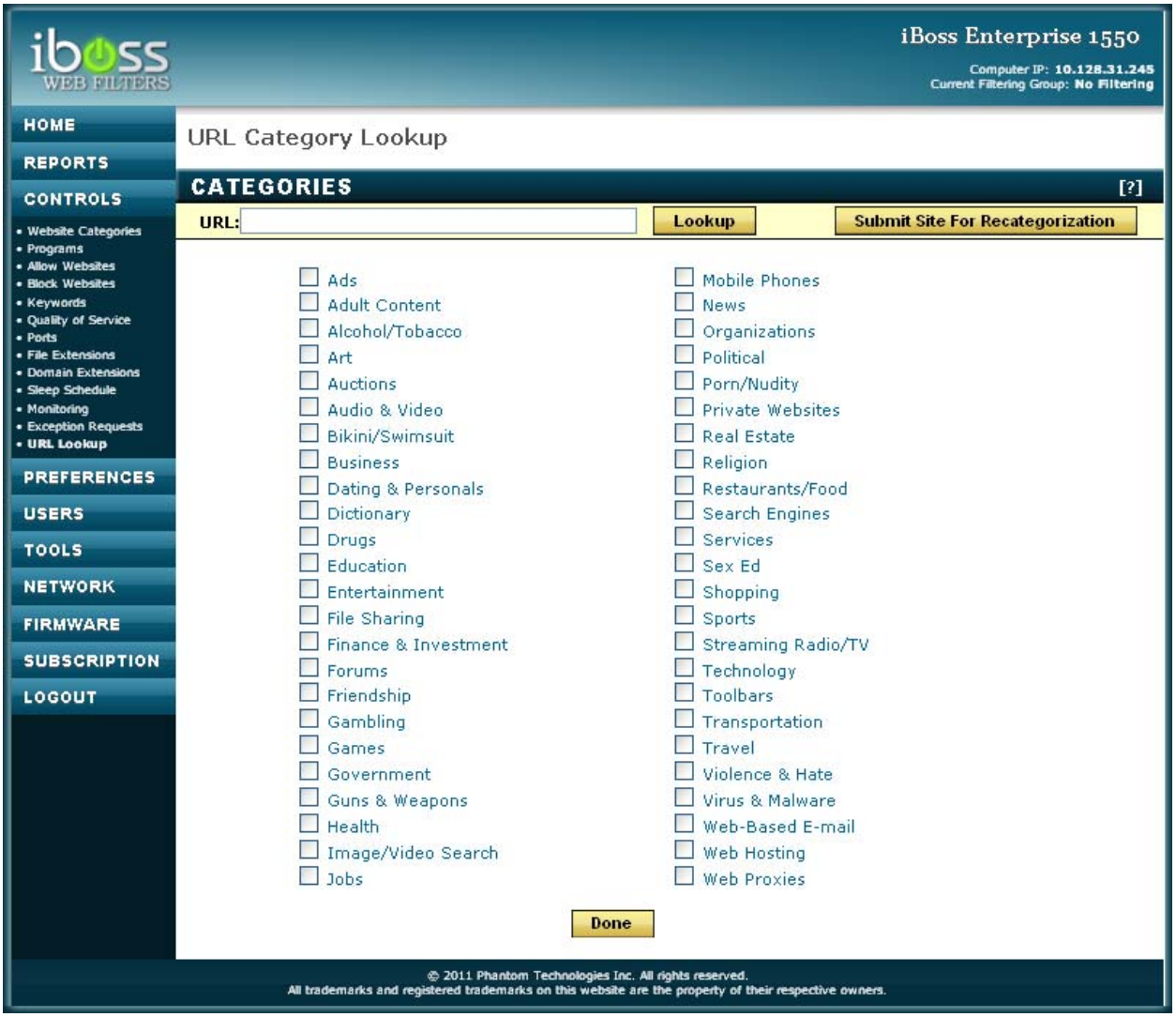

Figure 59 – URL Category Lookup

4.3 Edit My Preferences

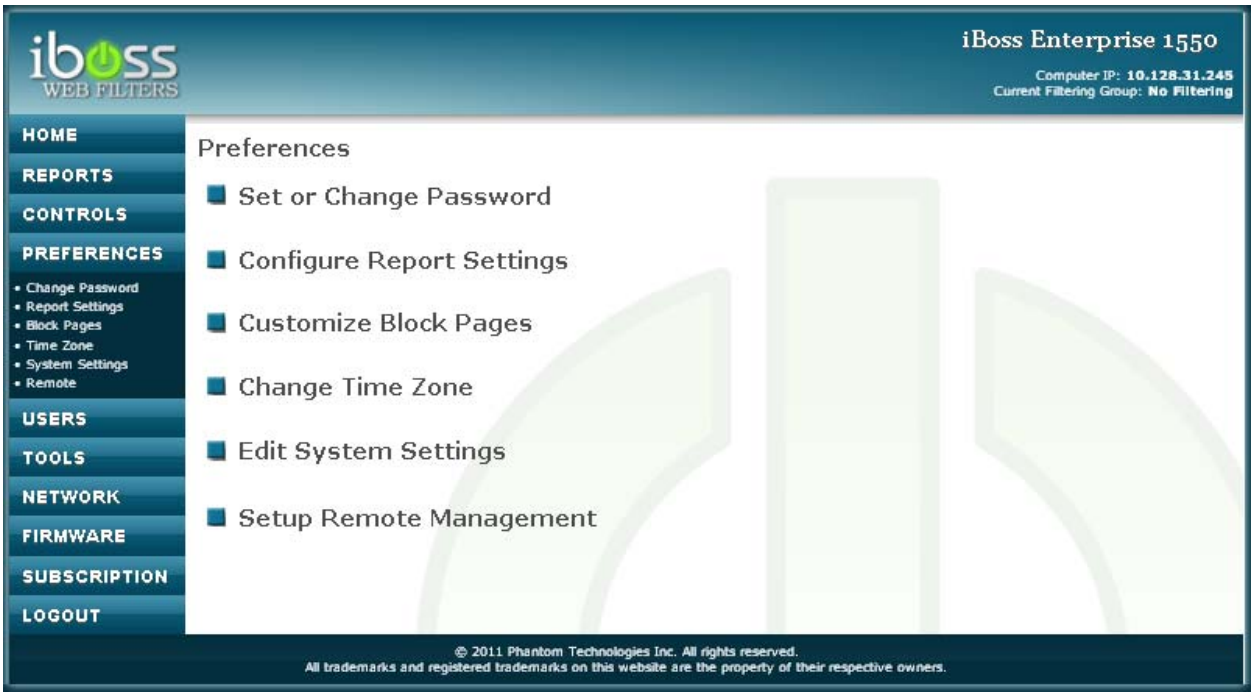

Figure 60 - Edit My Preferences

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

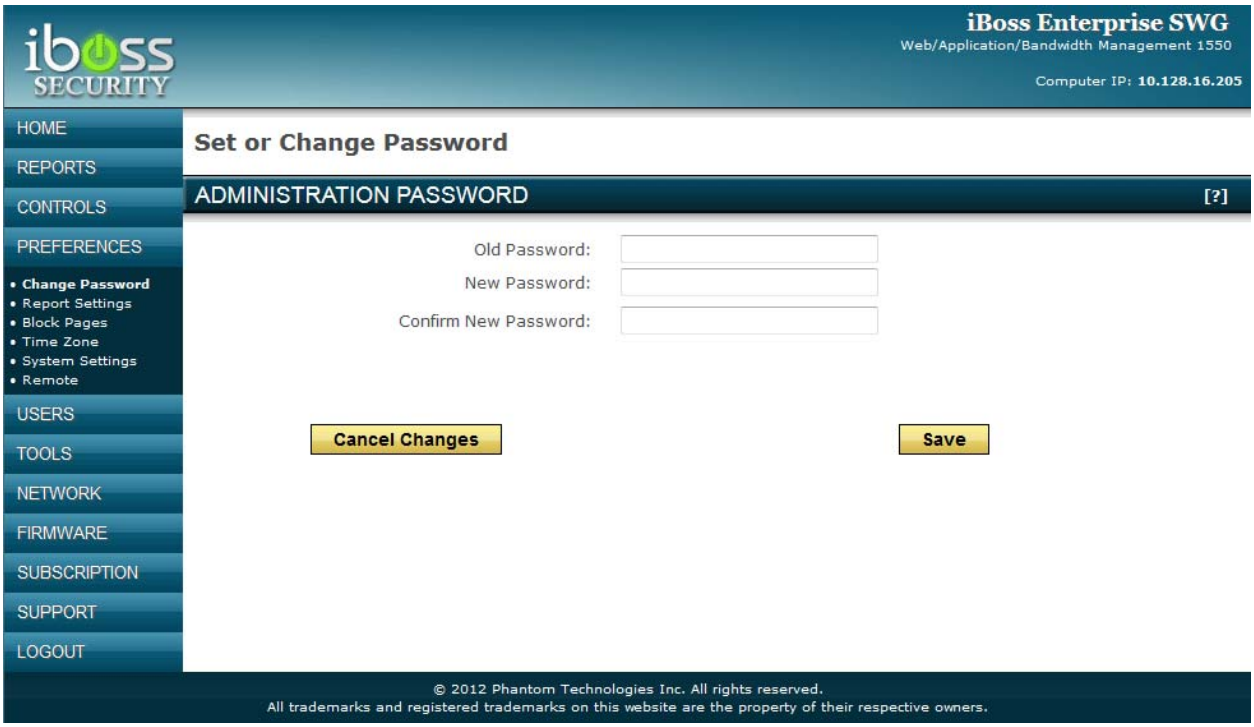

Figure 61 - Set or Change My Password

You may set or change the password used for managing the iBoss. The password may be a maximum of 24 characters in length.

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

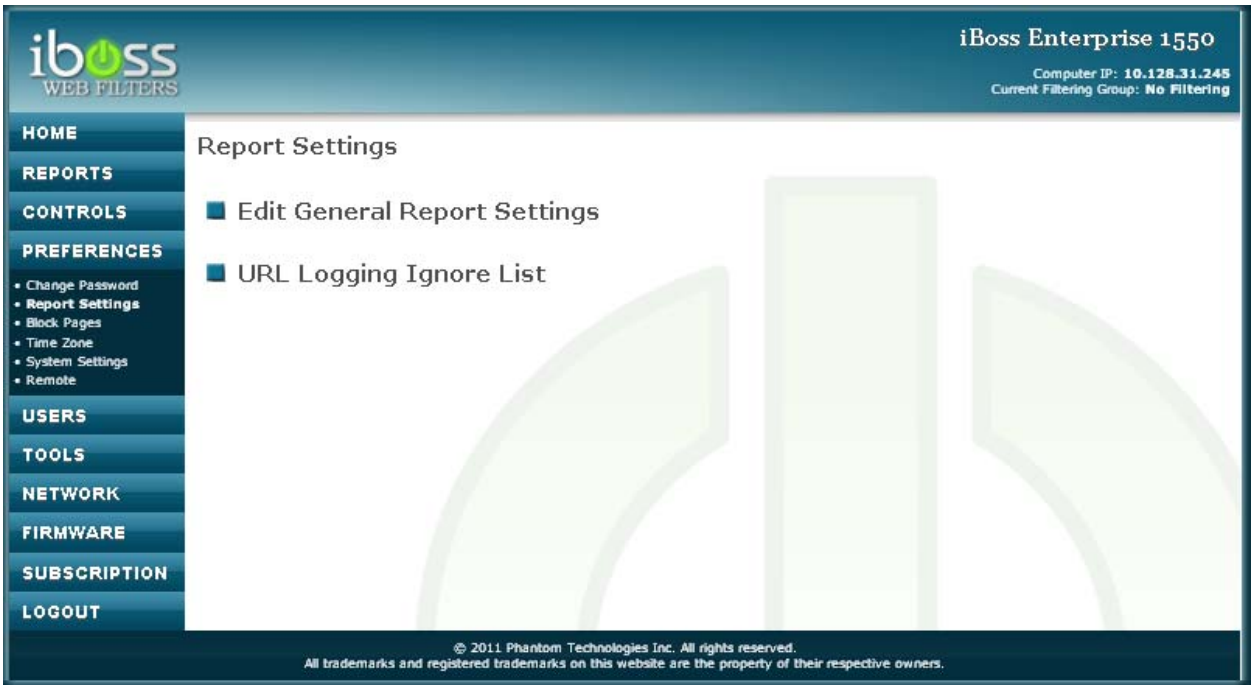

Figure 62 - Configure Report Settings

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

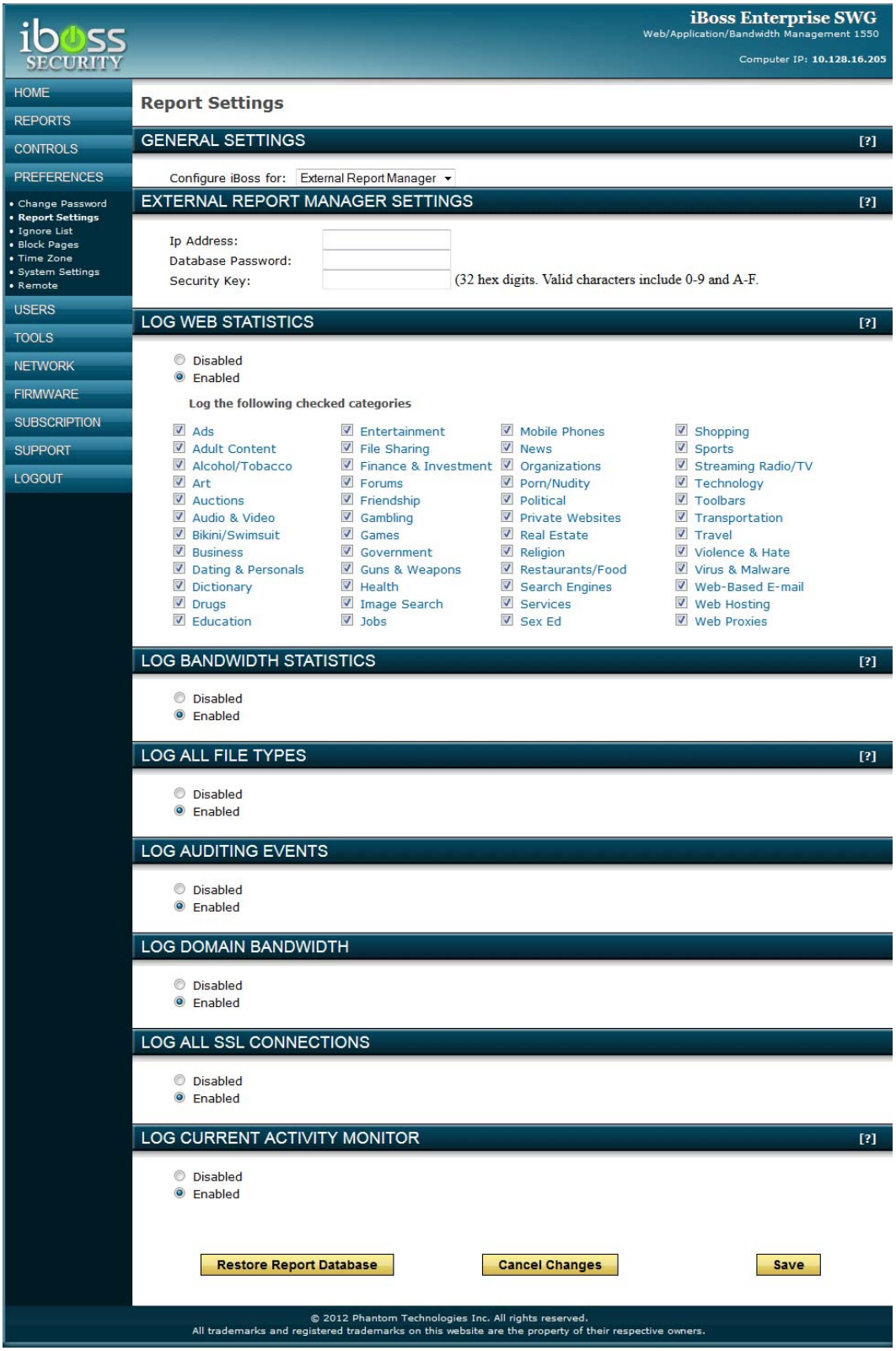

Figure 63 - Edit General Report Settings

These report settings are for the Report Manager.

General Settings – You may choose between Onboard Reporting and External Report Manager. If you have an External Report Manager, please choose External Report manager and refer to the following:

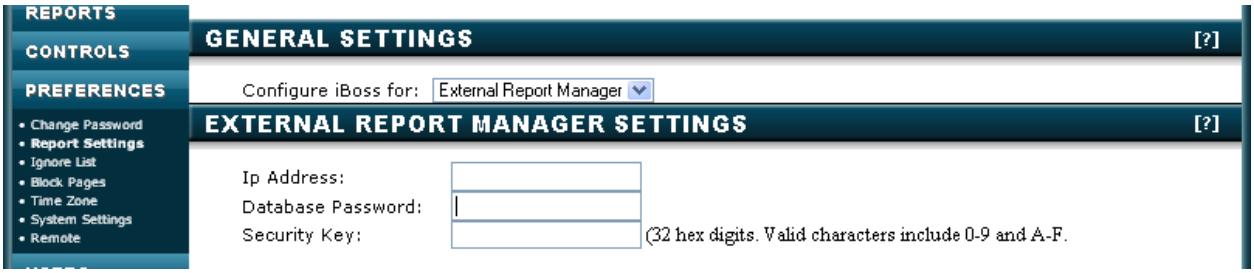

Figure 64 - External Report Manager Settings

* 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 general 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 – This allows you to enable or disable logging for web statistics. You may choose from the different categories to log.

Log Bandwidth Statistics – This allows you to enable or disable bandwidth statistics.

Log All File Types – This allows you to enable or disable logging of all file types. By default, this is disabled for images and resources on the page that may not be logged in the URL Log.

Log Auditing Events – This allows you to enable or disable logging of auditing events. These are changes that are made in the controls of the iBoss made by delegated administrators. You can go to the Logs of the reports and change the value for Audit Only to Yes to see only auditing events for setting changes.

Log Domain Bandwidth – This allows you to enable or disable the logging of bandwidth per domain for statistics. This is disabled by default as will have faster performance.

Log All SSL Connections – This allows you to enable or disable logging for SSL connections.

Log Current Activity Monitory – This allows you to enable or disable the current activity monitor.

4.3.2.2 URL Logging Ignore List

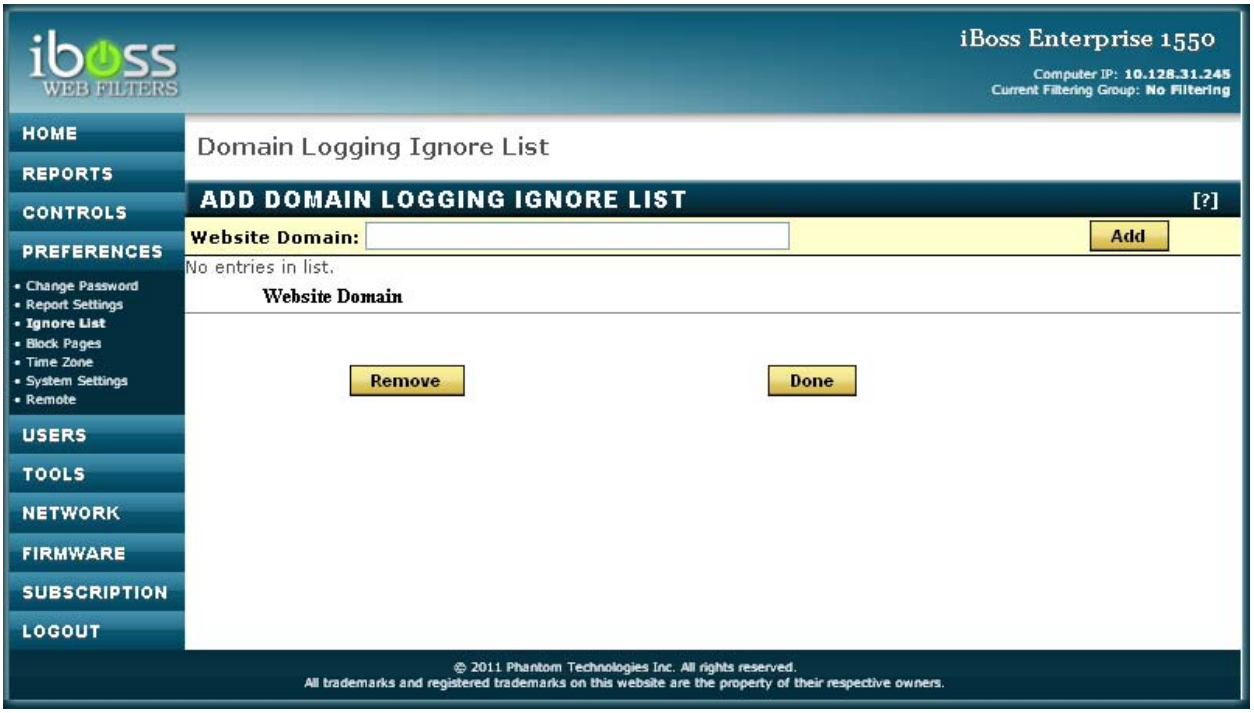

Figure 65 - URL Logging Ignore List

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

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.

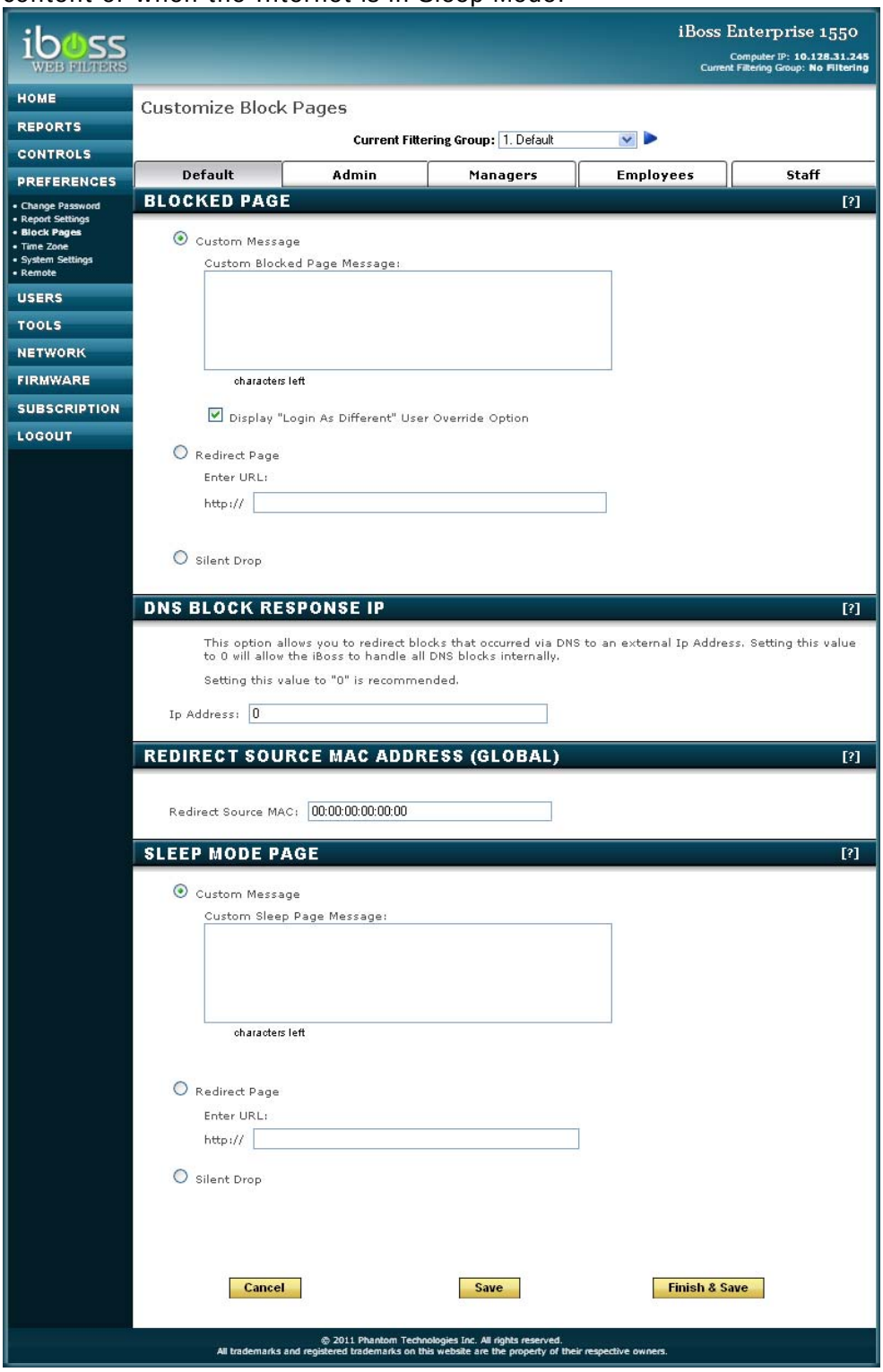

Figure 66 - Customize Block Pages

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.

DNS Block Response IP - This 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.

Redirect Source MAC Address - This allows specifying the source MAC address of the redirect packets injected by the iBoss. By default the iBoss uses its own MAC Address as the source within the redirect packet. This default behavior works for a majority of networks. In rare occasions, mostly involving the optional management interface, it is necessary to specify this if the internal switch gets confused. It is recommended that this setting only be changed if you absolutely know what you're doing. Setting the value below to 00:00:00:00:00:00 disables the feature and is the default.

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

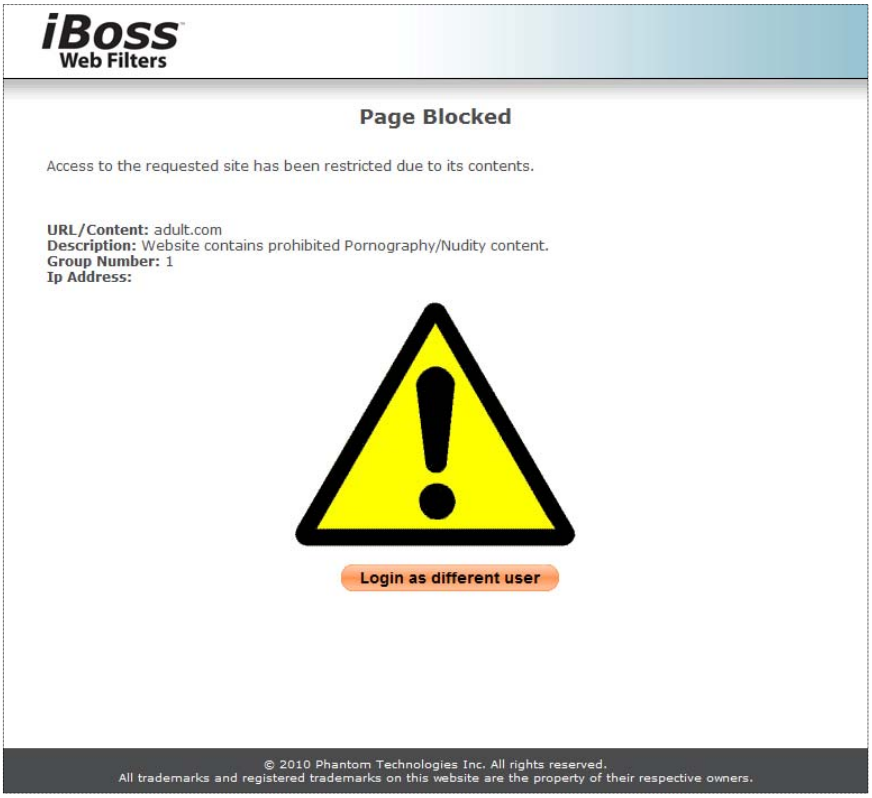

Figure 67 - iBoss Blocked Page

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

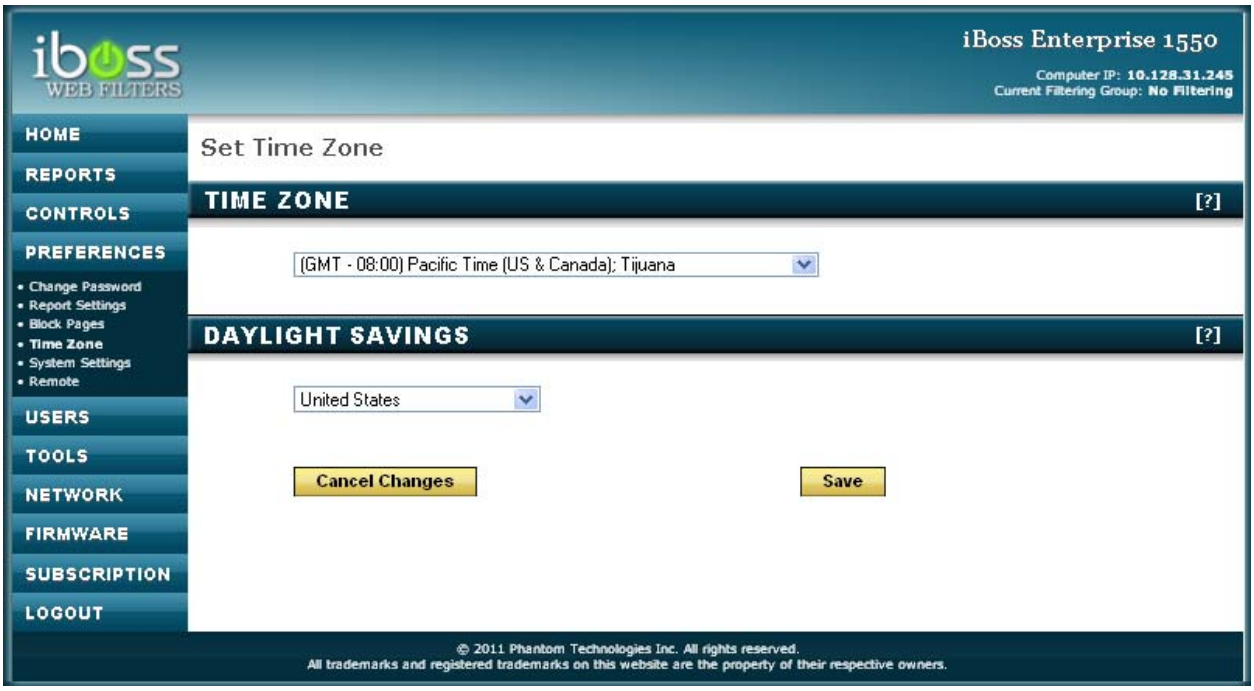

Figure 68 - Set Time Zone

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

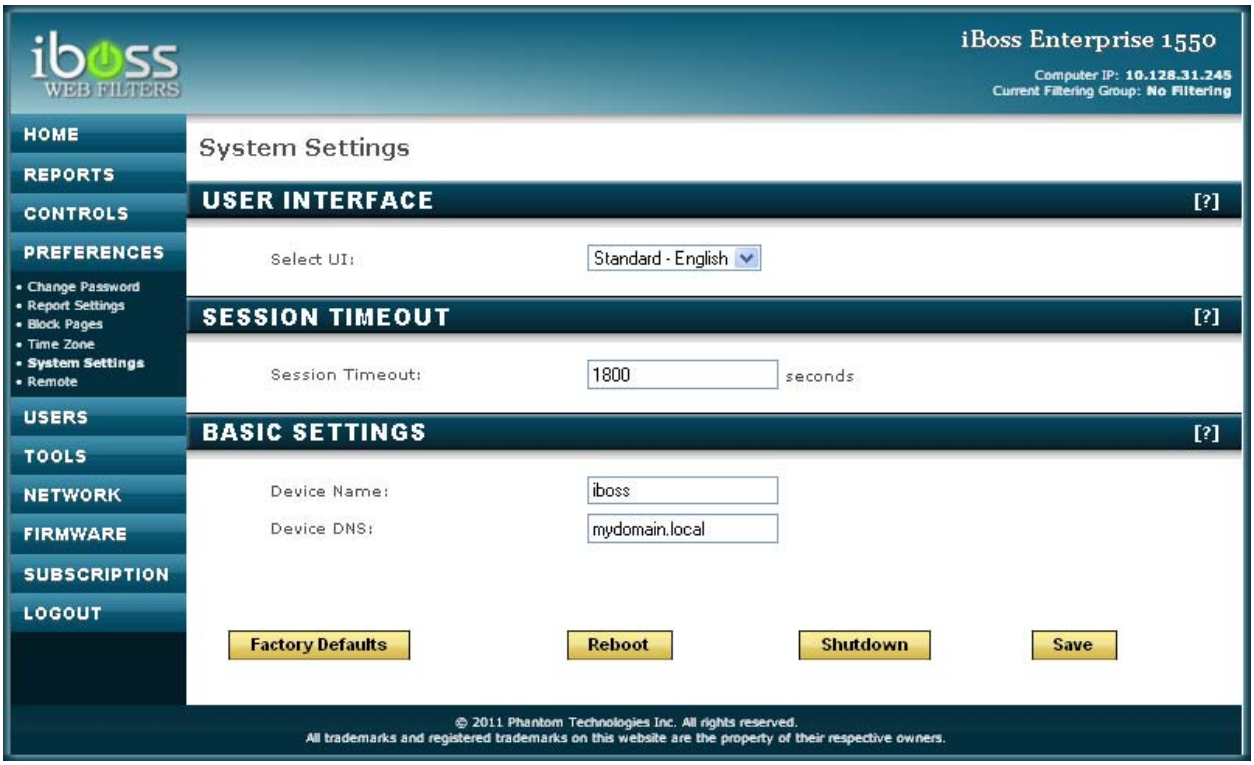

Figure 69 - Edit System Settings

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

Session Timeout – 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).

Device Name – This is the hostname of the iBoss device.

Device DNS – This is the domain that the device is to be part of. If you use active directory, enter your domain here.

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

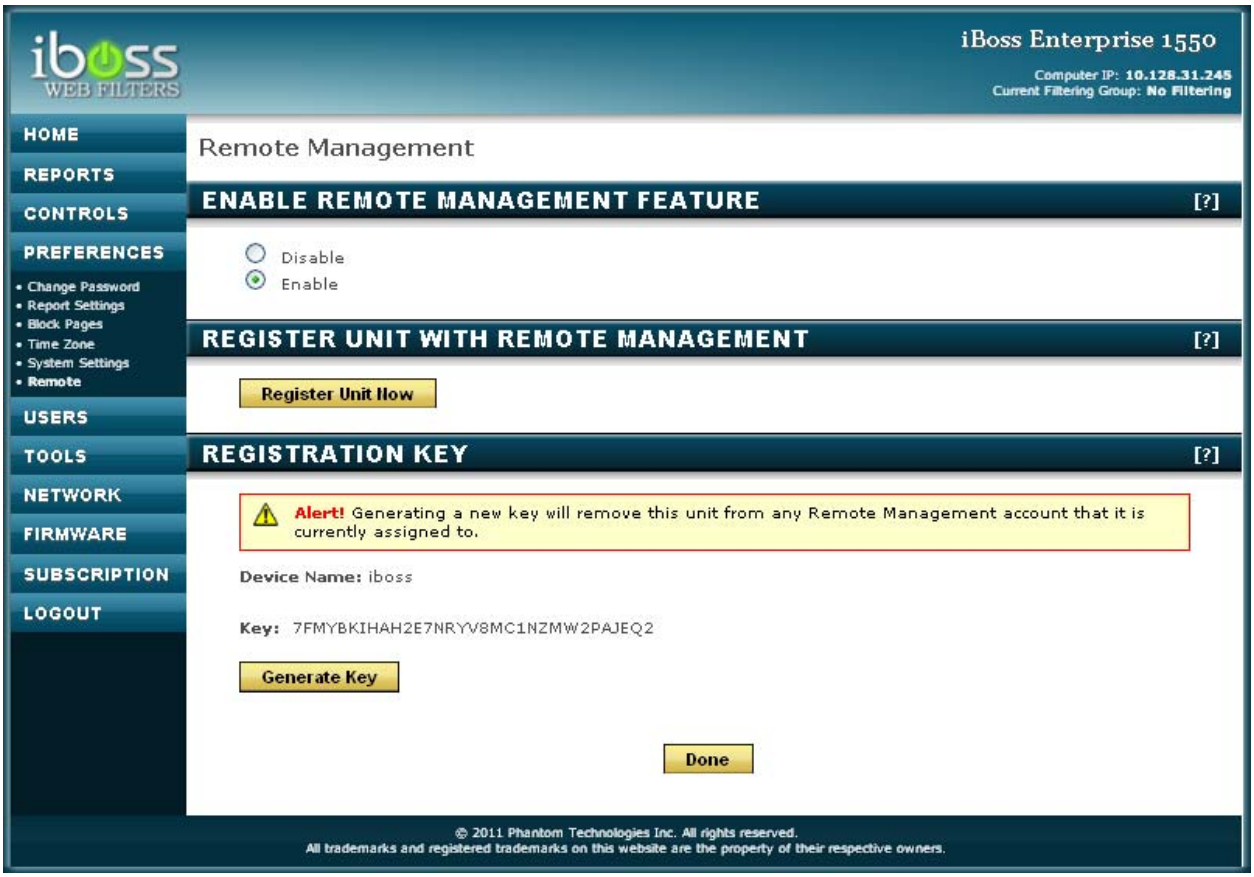

Figure 70 - Setup Remote Management

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 Users

Figure 71 - Users

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

4.4.1 Identify Computers

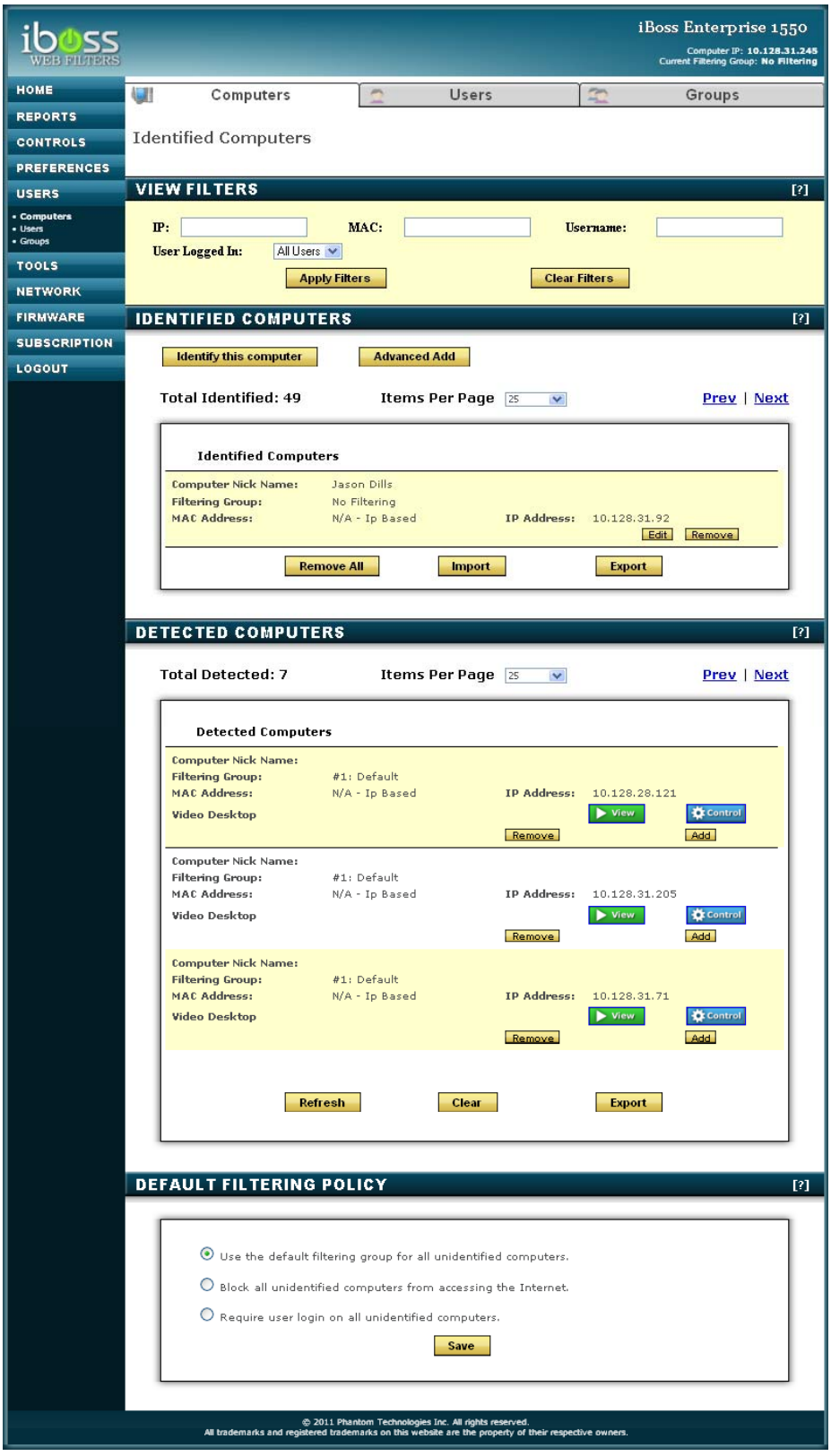

Figure 72 - Identify Computers

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

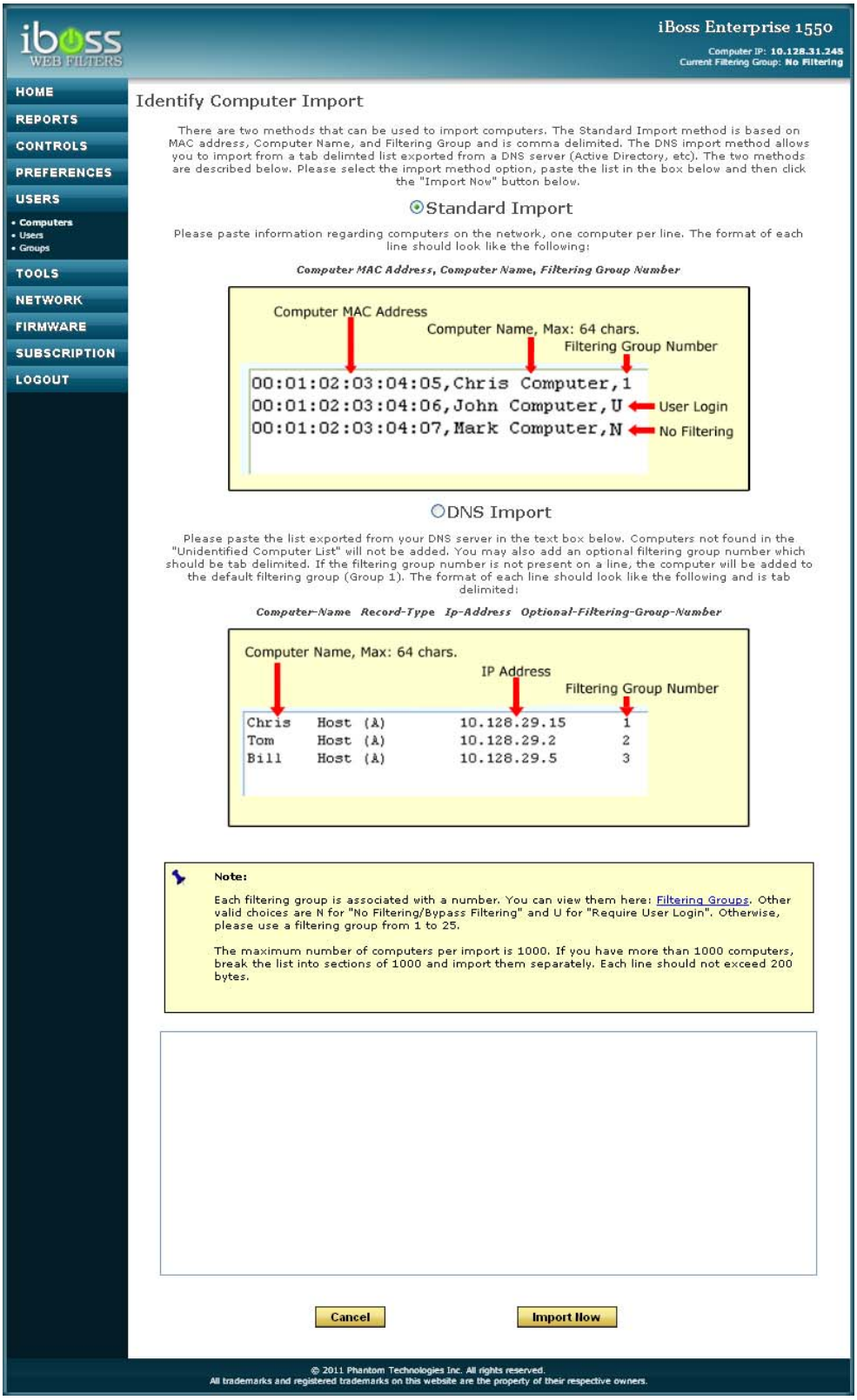

Figure 73 - Importing Computers

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

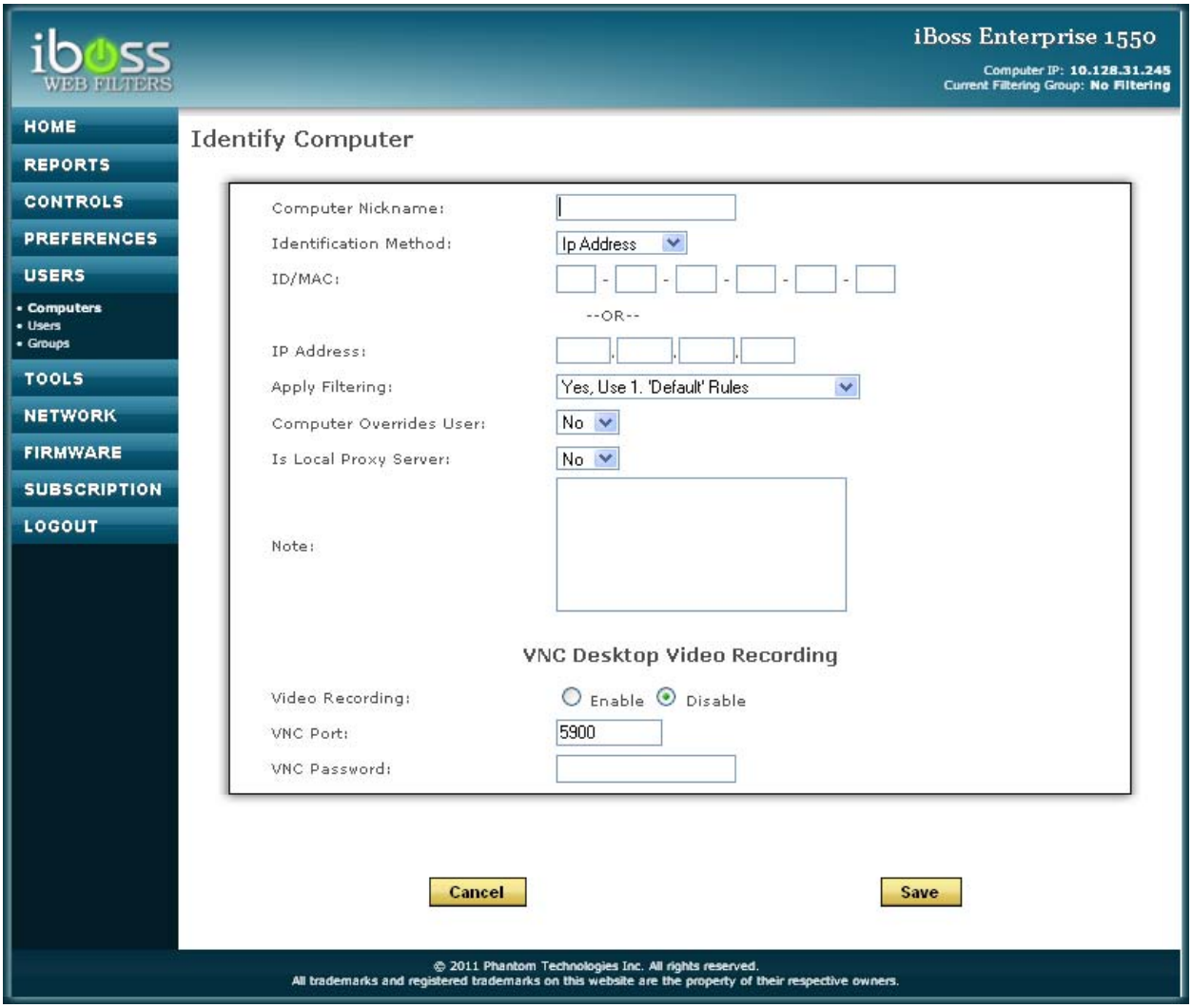

Figure 74 - Identifying a Computer

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

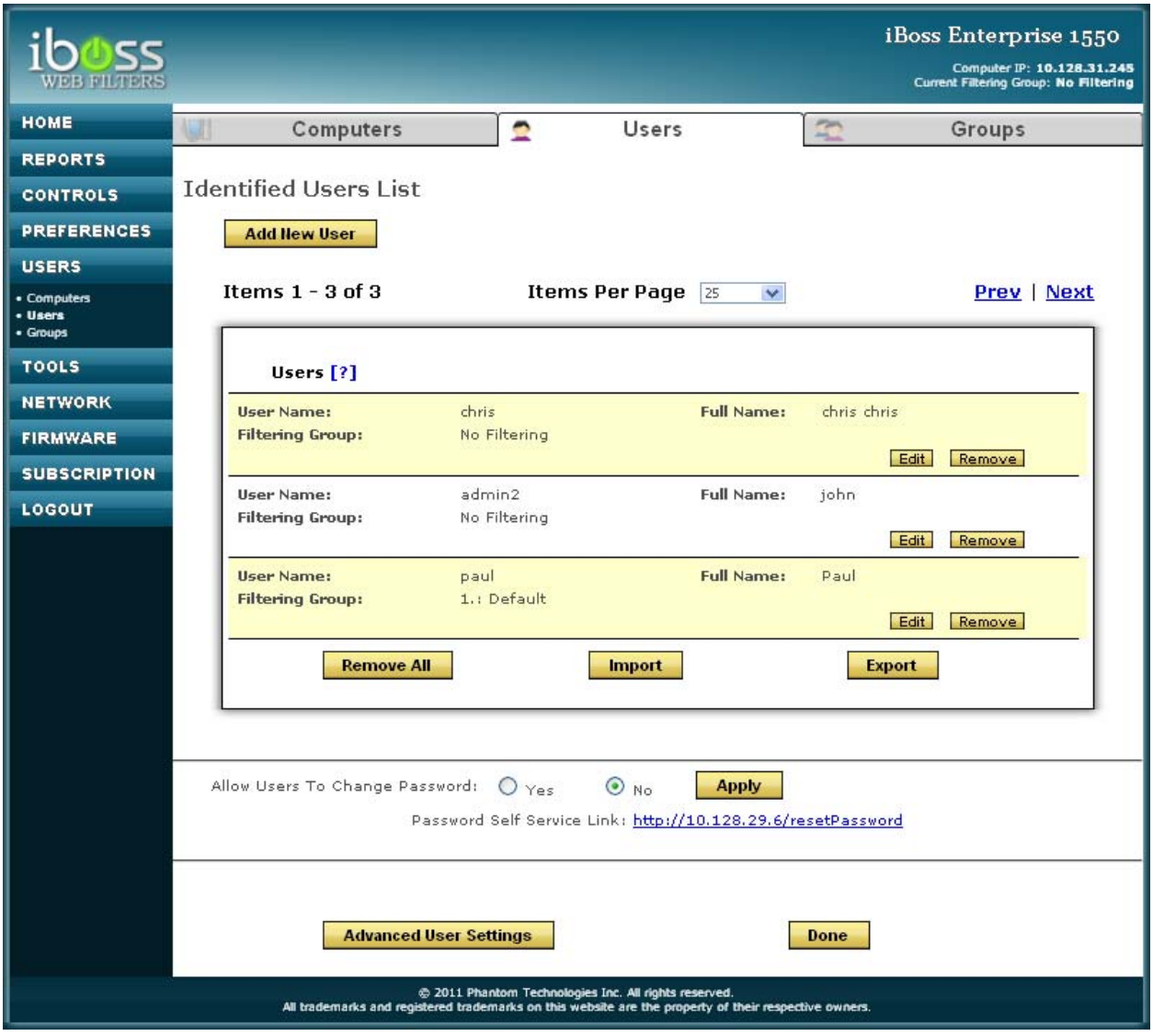

Figure 75 - Identify Users

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

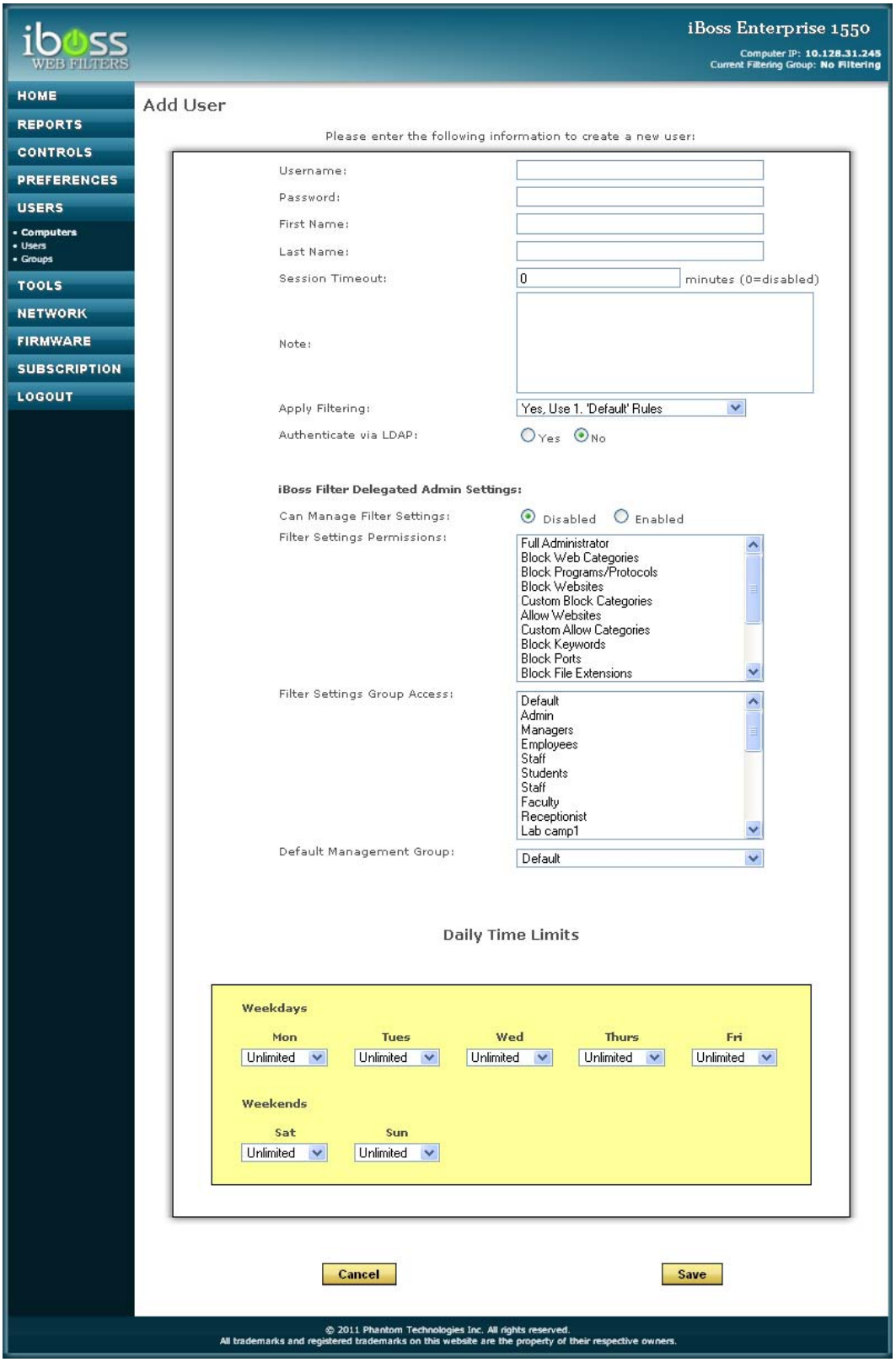

Figure 76 - Adding a User

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

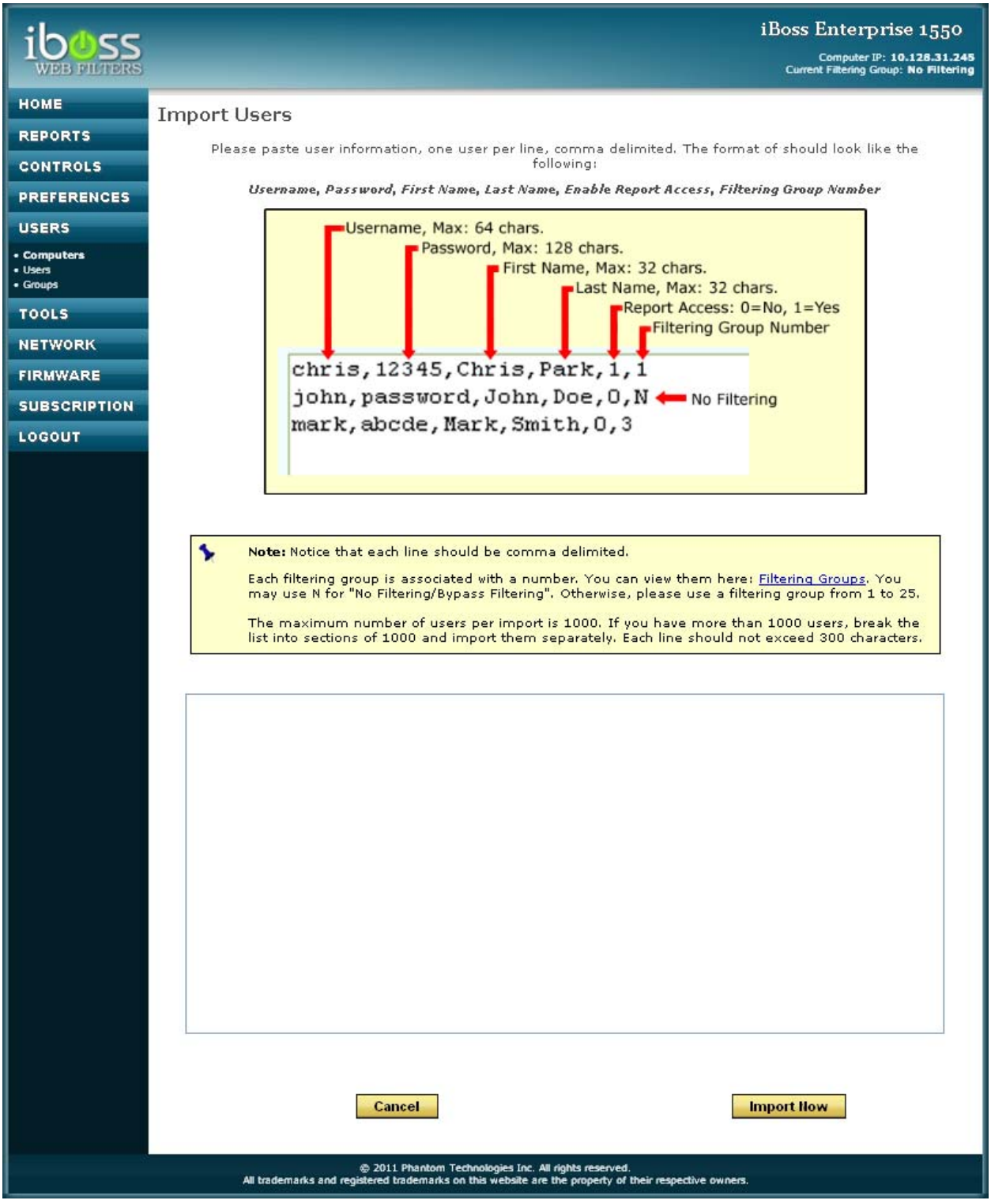

Figure 77 - Importing Users

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

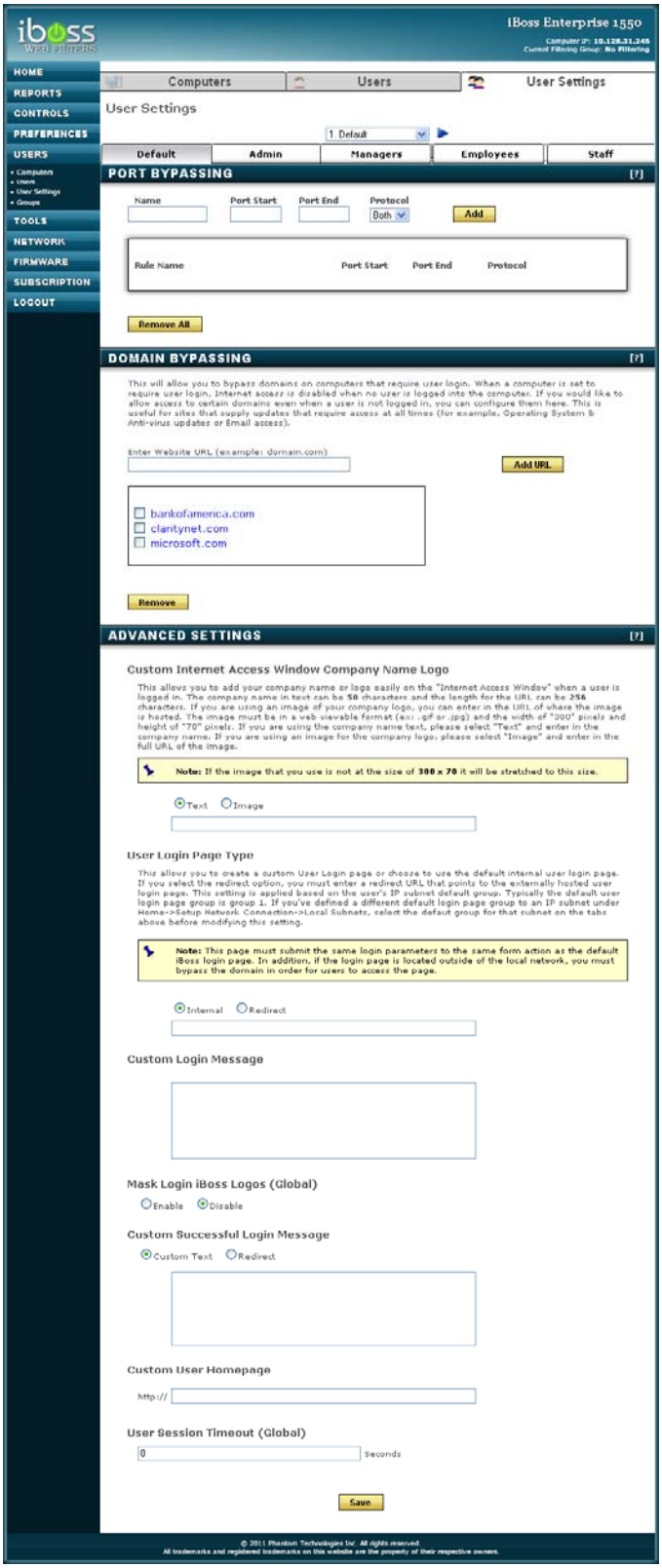

Figure 78 - Advanced User Settings

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 default 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 ensure filtering rules allow the 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.

Use Secure HTTPs Connection When Submitting Credentials on Login Window – This feature allows you to select to submit credentials on the Internet Access Window securely with https to the hostname of the iBoss or to the IP address of the iBoss.

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.

Manual Login User Session Timeout (Global) – 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. Whenever a manual user session timeout is specified under the user advanced user settings page, the timer is refreshed anytime traffic is detected going from LAN->WAN from that client. That keeps the client session alive as long as there is Internet activity from the client. In this way, even if the session activity window does not send heartbeats (for example with some mobile devices), any activity from the user keeps the session alive. If a session is set to 5 minutes, the user can surf for hours or more and whenever the user becomes idle for more than 5 minutes, the user is logged out. 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.

Auto-Login User Session Timeout (Global) – This allows you to change how long it will take before a user is automatically logged out after they have automatically been authenticated to login. 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

Figure 79 - Internet Access Window Login

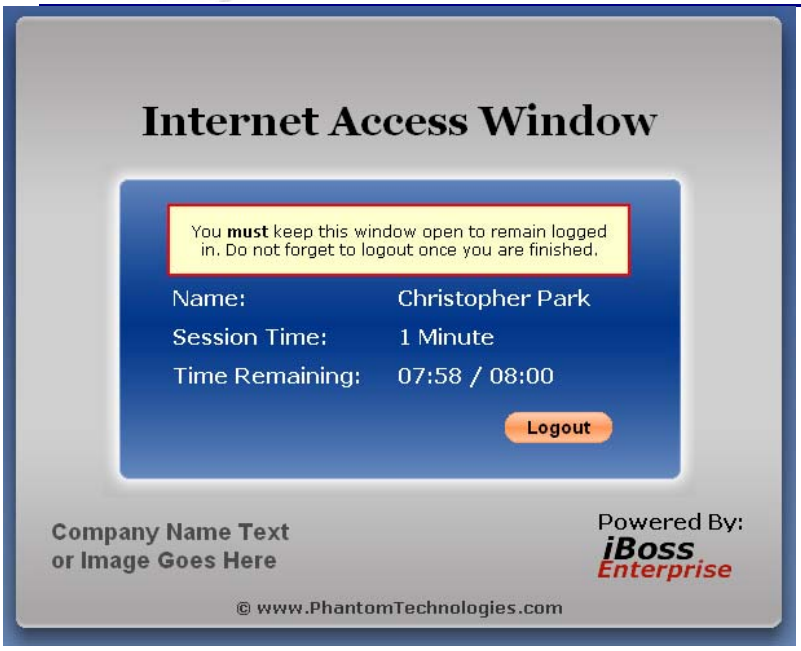

Figure 80 - Internet Access Window Session

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

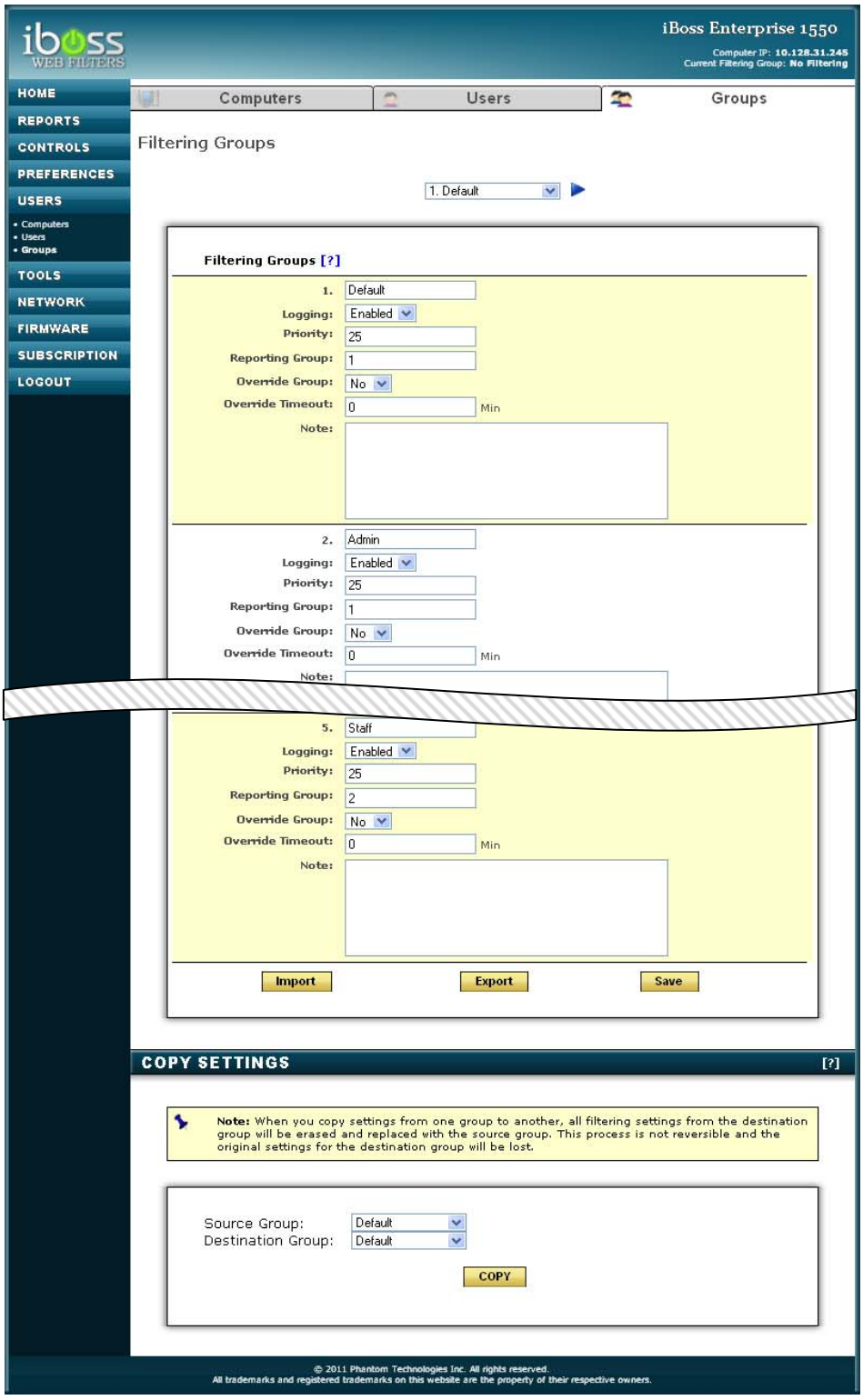

Figure 81 - Edit Filtering Groups

Filtering groups are used to apply Internet filtering rules to computers and/or users on your network. You may customize the group names to easily its purpose. Group names may be up to 50 characters in length.

When using transparent login via Active Directory, eDirectory, or LDAP, the group with the highest priority number is used if a user is a member of multiple groups that match the Active Directory, eDirectory, or LDAP server.

An iBoss filter group may be designated as an 'Override Group' which can be used as a method of temporarily changing to a different filtering group. This filter group should be given a priority higher than any additional filter groups a user may belong to. The Override Group will not initially be assigned for an Automatic login. A user presented with a block page may revalidate his credentials and be "bumped" up to the override group until logout or 'Override Timeout'.

Note: When identifying computers under 'Identify Computers & Users' you may choose one of the filtering groups or 'Bypass Filtering Rules' for a particular computer.

Copy Settings – This allows you to quickly copy filtering settings from one group to another. Select the group to copy settings from and a group to copy settings to and then click the COPY button below. This will completely overwrite the destination and provides a configuration starting point but there is no connection between the groups from this point.

Note: This process is not reversible and the original settings for the destination group will be lost.

4.4.3.1 Filtering Group Tabs

Figure 82 - 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 Tools

4.5.1 Backup & Restore Manager

Figure 83 - Backup & Restore Manager Login

The login for this interface requires the full admin password to login.

Figure 84 - Backup & Restore - Restore Points & Creating Restore Point

Once you login, you can see all the restore points that have been created. There are no restore points created by default. It is recommended to create a restore point after you have configured your controls settings and then click the Download button to copy the restore point off of the device.

When a restore point is created, you have the option to delete it off the device, download the restore point which contains all of the settings and firmware, and the option to restore the iBoss device back to a specific Restore Point.

Restoring the iBoss from a restore point must be from the same model of the iBoss. It does revert back to the firmware version number that the iBoss was on when the restore point was created.

If you have multiple iBoss devices and would like to copy settings from one device to another, one thing to note is that the subscription key also gets copied and restored. This may overwrite your current subscription key for the second unit. If this is the case, you will want to save the restore point of the second iBoss device and after restoring an imported restore point, overwrite the subscription key with the original subscription key that was there prior.

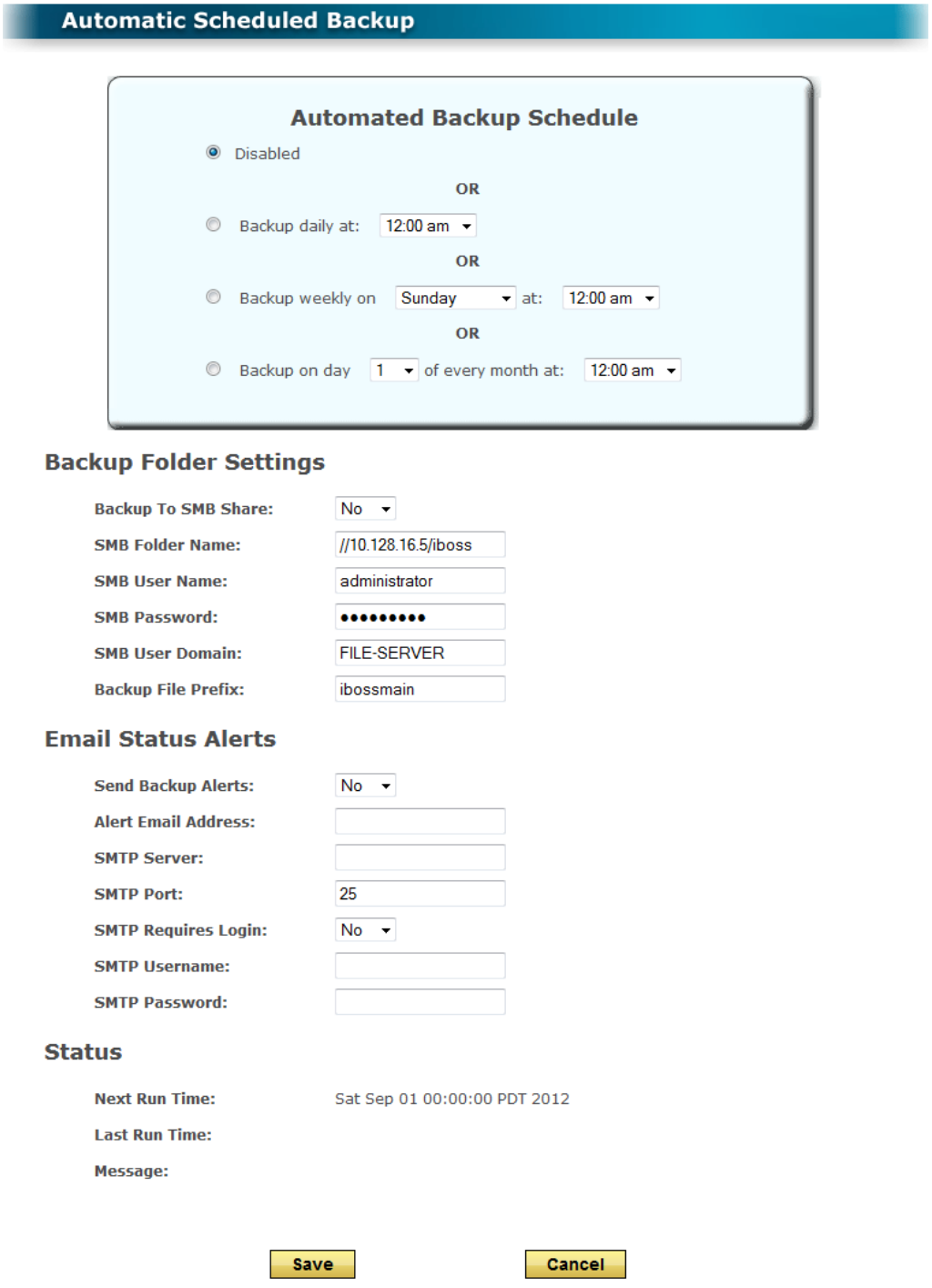

Figure 85 - Automated Scheduled Backup

You can setup a schedule to create a restore point of the settings on a daily, weekly, or monthly schedule. This saves a restore point onto the iBoss device.

Backup Folder Settings – You can save these scheduled restore point backups to a SMB Share folder. You will want to enable this feature and setup the folder path and authentication settings.

Email Status Alerts – These options will allow you to use an SMTP server to email you when a backup was successfully run.

Figure 86 - Restore Settings

This option allows you to import a restore point into the device. This is handy if you'd like to copy settings from one device to another or if you have an onsite spare device and have automated backups running and need to restore to a backed up restore point.

To restore to a backup, click **Browse** and find the .ibrp backup file for the restore point and click **Import**. This will add it to the list of Restore points at the top of this page. When you are ready, click the **Restore** button next to the Restore point which will reboot the device and load this restore point.

4.5.2 Clear Internal Caches

This option will clear all cached usernames to filtering groups used with the AD Logon Scripts. It will also clear any signature matches for applications that have been detected based on signature footprint.

4.5.3 Trigger MDM Sync

This option syncs the settings with the MDM MobileEther. This feature would need to be enabled on the iBoss under Home → Preferences → System Settings. This option would also need to be enabled on the iBoss Enterprise Reported and integrated with the MDM MobileEther interface.

4.6 Firmware Updates

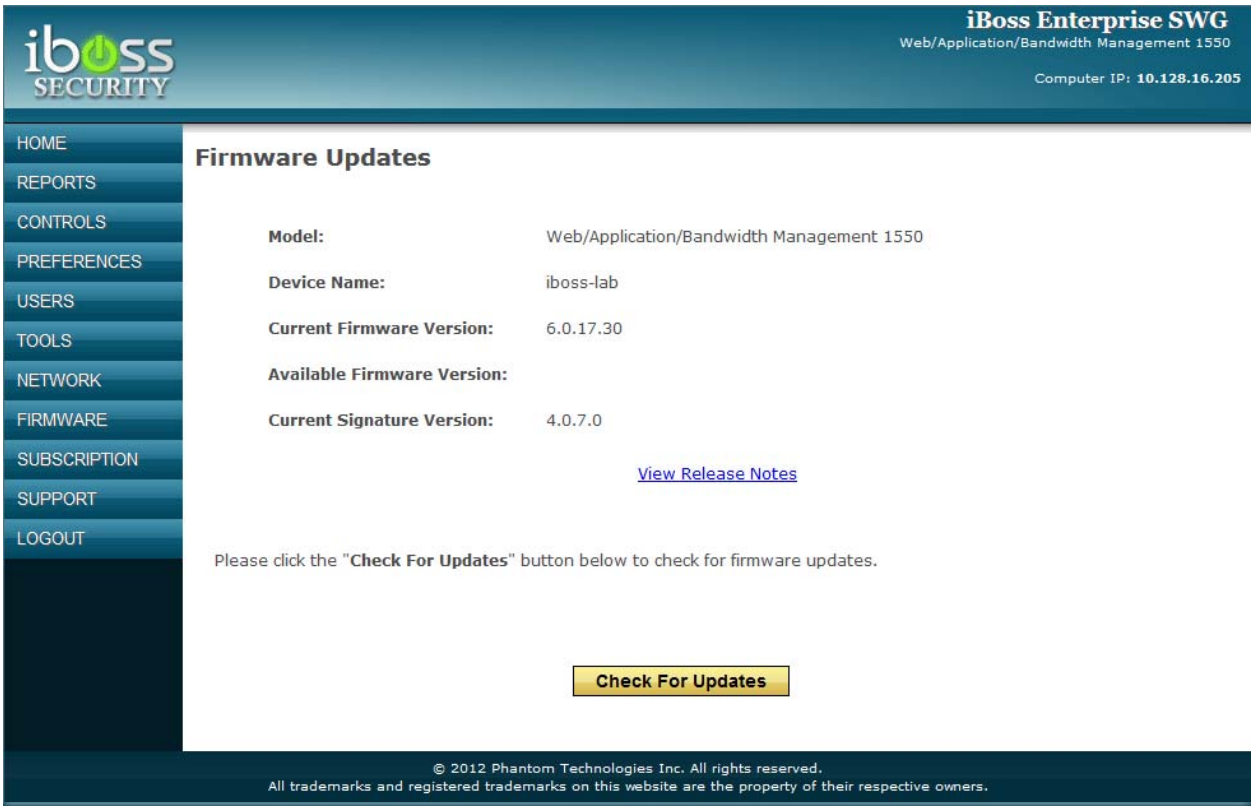

Figure 87 - Firmware Updates

Firmware updates are published as needed. 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 REMOTE MANAGEMENT

Figure 88 - 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.

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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.

6 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.

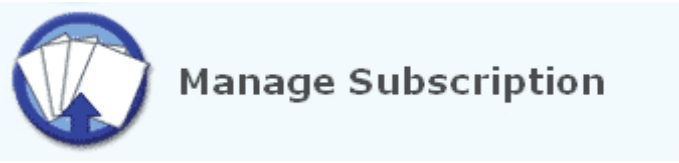

Figure 89 - Manage Subscription

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.

6.1 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 90 - 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.

7 TROUBLESHOOTING

7.1 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.

7.2 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.

7.2.1 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.

7.2.2 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.

7.3 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

8 APPENDIX

8.1 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.iboss.com/product_terms.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

9 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.

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.

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.

10 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.