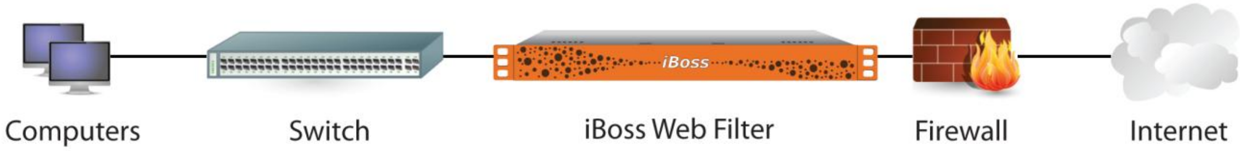
iBoss Enterprise Deployment Guide

iBoss Web Filters



www.iBossWebFilters.com

Table of Contents

Table of Figures

1 iBoss Enterprise Installation And Deployment Guide

1.1 Overview

This guide will provide step-by-step instructions for deploying the iBoss Enterprise Web Filter on your network. The guide provides instructions for both the hardware installation as well as initial configuration of the iBoss settings.

2 Getting Started

This section describes the initial preparation of the iBoss and provides an overview of what is included in the iBoss packaging.

2.1 Package Contents

The following items are included with the iBoss Enterprise:

- iBoss Enterprise appliance
- Power cable
- RS-232 null terminated console cable
- Quick Install Reference Pamphlet

2.1.1 iBoss Enterprise Appliance Description

The iBoss Enterprise is a rack-mountable appliance. Typically, the iBoss will occupy 1U of rack-mount space.

2.1.1.1 Front Panel

The front panel consists of a power button and status LEDs. The power button provides soft power up and power down by pressing and releasing the button quickly.

To perform a hard power down, press and hold the front panel power button while the appliance is powered on. It is recommended that you use the normal soft power down by quickly pressing and releasing the panel button and waiting approximately 1 minute for the iBoss to gracefully shutdown.

2.1.1.2 Back Panel

There back panel consists of two 10/100/1000 copper Ethernet network ports and a serial console port.

The serial console port is accessible with the provided RS-232 null terminated console cable.

The network ports are labeled LAN and WAN, respectively. These are used to connect the iBoss inline on your network.

NOTE	On certain models, there is a third network interface. This interface is labeled "**Management Interface**". With this interface, the iBoss is able to provide out of band packet filtering support (via port monitoring/mirroring/spanning which is configured on the switch or firewall). This is described later in the guide.

3 Detailed Step By Step Deployment Guide

This section provides a step by step guide to deploying the iBoss on your network. You may be asked to jump to step numbers depending on your specific configuration.

3.1 Configure the iBoss IP Address

3.1.1 Determine whether iBoss has Management Interface

There are two primary configurations the iBoss is shipped with. The two configurations are (1) without a management interface (2 network ports, LAN and WAN) and (2) with a management interface (3 network ports, LAN and WAN + management port).

Before proceeding, determine whether your iBoss is configured with a management interface or not. An iBoss with a management interface has 3 network ports on the back of the appliance. The two network ports in the center of the appliance are labeled LAN and WAN. In addition, the management interface is clearly labeled "**Management Interface**" and is typically located toward the right hand side of the appliance when facing the back of the appliance.

An iBoss without a management interface has two ports in the center of the appliance labeled LAN and WAN.

NOTE	In order to deploy the iBoss in a non-inline deployment (out of band) via a monitor/mirror/span port, a management interface is required.

3.1.2 Description of Network Ports And How To Access Them

3.1.2.1 iBoss without "Management" Network Interface (2 ports, LAN+WAN)

This section describes the iBoss in a 2 network port configuration (without a management interface).

The iBoss is a fully transparent network bridge which behaves similarly to a layer 2 network switch. It will use a *single* static IP Address which is accessible on both the LAN and WAN port. The iBoss does not route packets and behaves similar to a switch. Thus, the LAN will contain and use the same IP Address as the WAN port and they are not configured separately. The interfaces are a SINGLE "**logical**" interface.

The assigned management IP Address will be accessible via either network port (it does not contain an Inner + Outer IP Address typically found in a firewall/router).

A typical deployment with this configuration is show below:

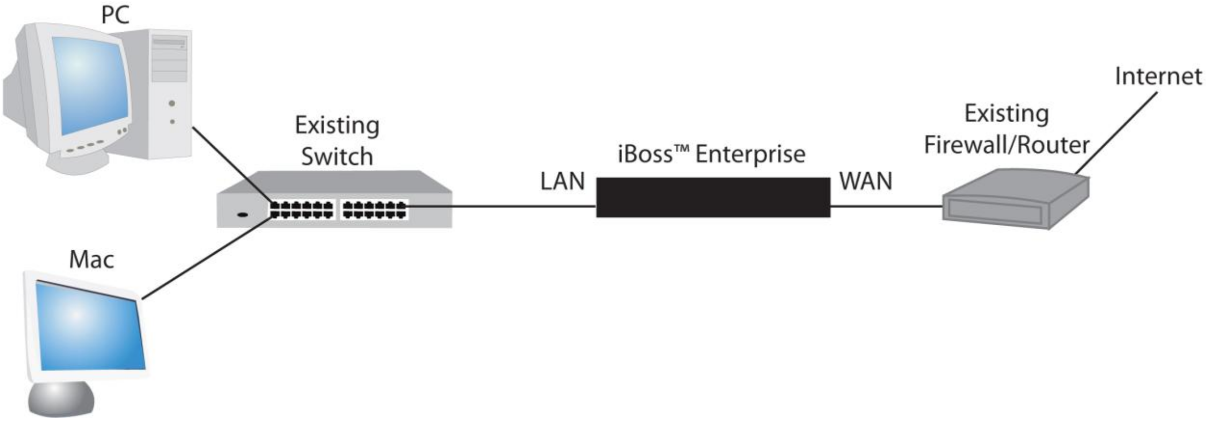


Figure 1 - iBoss inline deployment diagram

3.1.2.2 iBoss WITH "Management" Network Interface (3 ports, LAN+WAN+Management)

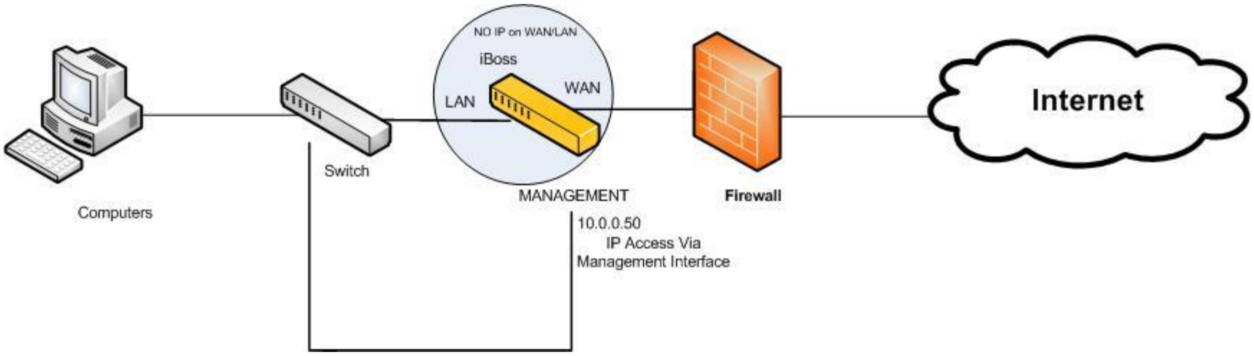
NOTE	This section does not apply if you do not have a management interface present on the iBoss Web filter. Typically, this configuration includes 3 network ports on the back of the iBoss device. If you do not have a management network interface present, you may skip this section.

This section describes the iBoss in a 3 network port configuration (1 network port for LAN, 1 network port for WAN, and 1 network port for the Management Interface).
The LAN and WAN port form a fully transparent network bridge that behaves similar to a layer 2 network switch. However, unlike the case without a management interface above, the LAN and WAN do not have an IP Address assigned and the management/configuration interface cannot be accessed via the LAN or WAN port. The LAN/WAN port do not route packets (like a firewall/router). The network interfaces (LAN/WAN) forward packets between interfaces like a switch. A packet received on the WAN port is sent on the LAN port. A packet received on the LAN port is sent on the WAN port.

The IP Address is assigned to the "**Management**" interface. This port is used to access the iBoss configuration web interface. The LAN/WAN port are blind and the web configuration interface cannot be accessed via those two ports.

When used in an inline mode, the LAN and WAN port are placed inline with the network traffic typically between the inner network switch and outside firewall, while the "**Management**" interface is connected to the inner network switch as well which provides access to the iBoss web configuration interface.

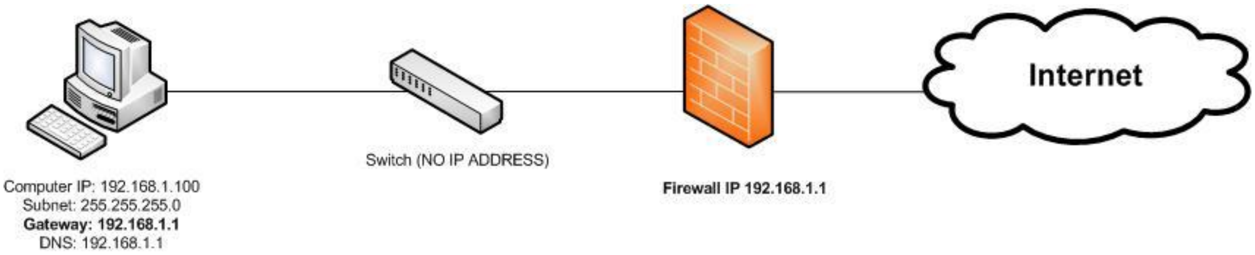
A typical deployment with this configuration is show below:



3.1.3 Selecting the appropriate IP Address Settings for the iBoss

It is important to select the appropriate IP Address in order to be able to access the iBoss via the web interface once installed. There are 2 typical network configurations which usually is dependent on network size. Determine your network configuration with the guided description below to help determine what the iBoss IP settings should be configured to.

1. **(Simple Network Topology) Inner switch is a layer 2 switch and performs no routing. In this case, the gateway IP Address configured in your computer is your outer firewall. See diagram below:**



Typical switches in this configuration are entry level Cisco switches (2150 series and below), entry level HP Procurves, etc. Notice that the switch does not have an IP Address and that the gateway of the computer is the firewall. Check the gateway on your computer if you cannot determine if this is your network configuration.

If your gateway is your firewall, then this is most likely your network configuration.

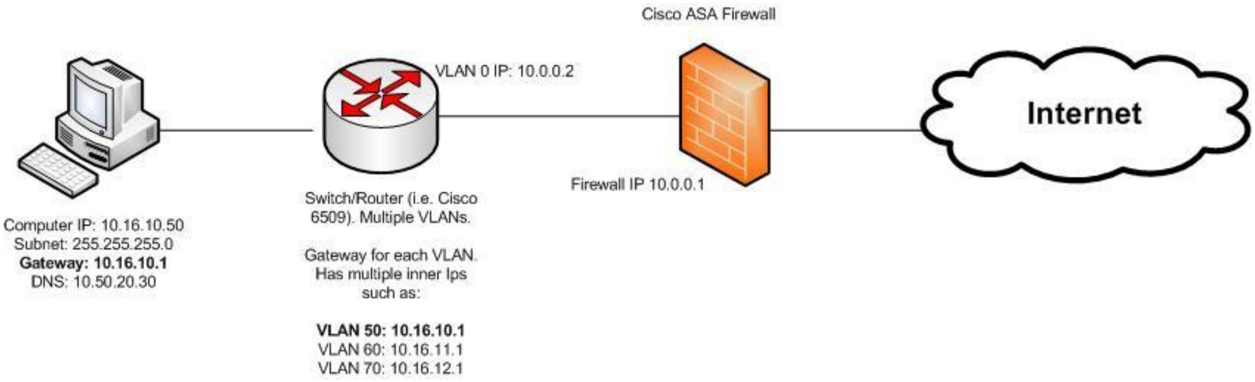
In this scenario, the iBoss should be configured with any available IP Address on the network that is outside the DHCP range. In addition, configure the gateway IP Address of the iBoss to be the outer firewall. If you use an internal DNS server, use those settings for the DNS IP Addresses. See sample settings below:

Table 1 - Simple Network Sample iBoss IP Settings

IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS1	192.168.1.1 –or— Internal DNS Server IP

DNS2	192.168.1.1 –or— Internal DNS Server IP (you can use the same as DNS1 if you do not have a secondary DNS server)

2. **(Complex Network Topology) Inner switch/router is a gateway and is capable of routing packets. Most computers on the network have their gateway IP Address set to the inner switch/router and not the outer firewall. See diagram below:**



In this configuration, the gateway IP Address of computers on the network is configured to point to the core switch/router on the network. Typical switch/routers include Cisco series 6500, etc. Notice the Firewall inner interface IP Address is NOT used as the gateway for computers on the network (in this case 10.0.0.1). Also, the switch router is the gateway for each VLAN on the network and performs Inter-VLAN routing.

If your computer uses the core switch/router as its gateway, then this is most likely your configuration.

In this configuration, the **iBoss should be configured with IP Address settings on the same VLAN as the inner interface of the firewall**. For example, in the diagram above, the firewall is in a 10.0.0.X VLAN, so the iBoss should be configured with an IP Address similar to 10.0.0.10.

In addition, **the gateway IP Address of the iBoss should be configured to the inner switch/router** (and not the outer firewall).

NOTE	If you set the switch as the gateway, you will need to add the iBoss to the bypass list so that it is not filtered.

See sample iBoss settings below:

Table 2 - Complex Network Sample iBoss IP Settings

IP Address	10.0.0.15
Subnet Mask	255.255.255.0
Gateway	10.0.0.2
DNS1	Internal DNS Server IP –or—

	External DNS Server IP (If not using Active Directory or Hosting Internal DNS)
DNS2	Internal DNS Server IP –or— External DNS Server IP –or— Same As DNS1

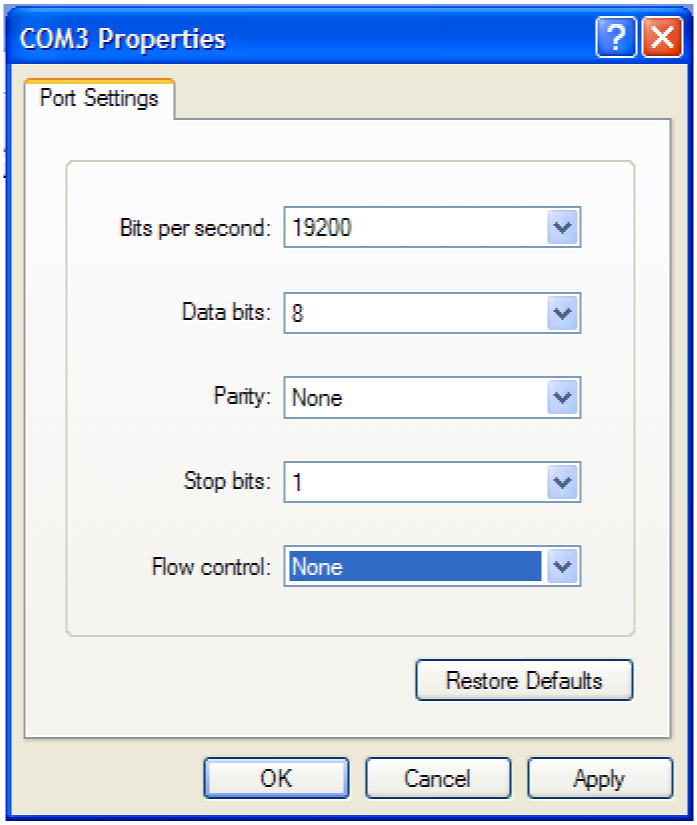
3.1.4 Methods for configuring iBoss IP Address

Once you have determined the appropriate IP Address settings for the iBoss, use one of the two methods below to configure the IP Address. You have two choices to do this. The first is via the serial console port on the iBoss. The alternative method is directly via the network interface on the iBoss.

3.1.5 Configuring the IP Address via the serial console port

Attach the included serial cable to your computer and to the back of the iBoss. Using a program such as HyperTerminal or Putty (available free of cost on the web), configure the following settings in the serial application:

Table 3 - Serial Console Settings



COM3 Properties

Port Settings

Bits per second: 19200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Once the iBoss is fully powered on (the iBoss beeps 3 times when fully powered which usually takes approximately 1-2 minutes), press Enter a few times in the serial console application to bring up the menu. The iBoss configuration menu should appear.

Select the "**Configure IP Address**" option.

Now enter the IP Address settings that were determined above. When finished, the iBoss will ask you to type the word "**yes**". Once this is entered, the settings are saved and the iBoss reboots. If you make a mistake while entering the settings, just press the enter key when asked to type the word "**yes**" and you will be returned to the main menu.

NOTE	While entering settings into the console menu, you must hold down the "**Ctrl**" key if you would like to use the backspace to remove characters.

3.1.6 Configuring the IP Address via the network port

You can configure the iBoss IP address by connecting your computer directly to the network port on the iBoss. If your iBoss has a management interface, connect your computer to the "**Management**" interface. If the iBoss does not have a management interface, connect your computer to either the LAN or WAN network port on the iBoss.

The iBoss is configured with a static IP Address and will not serve your computer an automatic IP Address via DHCP. You must configure your computer to have a static IP Address that is on the same network as the iBoss's default network settings. Follow the instructions below to do this.

The default IP Address settings of the iBoss are:

Table 4 - Default iBoss IP Address Settings

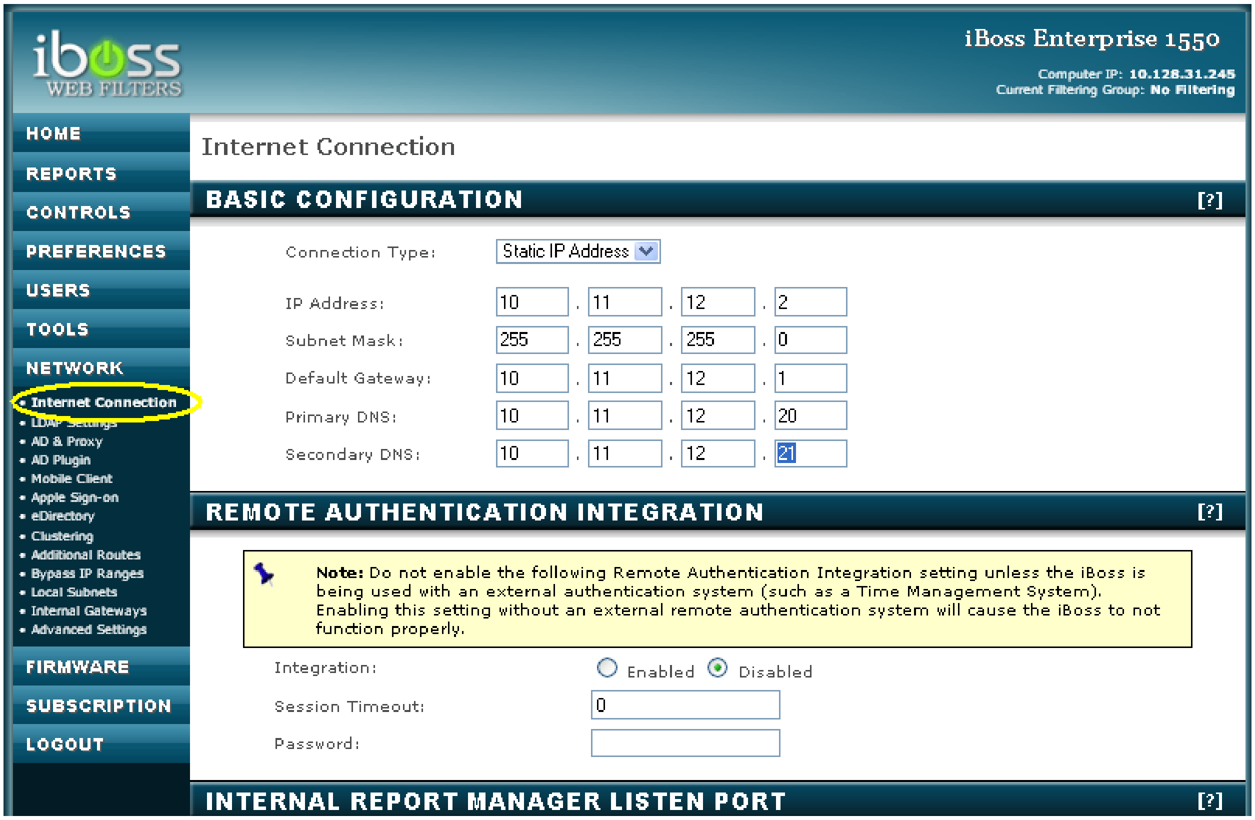
IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS1	192.168.1.1
DNS2	192.168.1.1

Configure your computer to have a static IP Address of 192.168.1.50 with a subnet mask of 255.255.255.0. Do not enter gateway or DNS IP Address settings.

IP Address	192.168.1.50
Subnet Mask	255.255.255.0
Gateway	None
DNS1	None
DNS2	None

Figure 2 - Sample Computer Network Settings for configuring iBoss IP Address via Network Interface

Now open a web browser and navigate to 192.168.1.10. The iBoss home page should come up in your browser.



iBoss Enterprise 1550

Computer IP: 10.128.31.245
Current Filtering Group: No Filtering

Internet Connection

BASIC CONFIGURATION

Connection Type: Static IP Address

IP Address: 10 . 11 . 12 . 2

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 11 . 12 . 1

Primary DNS: 10 . 11 . 12 . 20

Secondary DNS: 10 . 11 . 12 . 21

REMOTE AUTHENTICATION INTEGRATION

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

Integration: ○ Enabled ● Disabled

Session Timeout: 0

Password:

INTERNAL REPORT MANAGER LISTEN PORT

1. Click "**Setup Network Connection**".
2. Click "**Configure Internet Connection**".
3. Enter IP Address Settings and click "**Save**".

Enter the iBoss IP Address that was determined above and click "**Save**". You will be prompted for a reboot, click OK and the iBoss will reboot with the new network settings.

At this point, unplug your computer from the iBoss Interface and return your computer to its original IP Address configuration (either DHCP or static) and plug your computer back into the network.

3.2 Configure Initial iBoss Settings Before Deploying iBoss Inline

Once the iBoss has its IP Address configured, you can start configuring its initial integration settings. It is recommended that these settings are configured while the iBoss is not inline to minimize interruption on the network.

NOTE	Configure iBoss initial settings before putting the iBoss inline on your network. To do this, simply connect the LAN port (or Management port if iBoss has a management interface) to the network.

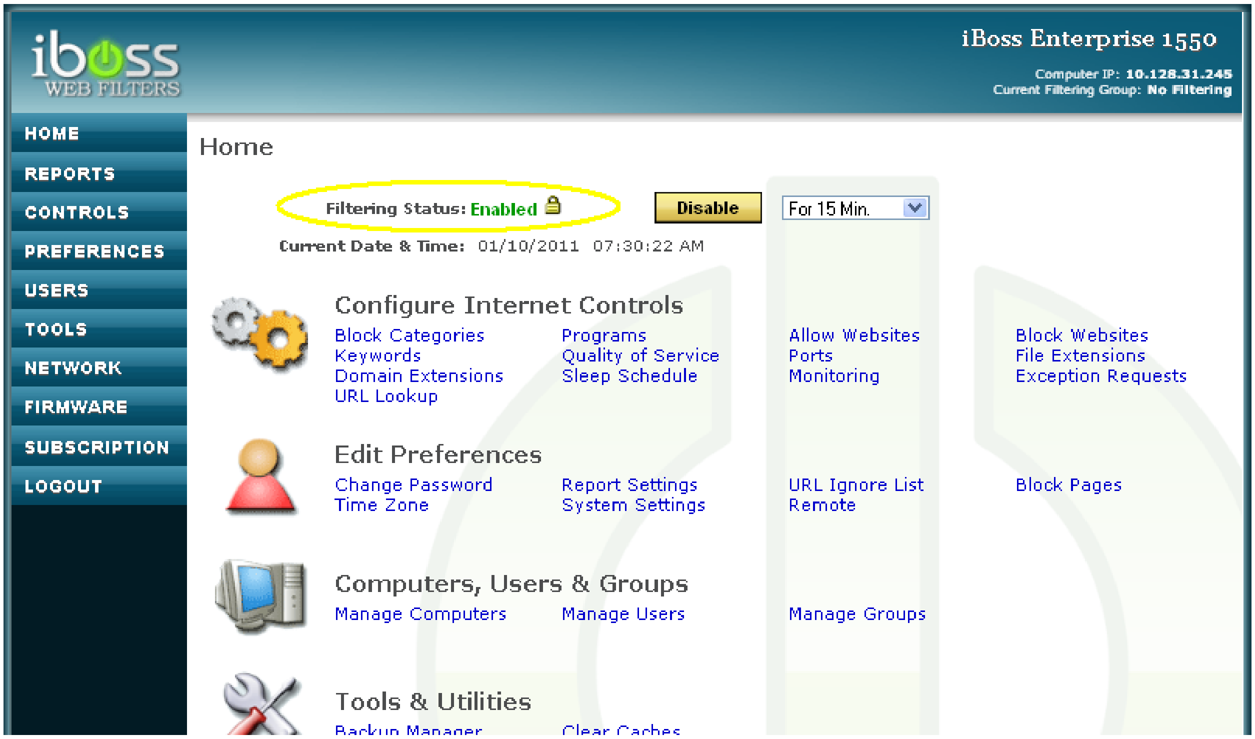
Connect the iBoss LAN port (or management port if iBoss is equipped with a management port) to the network switch. If you have configured the iBoss IP Address on a network with VLANs, make sure to connect the iBoss to a port on the switch that is part of the SAME VLAN as the IP Address configured for the iBoss.

Confirm your network IP Address settings worked by navigating to the IP Address you configured in the iBoss in your web browser. The home page of the iBoss should appear.

3.2.1 Confirm the iBoss is able to connect to the iBoss gateways and cloud database

The iBoss utilizes a high performance local database which is synchronized in real-time with a cloud database. The iBoss must be able to access the cloud database in order to receive its updates. The iBoss will indicate a status of "**Enabled**" under Filtering Status on the home page of the iBoss when it has successfully connected to the gateways.

The home page should look like the page below:



iBoss Enterprise 1550

Computer IP: **10.128.31.245**
Current Filtering Group: **No Filtering**

Home

Filtering Status: Enabled

For 15 Min.

Current Date & Time: 01/10/2011 07:30:22 AM

Figure 3 - iBoss Successfully Configured With Access to Gateways

Notice the "**Filtering Status**" in the figure above indicates "**Enabled**" in green.

If the "**Filtering Status**" indicates "**Connecting**…", the iBoss is having trouble connecting out of the network to the gateways.

The iBoss uses UDP ports 8000-8020 and http/https ports 80 and 443 to communicate with the iBoss gateways. The iBoss must be able to communicate out of the network on these ports. It is recommended that the firewall Access Control List (ACL) be configured to allow iBoss to communicate out of the network across all UDP and TCP ports via direct access.

Please refer to the table below for trouble shooting steps if the Filtering Status is not "**Enabled**":

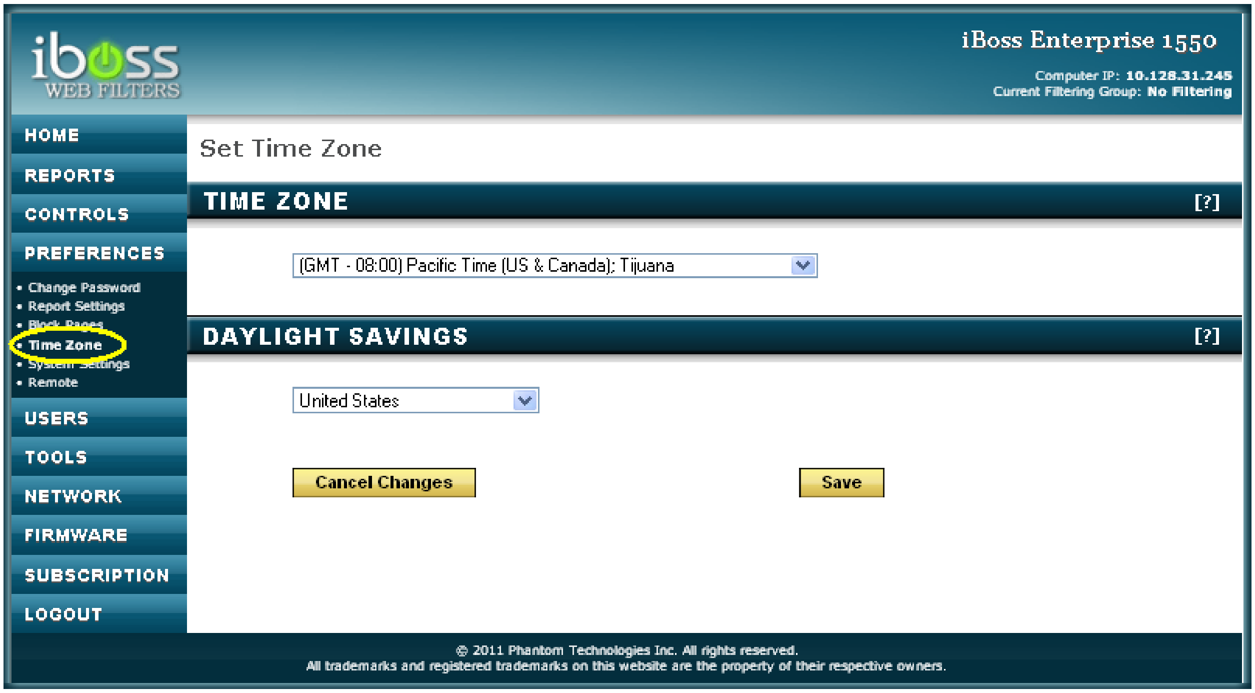
Problem	**Resolution**
Firewall is preventing or dropping UDP/TCP	Configure your firewall to allow at minimum

traffic from the iBoss out of the network.	UDP ports 8000-8020 and TCP ports 80 and 443 from the iBoss to the Internet. Alternatively, allow all traffic originating from the iBoss filter to the Internet through the firewall.
iBoss Network Settings are not correct	The iBoss network settings configured is not correct preventing access to the network. Check all network settings on the iBoss under Home→Setup Network Connection→Configure Internet Connection. Pay close attention to the gateway and DNS settings.
Gateway IP Address setting for iBoss is not correct	Check iBoss network settings for incorrect gateway IP Address
DNS IP Address settings for iBoss are not correct	Check iBoss network settings for incorrect DNS server IP Address settings.
iBoss is plugged into a switch network port that is not on the same VLAN as configured IP Address for iBoss	Check switch port settings to confirm port is the correct VLAN for network settings configured in iBoss.

Once the iBoss has connected to the gateways and has a filtering status of "**Enabled**", you are ready to start configuring initial configuration settings.

3.2.2 Configure the Time zone

The time zone can be configured from Home→Edit Preferences→Change Time Zone.



Set Time Zone

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

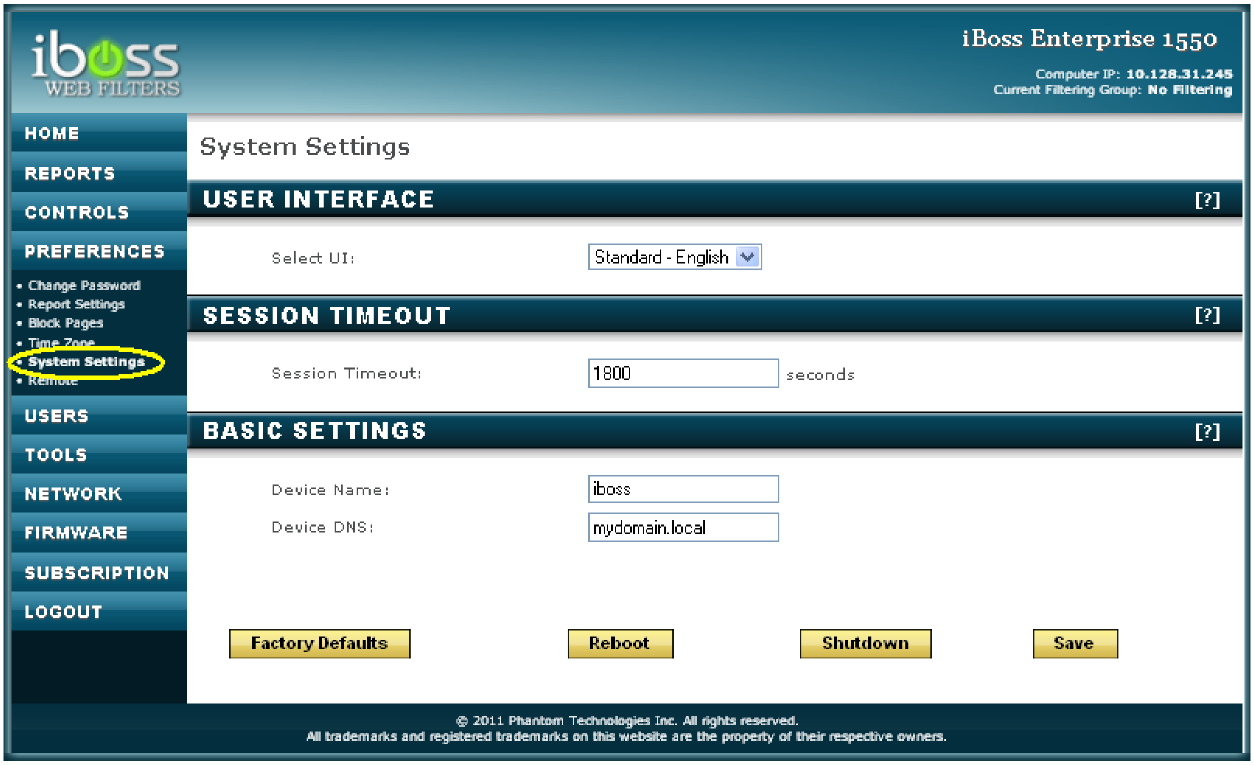
DAYLIGHT SAVINGS: United States

Figure 4 - Configure Timezone Page

Select the appropriate time zone and click Save to apply the settings.

3.2.3 Configure iBoss DNS settings

The iBoss DNS settings should be configured to match the local network domain. Go to Home→Preferences→Edit System Settings.



iBoss Enterprise 1550

Computer IP: 10.128.31.245
Current Filtering Group: No Filtering

System Settings

USER INTERFACE

Select UI: Standard - English

SESSION TIMEOUT

Session Timeout: 1800 seconds

BASIC SETTINGS

Device Name: iboss
Device DNS: mydomain.local

© 2011 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

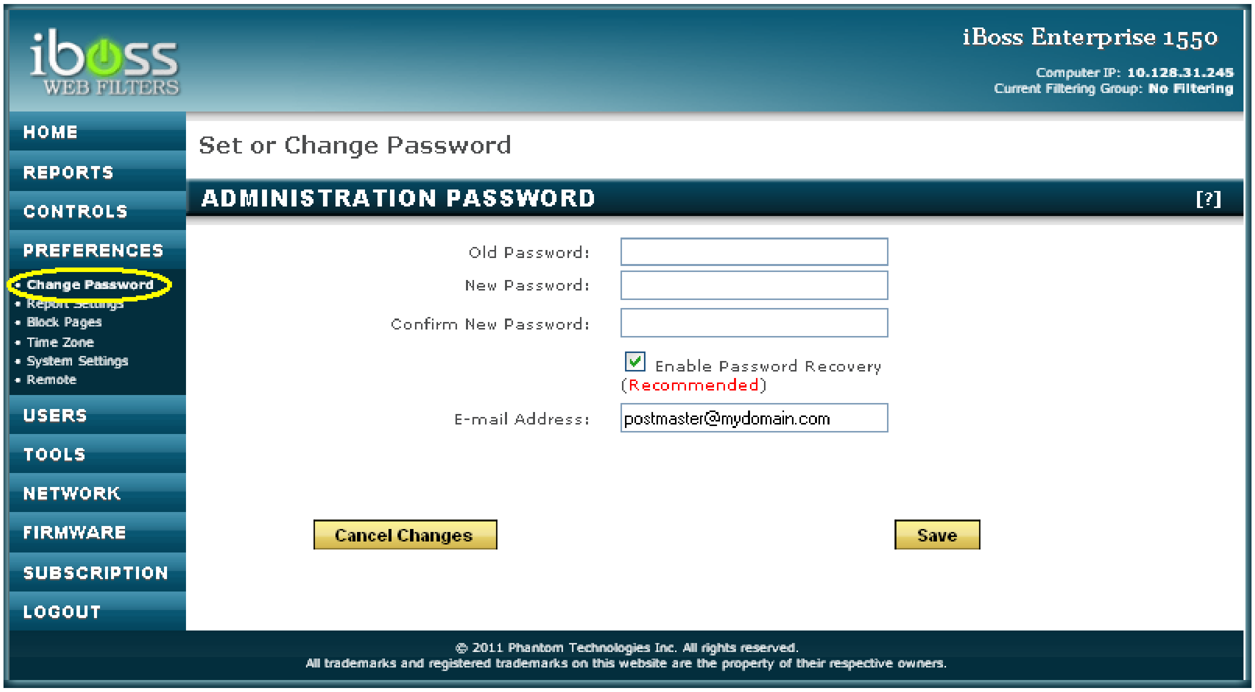
The iBoss default domain is myiboss.com. If you do not have a local DNS domain, you can leave the default configured.

Otherwise, rename the iBoss DNS settings to match your local domain. For example, if the local domain is phantomtech.local, change myiboss.com to phantomtech.local. The iBoss name is the NetBIOS name of the iBoss. You can use iboss as the iBoss's NetBIOS name if that name is not being used on the network.

In addition, add a DNS A record in your DNS server (if present) to match the iboss DNS name configured that points to the iBoss IP Address. This way you can access the iBoss by navigating to http://iboss rather than using its IP Address.

3.2.4 Set a password for the iBoss interface

Go to Home→Preferences→Set or Change Password. Enter a password for the iBoss configuration interface and click "**Save**".



iBoss Enterprise 1550

Computer IP: 10.128.31.245
Current Filtering Group: No Filtering

Set or Change Password

ADMINISTRATION PASSWORD [?]

Old Password:

New Password:

Confirm New Password:

☑ Enable Password Recovery (Recommended)

E-mail Address: postmaster@mydomain.com

© 2011 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

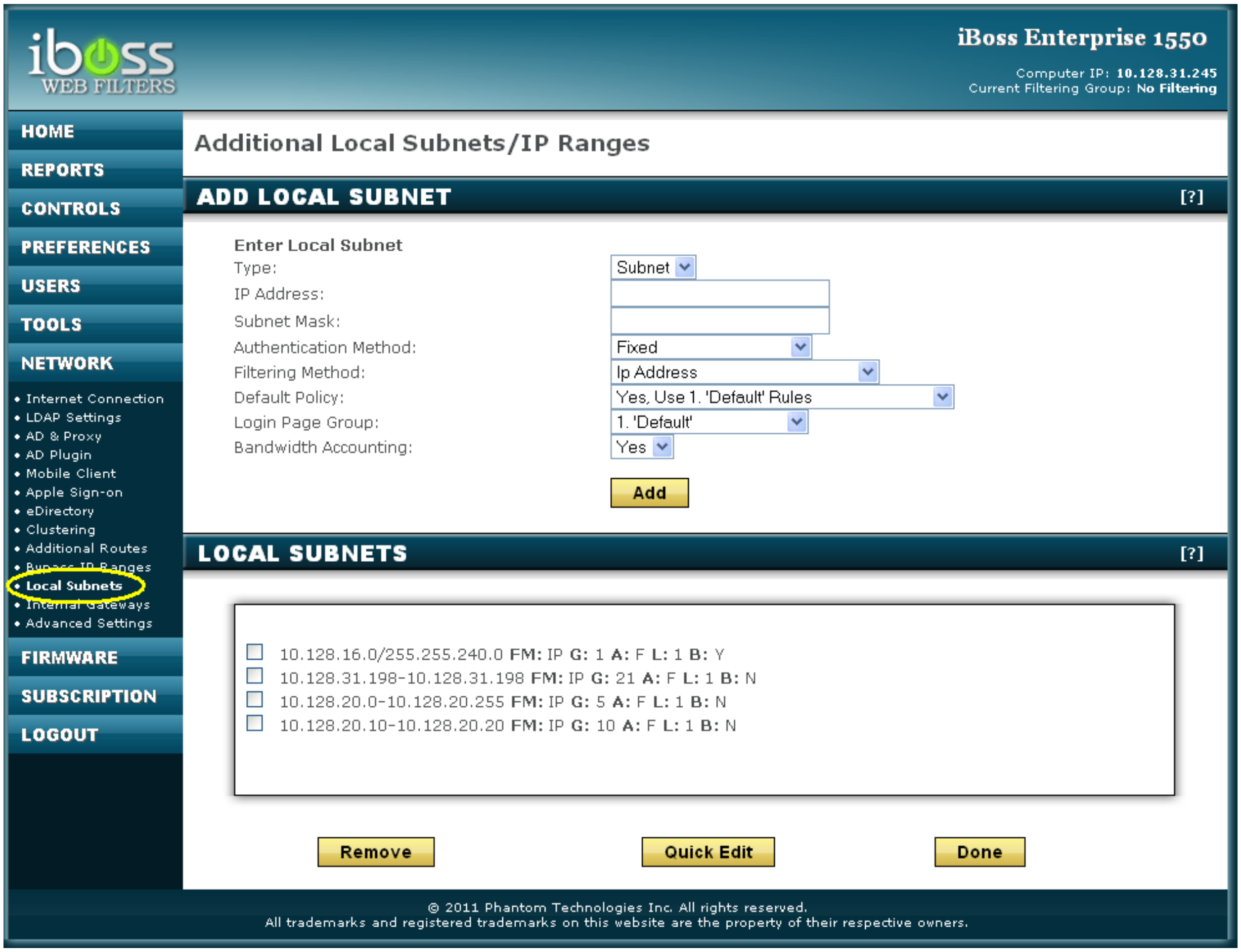
The default username for the iBoss is "**admin**". The password configured here applies to the "**admin**" user.

NOTE	The "**admin**" username is a global user. The "**admin**" username does not allow simultaneous logins. A second user using the "**admin**" username will bump the other concurrent "**admin**" user off of the iBoss interface. In order to create multiple simultaneous administrators, go to Home→Identify Computers & Users, click the "**Users**" tab and the click on "**Add New User**". Create a username and select "**Yes**" for the option "**Can Manage Filter Settings**" under the delegated administrator section. Select Full Administrator. You may want to create multiple administrators now if multiple users will be managing the iBoss at the same time.

3.2.5 Configure iBoss Local Subnets

The iBoss must determine which networks are local. The iBoss uses this information to determine which traffic to filter. The iBoss does not filter traffic between local networks and filters all traffic between the local networks and the Internet.

Navigate to Home→Setup Network Connection→Add Local Subnets. You should see the page below:



Computer IP: **10.128.31.245**
Current Filtering Group: **No Filtering**

Additional Local Subnets/IP Ranges

ADD LOCAL SUBNET

Enter Local Subnet

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

LOCAL SUBNETS

☐ 10.128.16.0/255.255.240.0 **FM:** IP **G:** 1 **A:** F **L:** 1 **B:** Y
☐ 10.128.31.198-10.128.31.198 **FM:** IP **G:** 21 **A:** F **L:** 1 **B:** N
☐ 10.128.20.0-10.128.20.255 **FM:** IP **G:** 5 **A:** F **L:** 1 **B:** N
☐ 10.128.20.10-10.128.20.20 **FM:** IP **G:** 10 **A:** F **L:** 1 **B:** N

© 2011 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

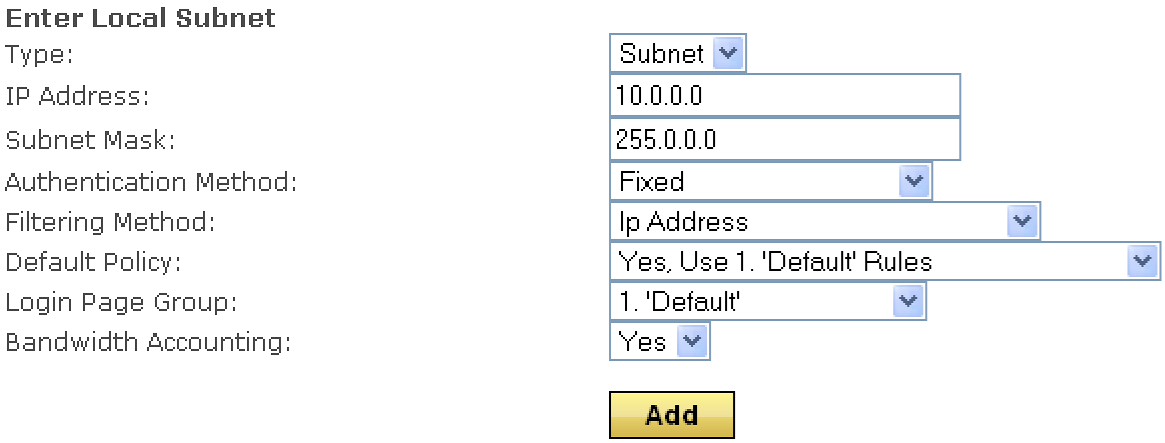
On this page, you will want to add the local subnets on your network. If your network is contained within a larger top subnet, there is no need to add all of the sub-networks. Add the top level subnet that contains the lower sub-networks.

For example, if your IP Address all fall within the 10.X.X.X network, adding the local network 10.0.0.0 with a subnet mask of 255.0.0.0 will include all private networks without the need to add each individual networks.

NOTE	Add the top level local subnet instead of adding each individual local subnet. For example, 10.0.0.0 with subnet mask 255.0.0.0, or 192.168.0.0 with subnet mask 255.255.0.0.

Adding local subnets allows you to specify what the default policy should be for each subnet on the network. If you have multiple subnets, you can specify different policies for each subnet.

If your network is based on the 10.X.X.X private network range, the following settings below will provide adequate coverage for the entire network:



Enter Local Subnet

Type:	Subnet
IP Address:	10.0.0.0
Subnet Mask:	255.0.0.0
Authentication Method:	Fixed
Filtering Method:	Ip Address
Default Policy:	Yes, Use 1. 'Default' Rules
Login Page Group:	1. 'Default'
Bandwidth Accounting:	Yes

Figure 5 - Adding local subnets

The following table describes the settings available while adding local subnets:

Option	**Description**
Type	Subnet or Range. Select "**Subnet**" to add your local subnets. You can specify a range, but it is recommended that you add at least your top level subnet as a "**Subnet**" first. Each subnet/range can have a different default policy. If you would like to specify a different default policy for a range within the network, add the top level subnet and then add a range below that subnet to specify the range policy.
IP Address	The base IP for the subnet
Subnet Mask	The subnet Mask for the subnet
Authentication Method (Default: Fixed)	Fixed or Active Directory/NTLM. 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). Note that 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.
Filtering Method (Default: IP Address)	IP Address, MAC Address, or MAC Address

	Through Gateway. The recommended value is IP Address, which means that IP Addresses will be used while identifying network packets on the network. MAC Address will only work on flat networks where there is no internal router or internal layer 3 switch on the network. The MAC address in the packet is used for identification in this mode. MAC Address through Gateway is an advanced option not covered in this deployment guide. It allows the identification via MAC Address even on networks with internal routers and gateways. Select "**IP Address**" for this option.
Default Policy (Default: Group 1)	Select the default filtering group you would like for the subnet. You can have multiple filtering groups for each subnet.
Login Page Group (Default: Same as default policy selection)	Each subnet can have customized login pages. It is recommended you select the same value you select for the default policy.
Bandwidth Accounting (Default: Yes)	Whether or not bandwidth should be accounted for on this subnet. If you add a subnet that is contained within another subnet that already has bandwidth accounting set to yes, set this option to No. This indicates whether bandwidth should be accounted for on the subnet or range. If bandwidth is already being accounted by another subnet rule higher in the list, do not set this to yes as bandwidth will be accounted for twice.

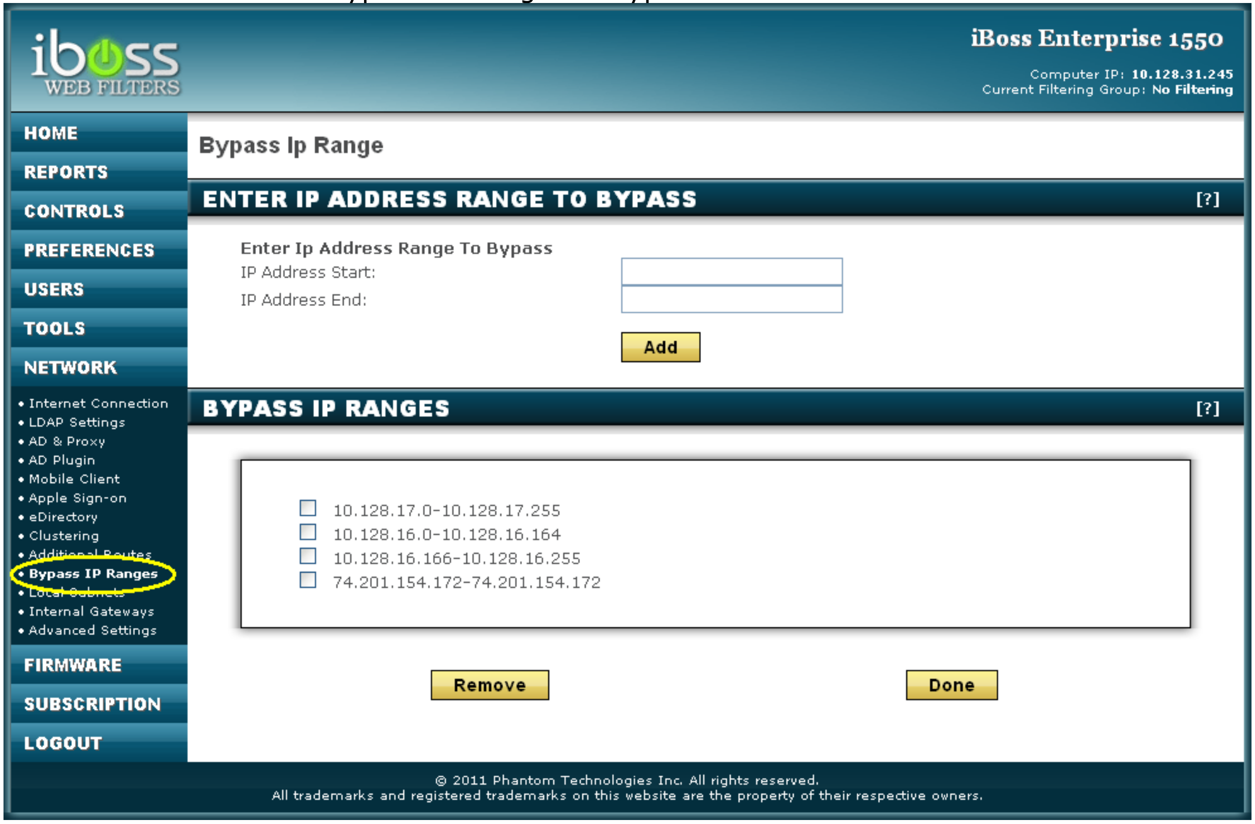
NOTE	You can add multiple subnets. In addition you can add a top level subnet and map it to a default policy and then add multiple subnets contained within the top level subnet below it and specify a different policy for those subnets. The iBoss will always start at the top of the list when determining the default policy to apply to an IP Address on the network and will work its way all the way down the subnet list finding more specific matches as it works its way down the list.

Once you have added your top level subnets, move on to the next step.

3.2.6 Bypass IP Ranges which contain servers and non-filtered nodes

The next step involves bypassing all IP Addresses that do not require network filtering and should be bypassed completely from filtering. It is recommended that all servers be bypassed, including mail servers, domain controllers, DNS servers, etc. In this section you are allowed to specify ranges, so if your servers are within a specific range of IP Addresses, you can exclude the entire range which will bypass all of the servers on that range.

Go to Home→Network→Bypass IP Ranges to bypass servers.



iBoss Enterprise 1550

Computer IP: 10.128.31.245
Current Filtering Group: No Filtering

Bypass Ip Range

ENTER IP ADDRESS RANGE TO BYPASS

Enter Ip Address Range To Bypass
IP Address Start:
IP Address End:

BYPASS IP RANGES

□ 10.128.17.0-10.128.17.255
□ 10.128.16.0-10.128.16.164
□ 10.128.16.166-10.128.16.255
□ 74.201.154.172-74.201.154.172

© 2011 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Simply enter the start and end IP Address and click add to bypass the IP Address.

NOTE	If you are bypassing a single IP Address, use the same Start and End IP Address.

3.3 Physical installation of the iBoss onto the network

This section describes the physical installation of the iBoss on your network. If you are going to integrate with Active Directory or eDirectory, you may choose to configure those settings first before placing the iBoss inline on your network. If you are integrating with Active Directory or eDirectory, skip this section and visit the appropriate Active Directory/eDirectory section and then return to this section once you have completed the steps described in those sections.

NOTE	If you are integrating with Active Directory or eDirectory, visit those sections first and return to this section once you are ready to install the iBoss on the network. If you are not integrating with Active Directory or eDirectory, continue with this section for installation instructions.

There are two primary physical placement options for installing the iBoss on your network. The first method is inline and the second method is out of band/non-inline.

In order to install the iBoss in a non-inline deployment, a management network interface is required.

3.3.1 Inline Installation

When installed inline, the iBoss is placed between the inner switch and the outer firewall. Typically there is a single cable connected between the core switch and the outer firewall on the network. The iBoss will be placed between the inner switch/router and outer firewall.

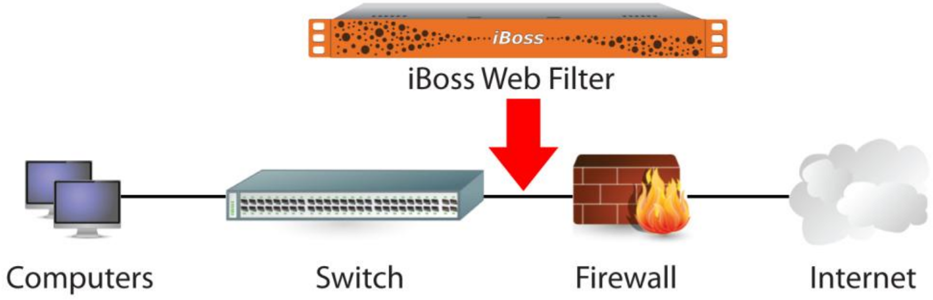


Figure 6 - iBoss Network Placement

To install the iBoss, the network cable going between the inner switch and outer firewall is removed. A cable is run from the inner switch to the LAN port of the iBoss. A second cable is run from the WAN port of the iBoss to the outer firewall.

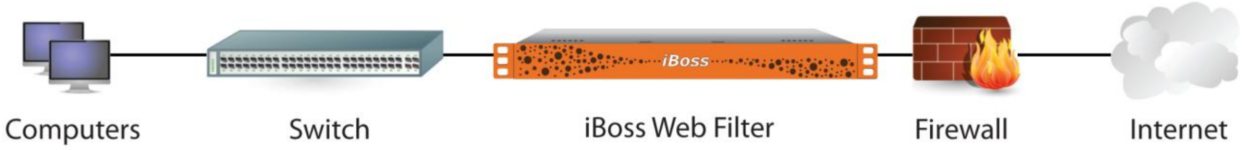


Figure 7 - Inline Installation

A detailed diagram of the back of the iBoss is shown below showing the cables and their placement.

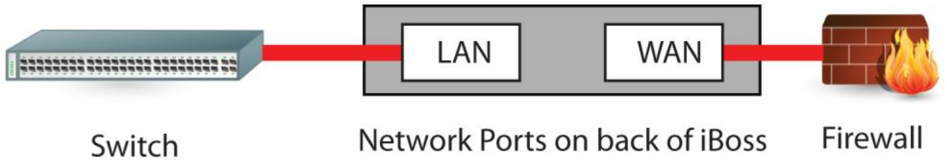


Figure 8 - Cable Placement

NOTE	Before placing the iBoss inline, verify whether the network ports connecting the inner switch to the outer firewall are configured for fixed duplex settings (for

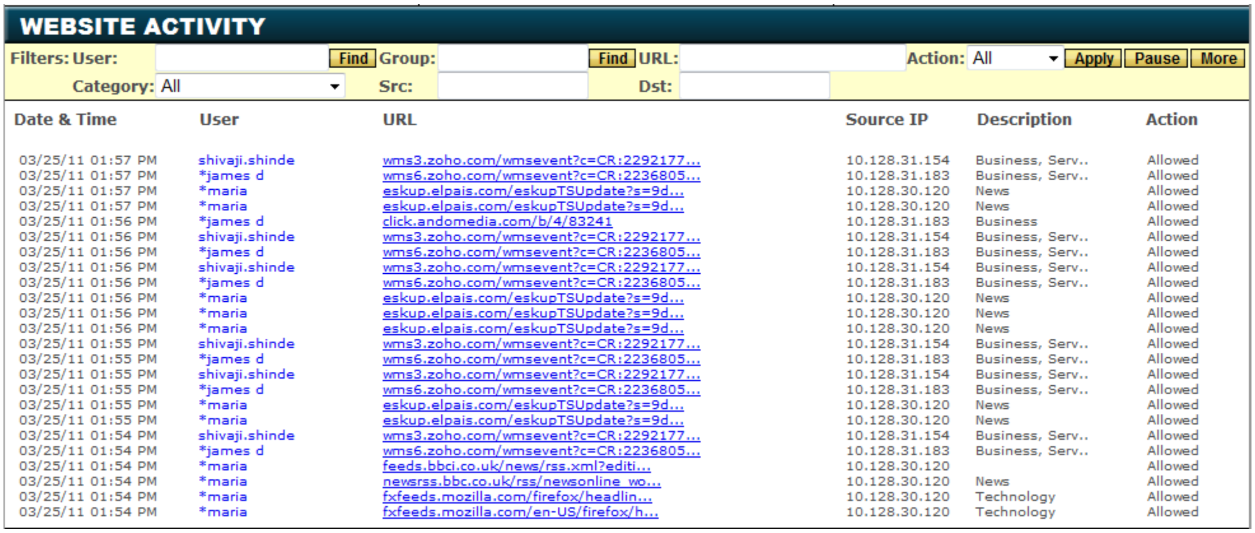
	example 100Mbps full duplex, no auto-negotiate). The iBoss network ports default to auto-negotiate 10/100/1000 Mbps. This will conflict if the network ports between the switch and the firewall are configured for fixed duplex settings.

To minimize downtime, install the iBoss near the inner switch and firewall. Then follow these instructions:

1. Power on the iBoss and wait for it to fully boot.
2. Once the iBoss has fully booted, disconnect the cable connected between the inner switch and firewall.
3. Connect a network cable between the inner switch and the LAN port of the iBoss. Use the same port of the inner switch that was connected to the firewall prior to installing the iBoss.
4. Connect a network cable between the outer firewall and the WAN port of the iBoss.

The network should come back up within 10-30 seconds.

Navigate to the iBoss reports. You should see URLs showing up at the bottom of the Current Activity section.



Date & Time	User	URL	Source IP	Description	Action
03/25/11 01:57 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:57 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:57 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:57 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:56 PM	*james d	click.andomedia.com/b/4/83241	10.128.31.183	Business	Allowed
03/25/11 01:56 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:56 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:56 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:56 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:56 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:56 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:56 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:55 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:55 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:55 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:55 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:55 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:55 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:54 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:54 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:54 PM	*maria	feeds.bbci.co.uk/news/rss.xml?editi...	10.128.30.120		Allowed
03/25/11 01:54 PM	*maria	newsrss.bbc.co.uk/rss/newsonline_wo...	10.128.30.120	News	Allowed
03/25/11 01:54 PM	*maria	fxfeeds.mozilla.com/firefox/headlin...	10.128.30.120	Technology	Allowed
03/25/11 01:54 PM	*maria	fxfeeds.mozilla.com/en-US/firefox/h...	10.128.30.120	Technology	Allowed

Figure 9 - Current Activity

Listed below are possible problems you may encounter while installing the iBoss inline.

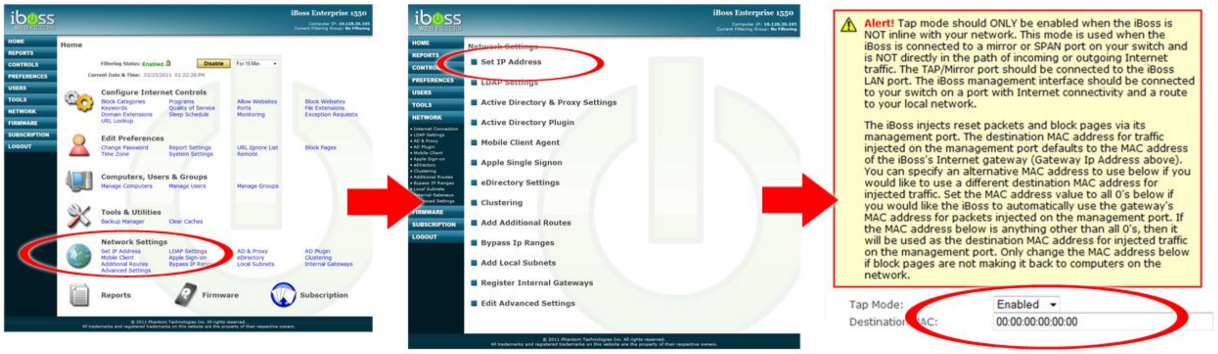
Symptom	Solution
After installing the iBoss, there is high packet loss and the network seems sluggish. You can confirm high packet errors or collisions by logging into your switch and looking at the status for the network port the iBoss is attached to.	The network ports between the inner switch and the outer firewall are configured for fixed duplex settings. Confirm the duplex settings and adjust the iBoss duplex settings via the serial console port to match. Connect your computer to the iBoss serial

	RS-232 console port with the provided cable and follow the menu options to configure the port settings to the fixed duplex settings configured on the switch and firewall.
You cannot navigate to the iBoss configuration web interface after installing the iBoss, but the Internet is accessible.	The routes are not configured properly on the iBoss. The iBoss is not routing packets properly back into the network. This scenario is typical in cases where the inner switch is also the gateway for most computers on the network and performs routing functions. Configure the iBoss's gateway IP Address to point to the inner switch/router instead of the outer firewall. Alternatively, you can add a route via the Home->Setup Network Connection->Add Additional Routes section. Create a route rule that routes all local traffic back to the inner router while leaving the gateway IP Address of the iBoss set to the outer firewall. A typical route might look like this: IP: 10.0.0.0 Subnet: 255.0.0.0 Gateway: 10.0.0.2 (Inner switch firewall)

3.3.2 Non-inline installation (Out of band filtering)

This section describes installing the iBoss in a non-inline configuration. A management interface is required for this configuration.

Log into the iBoss configuration interface and navigate to Home->Setup Network Connection->Configure Internet Connection:
Enable the Tap Mode option on the page and click Save:



Alert! Tap mode should ONLY be enabled when the iBoss is NOT inline with your network. This mode is used when the iBoss is connected to a mirror or SPAN port on your switch and is NOT directly in the path of incoming or outgoing Internet traffic. The TAP/Mirror port should be connected to the iBoss LAN port. The iBoss management interface should be connected to your switch on a port with Internet connectivity and a route to your local network.

The iBoss injects reset packets and block pages via its management port. The destination MAC address for traffic injected on the management port defaults to the MAC address of the iBoss's Internet gateway (Gateway Ip Address above). You can specify an alternative MAC address to use below if you would like to use a different destination MAC address for injected traffic. Set the MAC address value to all 0's below if you would like the iBoss to automatically use the gateway's MAC address for packets injected on the management port. If the MAC address below is anything other than all 0's, then it will be used as the destination MAC address for injected traffic on the management port. Only change the MAC address below if block pages are not making it back to computers on the network.

Tap Mode: Enabled
Destination MAC: 00:00:00:00:00:00

Figure 10 - Configure Tap Mode

Figure 11 - Tap Mode Option

Once the iBoss reboots, the iBoss will be configured for a mirror deployment.

When in a mirror deployment, the iBoss only uses two ports, the Management port and the LAN port. The management port is used for accessing the iBoss configuration interface. The LAN port is what the iBoss uses to sniff network traffic from the port on your switch that is configured as a destination port of monitor/mirror/span configuration.

Refer to your switch manual to configure a monitor/mirror/span port. The source of the SPAN/Monitor port is the primary VLAN or network interface carrying all traffic in and out of the network. The destination port of the Monitor port should be an available port on the switch where all traffic will be mirrored to.

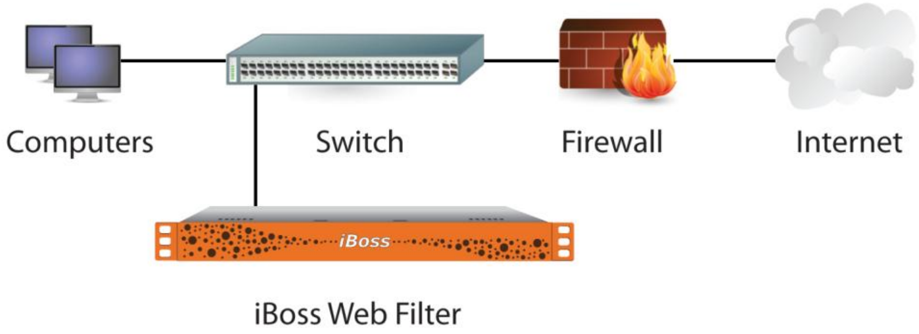


Figure 12 - Mirror/Tap Configuration

Connect the Management port of the iBoss to a port on the switch on the correct VLAN for the IP Address that was configured in the iBoss. You should be able to access the iBoss interface.

Connect the LAN port of the iBoss to the switch port that was configured as the destination port of the Monitor configuration.

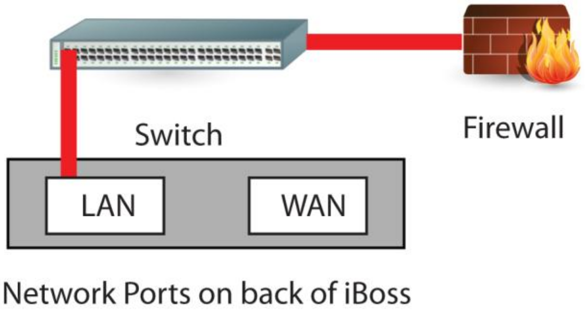
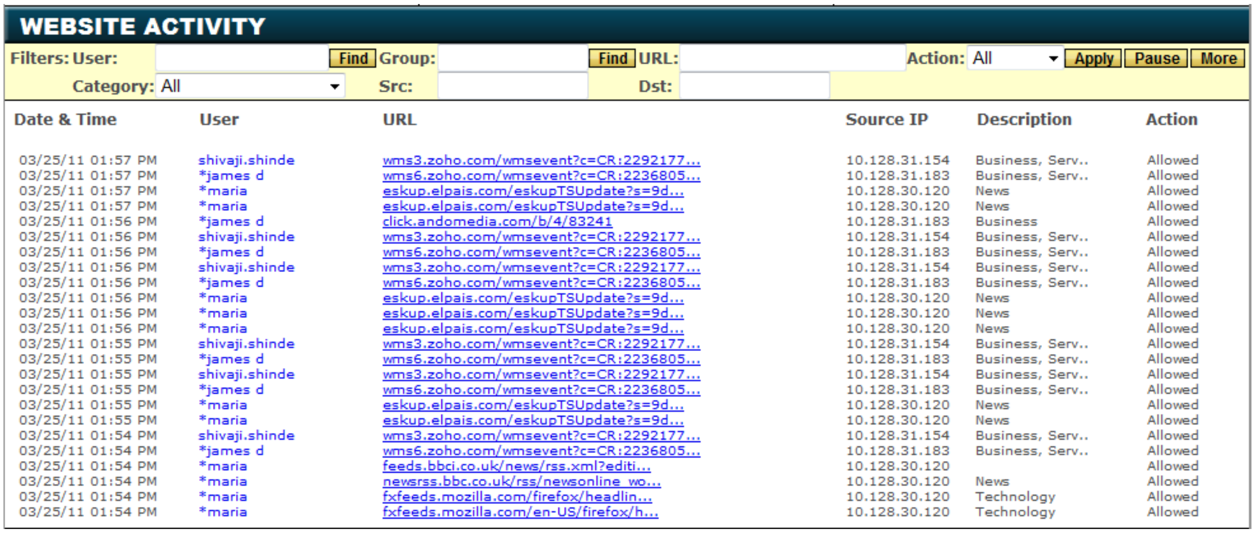


Figure 13 - Mirror/Tap Cable Configuration

Navigate to the iBoss reports. You should see URLs showing up at the bottom of the Website Activity section.



WEBSITE ACTIVITY

Filters: User: [Find] Group: [Find] URL: Action: All [Apply] [Pause] [More]
Category: All Src: Dst:

Date & Time	User	URL	Source IP	Description	Action
03/25/11 01:57 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:57 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:57 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:57 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:56 PM	*james d	click.andomedia.com/b/4/83241	10.128.31.183	Business	Allowed
03/25/11 01:56 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:56 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:56 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:56 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:56 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:56 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:56 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:55 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:55 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:55 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:55 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:55 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:55 PM	*maria	eskup.elpais.com/eskupTSUpdate?s=9d...	10.128.30.120	News	Allowed
03/25/11 01:54 PM	shivaji.shinde	wms3.zoho.com/wmsevent?c=CR:2292177...	10.128.31.154	Business, Serv..	Allowed
03/25/11 01:54 PM	*james d	wms6.zoho.com/wmsevent?c=CR:2236805...	10.128.31.183	Business, Serv..	Allowed
03/25/11 01:54 PM	*maria	feeds.bbci.co.uk/news/rss.xml?editi...	10.128.30.120		Allowed
03/25/11 01:54 PM	*maria	newsrss.bbc.co.uk/rss/newsonline_wo...	10.128.30.120	News	Allowed
03/25/11 01:54 PM	*maria	fxfeeds.mozilla.com/firefox/headlin...	10.128.30.120	Technology	Allowed
03/25/11 01:54 PM	*maria	fxfeeds.mozilla.com/en-US/firefox/h...	10.128.30.120	Technology	Allowed

Figure 14 - Current Activity

Symptom	Solution
No URLs are showing up in the current activity section.	(1) The iBoss is not configured in TAP mode. Navigate to Home->Setup Network Connection->Configure Internet Connection and confirm the iBoss is configured in TAP mode. (2) The LAN port of the iBoss is not connected to the destination switch port of the monitor/span/mirror configuration. (3) The switch monitor/mirror/span port is not configured properly. Verify that your switch settings are correct and traffic is being sent to the monitor/span/mirror port.

3.4 Relation Between iBoss Filtering Groups and Directory Filtering Groups (Active Directory/eDirectory)

This section describes the iBoss filtering groups and their relation to Active Directory, eDirectory, and LDAP server groups.

3.4.1 Configure Filtering Groups

Following the iBoss network installation section is a high level description of how iBoss filtering group membership is related to Active Directory and eDirectory group membership (or other LDAP directory server group membership).

A detailed description of deploying the iBoss in an Active Directory or eDirectory environment is described afterwards.

The iBoss contains multiple individual filtering groups that can be mapped to your directory server groups. The mapping occurs in a one-to-one fashion, with a filtering group in the iBoss mapping to a filtering group in the directory server.

iBoss Filtering Group	Directory Server Group
Students	Students
Staff	Staff
Police Dept	Police Dept
IT Staff	IT Staff

For each group in your directory server that you would like filtering policy applied, the iBoss will be configured to contain the same named filtering group. When filtering policy is applied to the group in iBoss, that policy will apply to anyone that is part of that group in the directory server.

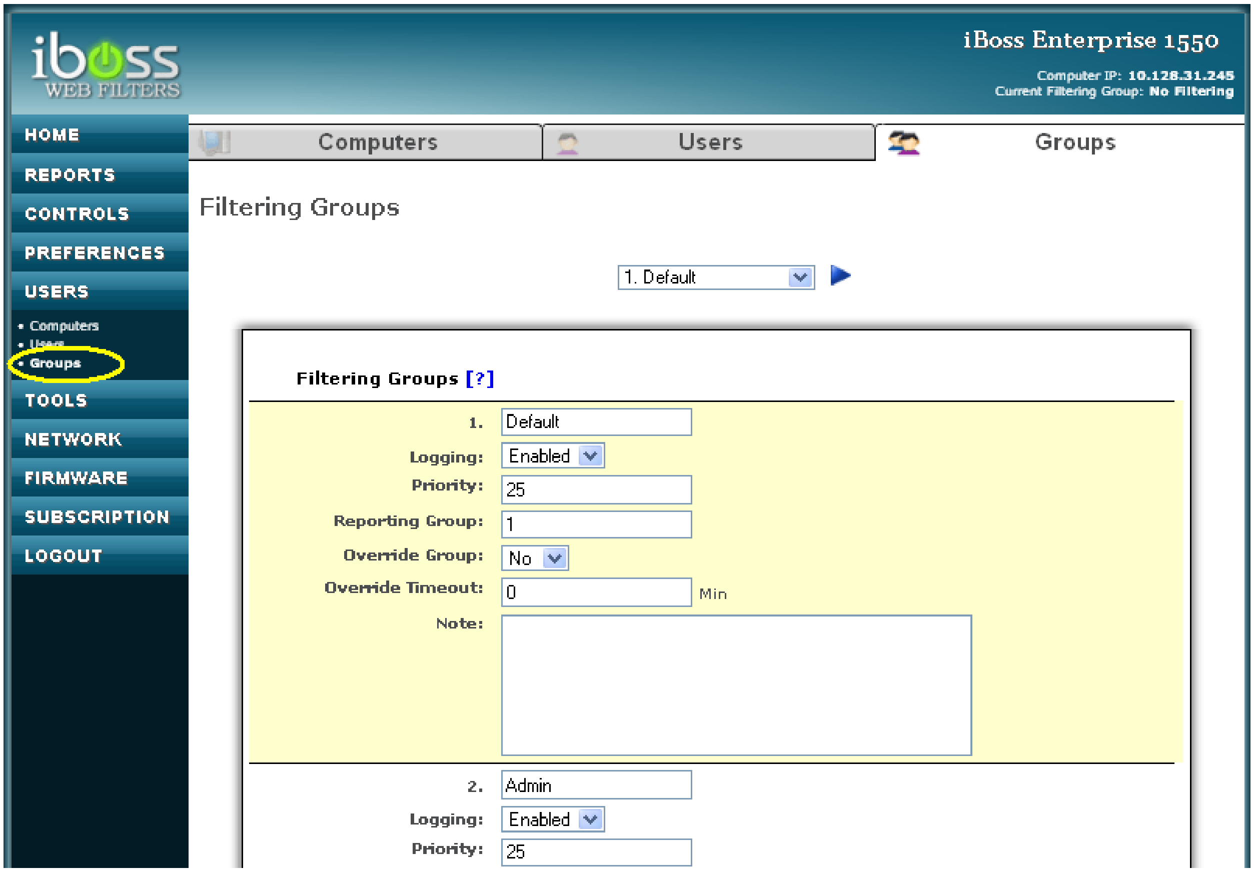
The iBoss will associate the filtering group transparently when the user logs into their workstation. The iBoss determines which filtering group should be applied by comparing all of the group names a user is a member of in the directory server to the group names in the iBoss. When the iBoss finds a group name match, it associates the filtering group to the user.

The different filtering groups within the iBoss do not inherit from each other. Each group is independent which allows simplicity when applying filtering policy as well as determining filtering policy when dealing with a large number of groups and rules.

In general regardless of directory server, you name the iBoss Groups with the same name as the group you would like to match in the directory server (LDAP, Active Directory, eDirectory, etc).

NOTE	The iBoss depends on direct group membership. Nested groups in general are not supported unless they show up directly as a group in the user's profile (such as the memberOf tab in Active Directory or groupMembership tab in eDirectory).

To find the filtering groups in iBoss, go to Home→Users→Groups Tab. The Groups page is shown below:



iBoss Enterprise 1550

Computer IP: 10.128.31.245
Current Filtering Group: No Filtering

Filtering Groups

1. Default

Filtering Groups

1. Default
Logging: Enabled
Priority: 25
Reporting Group: 1
Override Group: No
Override Timeout: 0 Min
Note:

2. Admin
Logging: Enabled
Priority: 25

You will want to look through your directory server and find the groups that you would like to use for filtering. Once you determine which groups will be used, rename the iBoss groups on the above page to match.

Remember that there is already a default filtering group for the subnet. You may want to save that group for the default policy for the subnet. Since it is the default group, you do not need this group to match a filtering group name in your directory server for users with the default policy as they will automatically get this policy even if they do not have a matching directory server group.

NOTE	Typically the default group in a school environment is used for students. There is no need to assign students to a matching directory server group as the default group for the subnet will be assign to them. Additional groups for staff and IT are common. In a government or business environment, the default group is typically assigned to standard employees. There is no need to assign a matching directory server group for employees as the default subnet policy will apply to them. Additional groups for staff and IT are common.

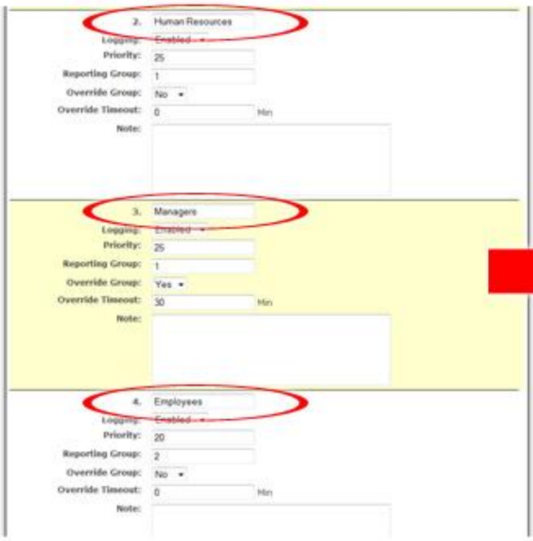
NOTE	If a user has more than one group that matches between the directory server and the iBoss, the group that is assigned the highest priority (highest number) will be the group that matches for filtering policy. The iBoss uses priority numbers to resolve cases where a user belongs to more than one group and always chooses the group with the highest number.

3.4.2 Look through the directory server and rename iBoss groups to match

The first step is to look through your directory server to find groups that you would like to use to match to iBoss filtering groups. Remember that a user must be a direct member of a group.

For example, in a school environment using Active Directory, find a teacher in the Active Directory server's "**Computers & Users**" and go to that user's properties. Then select the "**memberOf**" tab for the user. If the user is a member of a group named "**teachers**" and this group appears for all users that are teachers, then this will be a good group to use for a filtering group match.

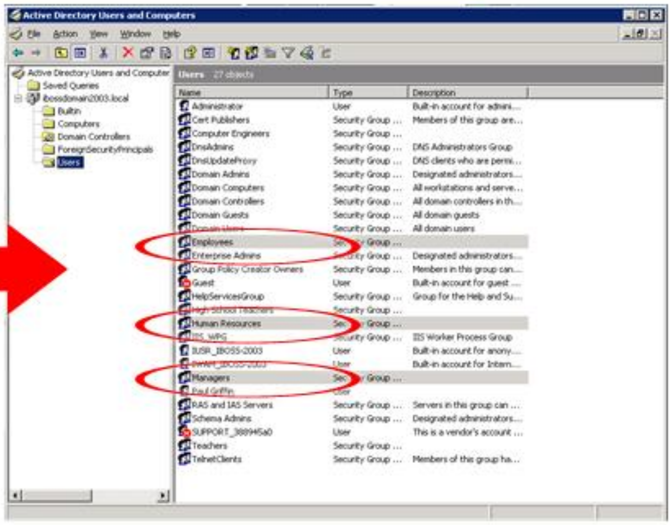
Once you have determined which groups you will use, rename the iBoss group names to match exactly to the group names in the directory server that will be used for assigning filtering policy.



2. Human Resources
Logging: Enabled
Priority: 25
Reporting Group: 1
Override Group: No
Override Timeout: 0 Min
Note:

3. Managers
Logging: Enabled
Priority: 25
Reporting Group: 1
Override Group: Yes
Override Timeout: 30 Min
Note:

4. Employees
Logging: Enabled
Priority: 20
Reporting Group: 2
Override Group: No
Override Timeout: 0 Min
Note:



Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
ibossdomain2003.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Users 27 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
Computer Engineers	Security Group ...	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Employees	Security Group ...	
Enterprise Admins	Security Group ...	Designated administrators...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServicesGroup	Security Group ...	Group for the Help and Su...
High School Teachers	Security Group ...	
Human Resources	Security Group ...	
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_IBOSS-2003	User	Built-in account for anony...
IWAM_IBOSS-2003	User	Built-in account for Intern...
Managers	Security Group ...	
Paul Griffin	User	
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_388945a0	User	This is a vendor's account ...
Teachers	Security Group ...	
TelnetClients	Security Group ...	Members of this group ha...

NOTE	The filtering group names in the iBoss must match exactly to the group names on your directory server that will be used for filtering.

Don't forget to hit "**Save**" when done. There are 5 groups per page, but you can scroll to the right or left with the arrows near the top of the page to reach more groups. You can also use the drop down list near the top of the page to reach more groups.

Once you have renamed your groups, follow the steps below to integrate with your directory server. Jump to the section (Active Directory or eDirectory) that applies to your scenario.

3.5 Integrating with Active Directory

The iBoss can integrate with Active Directory in order to apply filtering policy depending on Active Directory group membership. This section describes integrating the iBoss with Active Directory in order to apply filtering group policy transparently.

The iBoss offers two methods to identify computers based on group membership in Active Directory. Only one is required and is a matter of preference. Following is an overview of the two methods. After deciding which method fits your preference, jump to that section to continue.

Authentication	Description	Advantages	Disadvantages
Logon Scripts (method one)	Group Policy Object that executes a script in the background that authenticates the user to the iBoss when a user logs into their station.	-Quickly add script to any existing GPO script you may already have. -Will automatically replicate across all Active Directory servers in the domain if they are replicated servers.	-Will only support networks that have a single domain forest. -Typically will not work on computers with Internet Explorer 6 or earlier versions due to a single sign-on/NTLM bug. -Will only work for Windows computers.
AD Plug-in (method two)	Installs on the Active Directory server which sends authentication information to the iBoss when a user logs onto the domain.	-Can work with Mac, Windows, and Linux computers that authenticate to the Active Directory Domain. -One point of troubleshooting on server rather than each computer. -Can be installed on different domain controllers individually allowing multiple domain forests to be used with the iBoss. -Will work on networks that have many computers with Internet Explorer 6.	-Must be installed on every domain controller to which users authenticate. -2003/2008 Domain Controllers or above required. (no Win2000) -Must be installed on every Domain Controller a user may authenticate against.

3.5.1 Active Directory Group Policy Object (GPO) Logon/Logoff Scripts Overview

This method involves adding or modifying an existing Group Policy Object (GPO) to add an iBoss login script and logoff script. When the user logs on, a script runs and authenticates the user. When the user logs off, a script runs and disassociates the filtering policy from the user.

Once added to a GPO, the script replicates across all domain controllers.

An advantage to the logon script is that it will automatically replicate across all Active Directory servers in the domain if they are replicated servers. A disadvantage to the logon script is that it will only support networks that have a single domain forest.

3.5.2 Active Directory Plug-in Overview

If logon/logoff scripts are not desired, you can use an Active Directory plug-in which installs on the Domain Controller and sends authentication information to the iBoss whenever a user logs onto the domain.

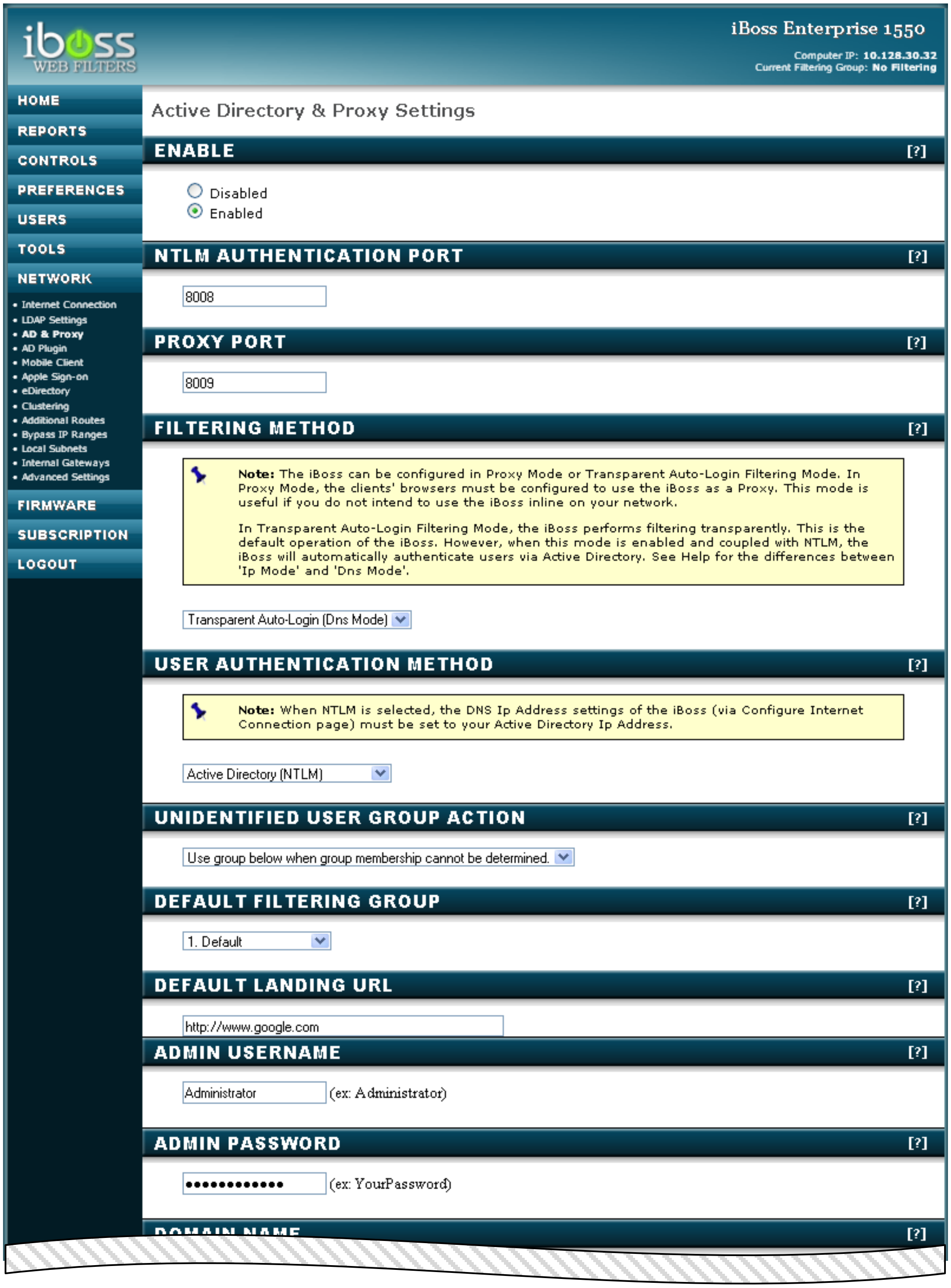
The advantages to this method are that it will work on networks that have many computers with IE6 installed. Since IE6 does not support NTLM/Single Sign-on reliably (which the logon scripts rely on), the plug-in will work in these environments.

A second advantage to the plug-in is that it supports networks that have multiple domain forests.

The disadvantage to the plug-in method is that it must be installed on every domain controller to which users authenticate.

3.5.3 Configuring the Active Directory Logon/Logoff scripts

Navigate to Network→Active Directory & Proxy Settings.



Active Directory & Proxy Settings

ENABLE [?]

○ Disabled
● Enabled

NTLM AUTHENTICATION PORT [?]

8008

PROXY PORT [?]

8009

FILTERING METHOD [?]

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

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

Transparent Auto-Login (Dns Mode)

USER AUTHENTICATION METHOD [?]

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

Active Directory (NTLM)

UNIDENTIFIED USER GROUP ACTION [?]

Use group below when group membership cannot be determined.

DEFAULT FILTERING GROUP [?]

1. Default

DEFAULT LANDING URL [?]

http://www.google.com

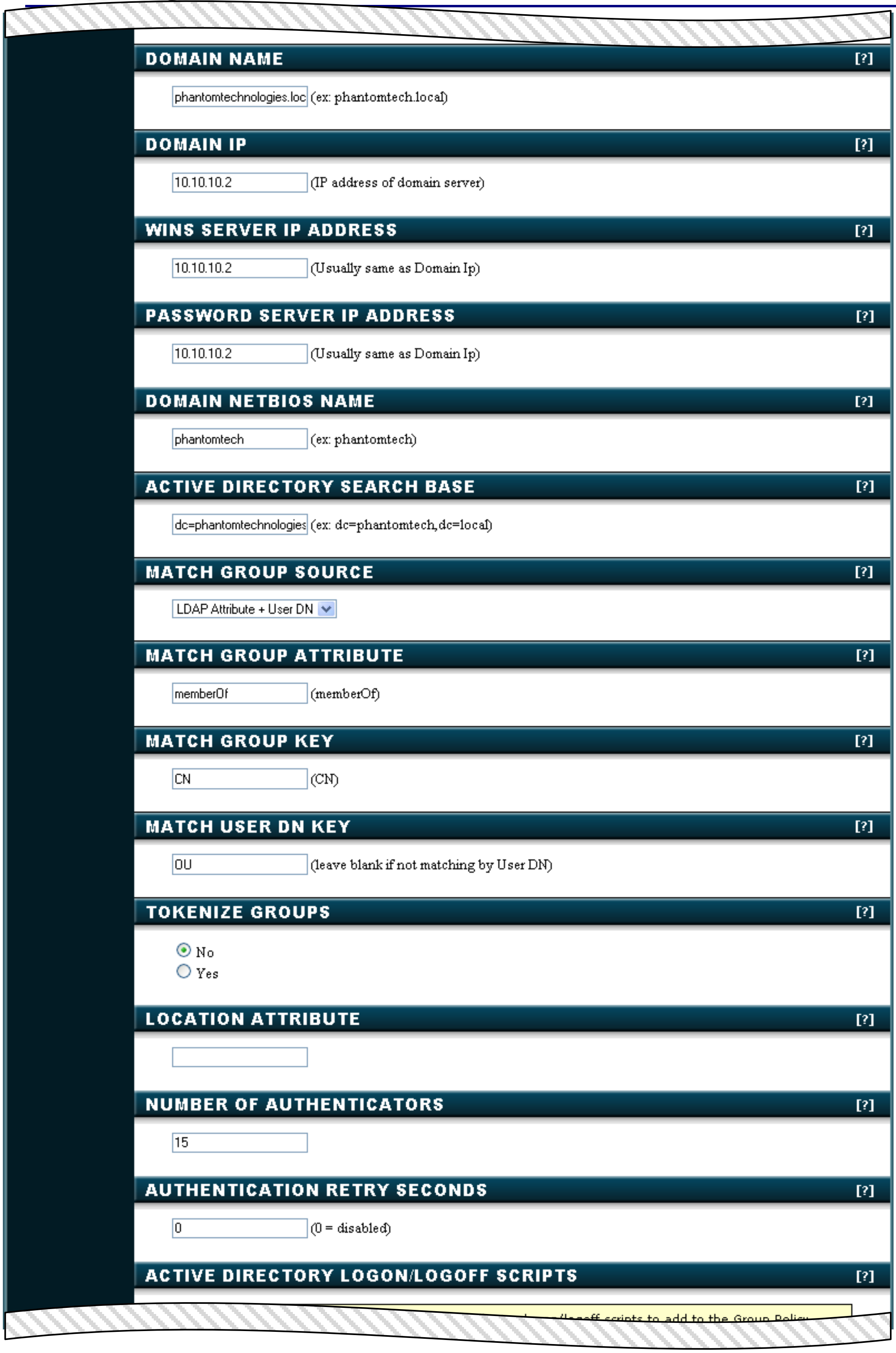
ADMIN USERNAME [?]

Administrator (ex: Administrator)

ADMIN PASSWORD [?]

••••••••••••• (ex: YourPassword)

DOMAIN NAME [?]



DOMAIN NAME [?]

phantomtechnologies.loc (ex: phantomtech.local)

DOMAIN IP [?]

10.10.10.2 (IP address of domain server)

WINS SERVER IP ADDRESS [?]

10.10.10.2 (Usually same as Domain Ip)

PASSWORD SERVER IP ADDRESS [?]

10.10.10.2 (Usually same as Domain Ip)

DOMAIN NETBIOS NAME [?]

phantomtech (ex: phantomtech)

ACTIVE DIRECTORY SEARCH BASE [?]

dc=phantomtechnologies (ex: dc=phantomtech,dc=local)

MATCH GROUP SOURCE [?]

LDAP Attribute + User DN

MATCH GROUP ATTRIBUTE [?]

memberOf (memberOf)

MATCH GROUP KEY [?]

CN (CN)

MATCH USER DN KEY [?]

OU (leave blank if not matching by User DN)

TOKENIZE GROUPS [?]

● No
○ Yes

LOCATION ATTRIBUTE [?]

NUMBER OF AUTHENTICATORS [?]

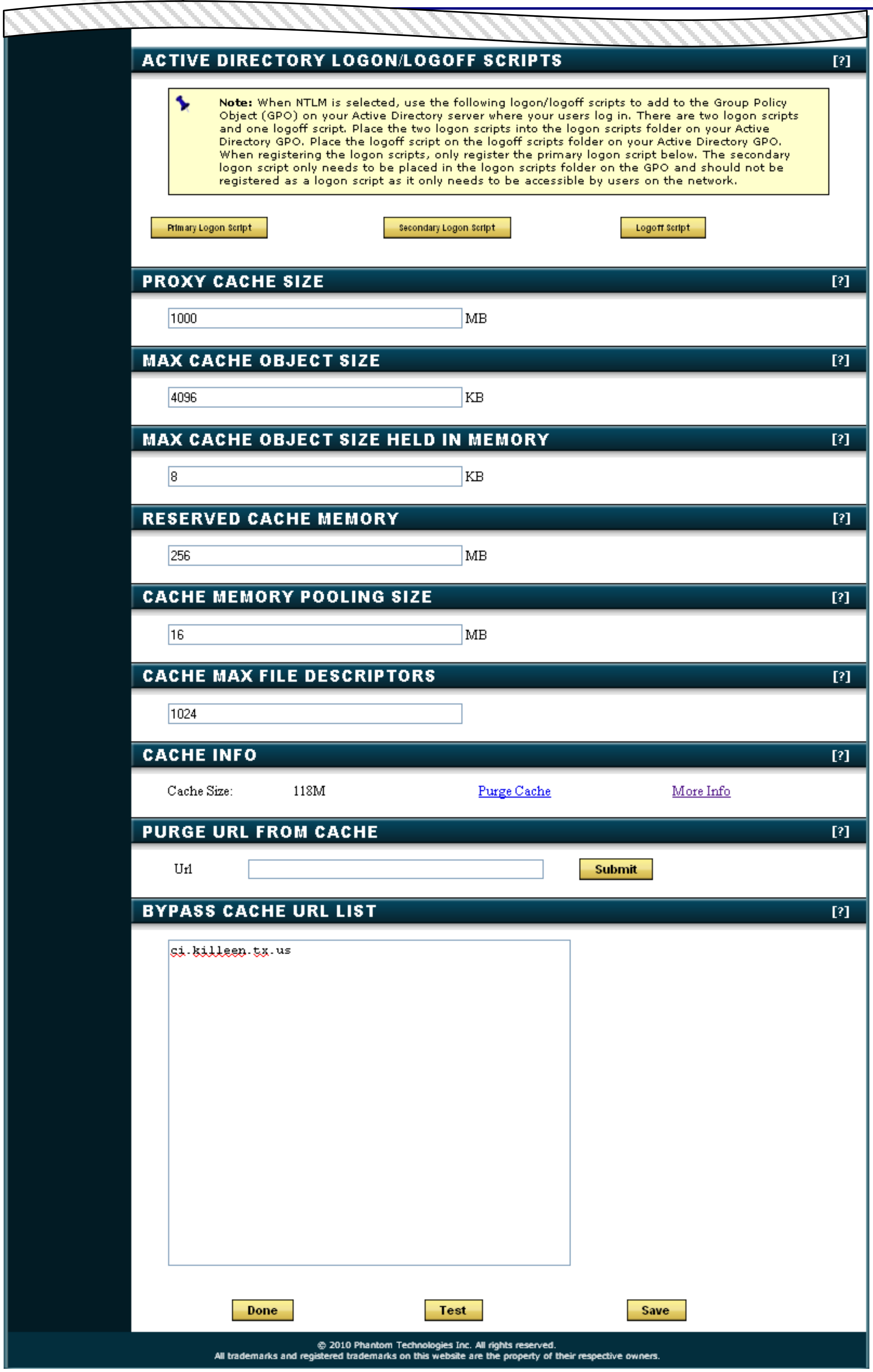
15

AUTHENTICATION RETRY SECONDS [?]

0 (0 = disabled)

ACTIVE DIRECTORY LOGON/LOGOFF SCRIPTS [?]

/logoff scripts to add to the Group Policy



ACTIVE DIRECTORY LOGON/LOGOFF SCRIPTS [?]

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

PROXY CACHE SIZE [?]

1000 MB

MAX CACHE OBJECT SIZE [?]

4096 KB

MAX CACHE OBJECT SIZE HELD IN MEMORY [?]

8 KB

RESERVED CACHE MEMORY [?]

256 MB

CACHE MEMORY POOLING SIZE [?]

16 MB

CACHE MAX FILE DESCRIPTORS [?]

1024

CACHE INFO [?]

Cache Size: 118M Purge Cache More Info

PURGE URL FROM CACHE [?]

Url

BYPASS CACHE URL LIST [?]

ci.killeen.tx.us

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

Figure 15 - Active Directory via Logon/Logoff scripts

Enable proxy support and fill in the values that pertain to your Active Directory server. The logon/logoff scripts accesses the proxy ports of the iBoss, but users will not be filtered via proxy settings.
Use the examples next to each box to determine the format of the field. For example, for the username, enter the username as "**Administrator**" and not \\mydomain\Administrator.

It is important to select "**Active Directory** (**NTLM**)" for the User Authentication Method. In addition, enter your Active Directory IP Address for both "**WINS Server Ip Address**" and "**Password Server Ip Address**" if you are not using WINS.

The figure above shows sample configuration settings.

In a Windows 2008 server environment, you can select any domain controller in the domain. In a 2003 server environment, typically the primary domain controller is used, but any Active Directory server can be used.

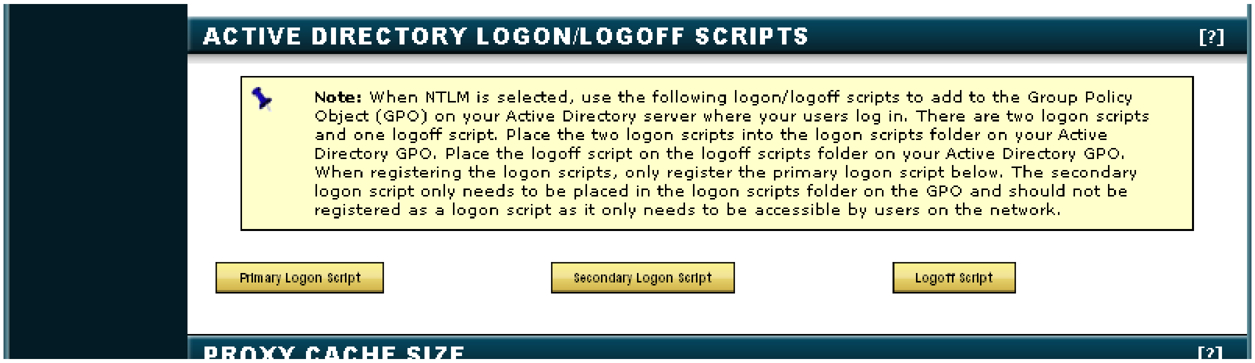
Once finished entering the settings, click "**Save**". Once settings are saved, click "**Test**" to confirm the settings are successful.

3.5.3.1 How the Logon/Logoff Scripts work

The logon and logoff scripts are configured as a part of a Group Policy Object that execute the logon script at user logon and execute the logoff script at user logoff.

Essentially, a web request is made to the iBoss in the background from the script when the user logs into his station. When the user logs off of his station, a web request is made to the iBoss indicating the user is logging off.

To download the scripts, click on "**Primary Logon Script**", "**Secondary Logon Script**", and "**Logoff Script**" on the Active Directory & Proxy Settings page.

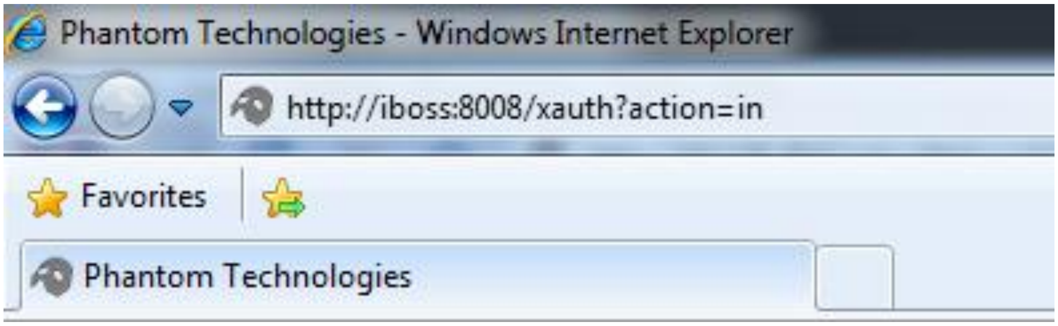


Note: When NTLM is selected, use the following logon/logoff scripts to add to the Group Policy Object (GPO) on your Active Directory server where your users log in. There are two logon scripts and one logoff script. Place the two logon scripts into the logon scripts folder on your Active Directory GPO.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

3.5.3.1.1 *The Logon Script*

For the logon script, the web request contained within the script looks similar to below:

http://iboss:8008/xauth?action=in



Phantom Technologies - Windows Internet Explorer

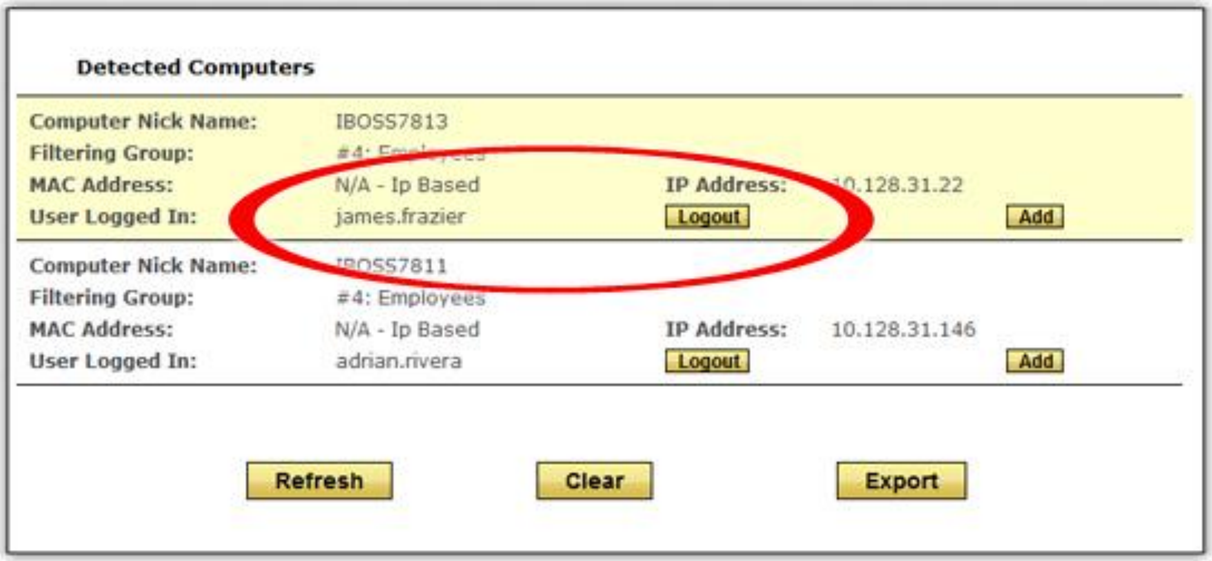
http://iboss:8008/xauth?action=in

Figure 16 - Logon

Notice that the script makes a request to the iboss DNS name given in the iBoss DNS settings page in the earlier section. It is important that the request is made to the DNS name rather than the iBoss IP Address as the single sign-on process is initiated with this request which authenticates the user on the computer and confirms the user reported is the user logged in. If an IP Address is used, the computer will not perform the single sign-on process as computers on the network only trust other computers on the same network under the same domain.

You can manually test the login process by pasting this URL in the browser of a computer logged into the domain, then navigating to Home→Identify Computers & Users within the iBoss.

You should see your computer in the computers list with your username logged into it. Note that the iBoss may have to be inline first in order for the iBoss to see your IP Address on the network.



Detected Computers

Computer Nick Name:	IBOSS7813			
Filtering Group:	#4: Employees			
MAC Address:	N/A - Ip Based	IP Address:	10.128.31.22	
User Logged In:	james.frazier	Logout		Add
Computer Nick Name:	IBOSS7811			
Filtering Group:	#4: Employees			
MAC Address:	N/A - Ip Based	IP Address:	10.128.31.146	
User Logged In:	adrian.rivera	Logout		Add

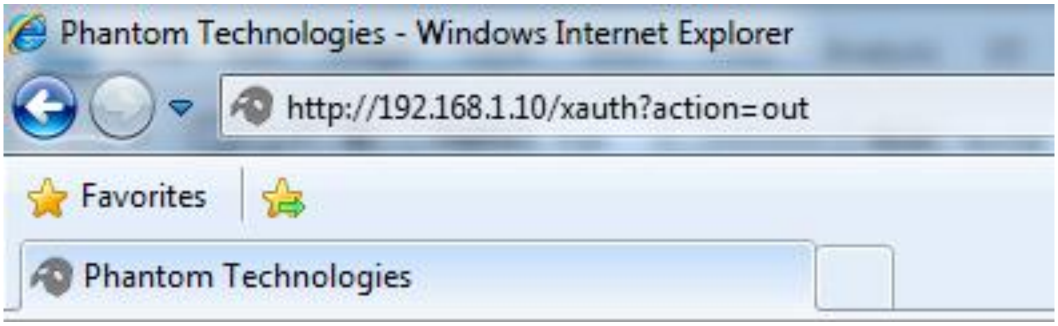
Figure 17 - User Logged In

If you are prompted with a login window when using the URL above in your browser, then the iBoss has not been properly configured via the Active Directory & Proxy Settings page. When this URL is pasted, no visible password prompts should be noticed and you should be taken to your home page (or the default page configured on the Active Directory & Proxy settings page.

3.5.3.1.2 *The Logoff Script*

The logoff script works similarly to the logon script, and the URL looks similar to the following:

http://[ip address of iboss]/xauth?action=out



Phantom Technologies - Windows Internet Explorer
http://192.168.1.10/xauth?action=out
Favorites
Phantom Technologies

Figure 18 - Logoff

When a computer that is logged into the domain logs off the network, the script makes a background call to the above URL. This triggers the iBoss to disassociate the user from the computer.

You can test the logoff script by pasting the URL into your web browser. You should see a message indicating "**SUCCESS**". When returning to the Identify Computer & Users page in the iBoss, the username that was associated to the computer should now be removed.

3.5.3.2 Configuring the Logon and Logoff scripts in an Active Directory GPO

From the Active Directory server, navigate to the iBoss in the web browser, then go to Home→Setup Network Connection→Active Directory & Proxy Settings.

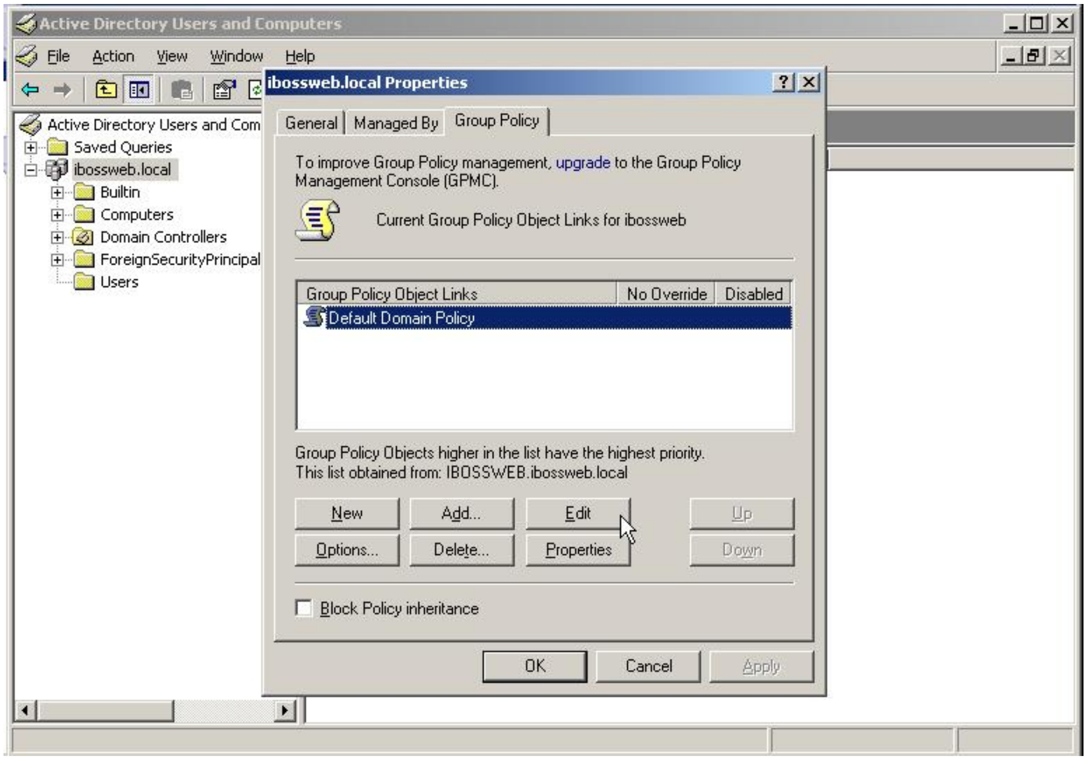
On that page, there are three orange buttons located in the center of the page – (1) Primary Logon Script, (2) Secondary Logon Script, (3) Logoff Script.

Download all three scripts onto the desktop of the domain controller by clicking each button. You will use these scripts in the next steps.

1. From within your Active Directory server, go to Start→Programs→Administrative Tools and click on 'Active Directory Users and Computers'

NOTE	If you have Group Policy Management installed, you may click on Start→Program→Administrative Tools→Group Policy Manager.

2. Right-click on the domain and select Properties, then select the Group Policy tab.
3. Select the 'Default Domain Policy' and click Edit.



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

Current Group Policy Object Links for ibossweb

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

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

□ Block Policy inheritance

Figure 19 - Configuring Logon/Logoff Group Policy

4. Expand and select User Configuration→Windows Settings→Scripts (Logon/Logoff).

You should see two options in the right pane, one for logon and another for logoff.

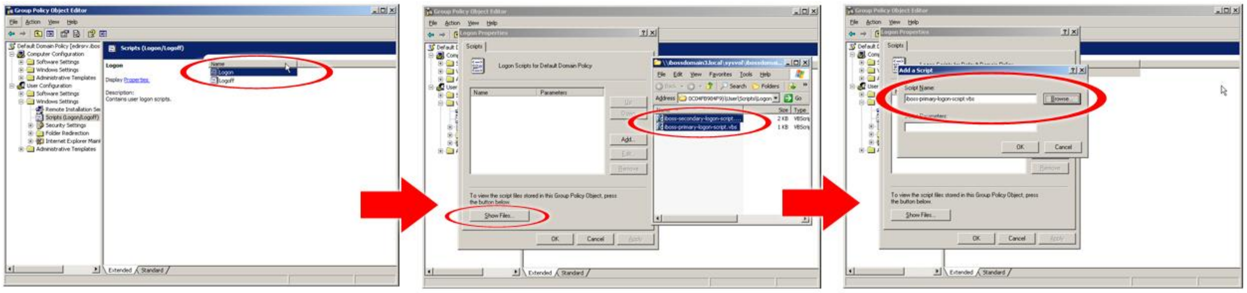


Figure 20 - Installing Logon Script

5. Open the Logon script configuration by double clicking on the Logon option in the right pane.

6. Click the button that says "**Show Files**" located toward the bottom of the new window. Click this button which will open a new folder window.

7. Copy the Primary Logon Script and Secondary Logon Script to the folder window that appeared when you clicked "**Show Files**" and close the window.

8. Now click the “**Add**” button and select the Primary Logon Script. Click ok to close all Logon Script configuration windows.

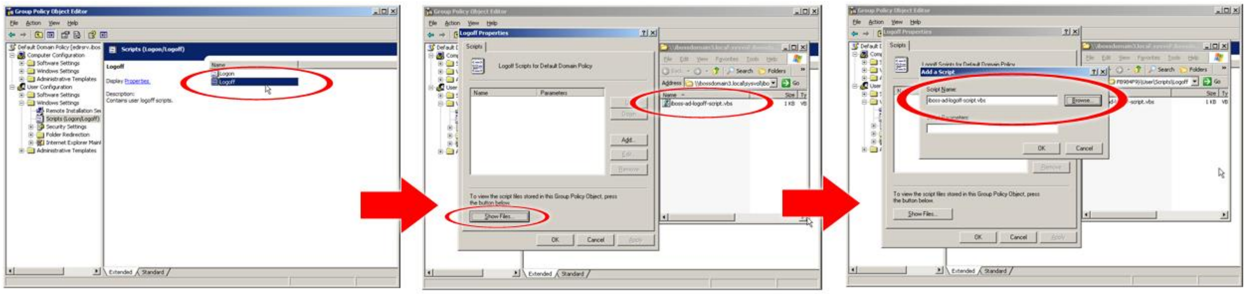


Figure 21 - Installing Logoff Script

9. Click the Logoff option in the right pane.

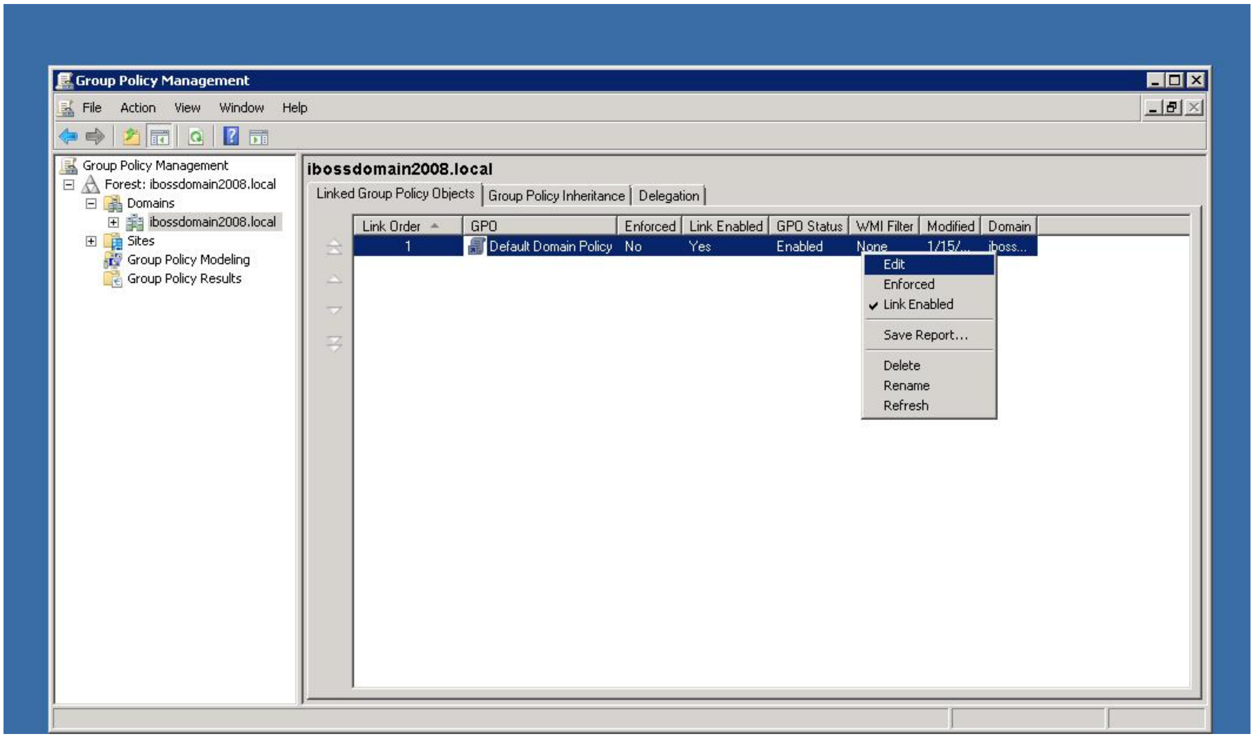
10. Click “**Show Files**” and copy the iBoss Logoff script from the desktop to this folder and close the window.

11. Click the “**Add**” button and select the logoff script. Click ok to close all Logoff configuration windows.

12. This completes the configuration of the Logon/Logoff scripts.

For Windows 2008 server, follow these instructions:

1. From within your Active Directory server, go to Start→Programs→Administrative Tools and click on “**Group Policy Manager”**
2. Expand Domains and click on your Domain.
3. Right click the ‘**Default Domain Policy’** and click **Edit**.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	1/15/...	iboss...

Figure 22 - Configuring Logon/Logoff Group Policy on 2008 Server

4. Expand and select User Configuration→Windows Settings→Scripts (Logon/Logoff).

You should see two options in the right pane, one for logon and another for logoff.

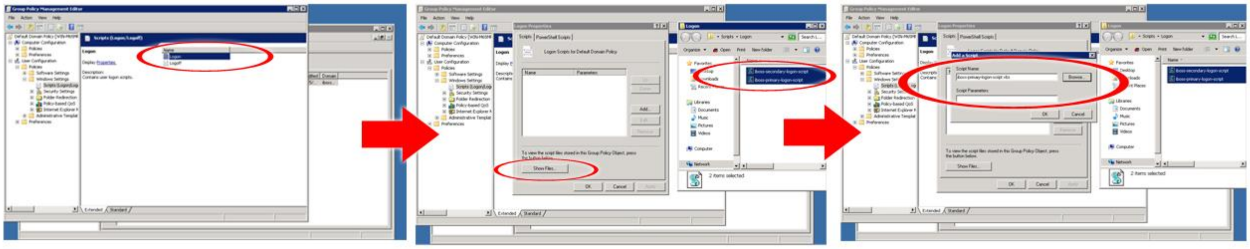


Figure 23 - Installing 2008 Logon Script

5. Open the Logon script configuration by double clicking on the Logon option in the right pane.

6. Click the button that says "**Show Files**" located toward the bottom of the new window. Click this button which will open a new folder window.

7. Copy the Primary Logon Script and Secondary Logon Script to the folder window that appeared when you clicked "**Show Files**" and close the window.

8. Now click the "**Add**" button and select the Primary Logon Script. Click ok to close all Logon Script configuration windows.

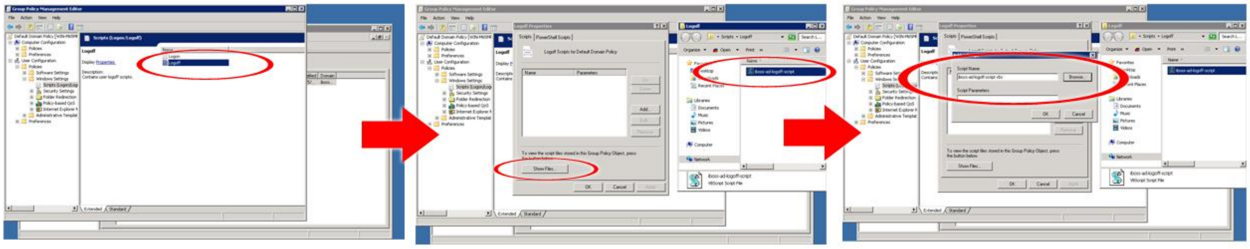


Figure 24 - Installing 2008 Logoff Script

9. Click the Logoff option in the right pane.

10. Click "**Show Files**" and copy the iBoss Logoff script from the desktop to this folder and close the window.

11. Click the "**Add**" button and select the logoff script. Click ok to close all Logoff configuration windows.

12. This completes the configuration of the Logon/Logoff scripts.

You can test that the scripts have been applied properly by using a computer that is part of the domain and logging into the computer. Once you are logged in, use a different computer to navigate to the iBoss Home Page→Identify Computers & Users. Find the computer that you just logged into in the Computers list by using that computer's IP Address in the filters.

You should see the username associated with the IP.

Logoff the workstation and wait for the logoff process to fully complete. Refresh the iBoss computers page by clicking "**Apply Filters**". The computer should appear with no user logged into it.

3.5.4 Configuring the Active Directory Plug-in

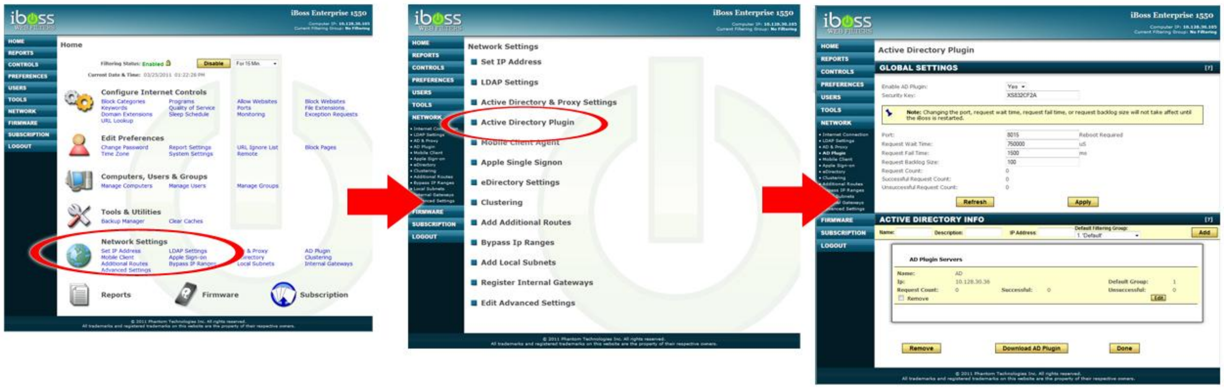
This section details configuration of the Active Directory plug-in. Use the plug-in if you would prefer to use this method over the logon/logoff scripts.

NOTE	Choose either the Logon/Logoff scripts or the Active Directory plug-in. There is no need to use both and only one is necessary.

The plug-in needs to be installed on any server within the domain to which users authenticate. This section details the process for one server. Repeat the steps for each Active Directory server on the network.

3.5.4.1 Step By Step Install Instructions

1. Navigate to the iBoss Active Directory Plug-in configuration page. It is located under Home→Setup Network Connection→Active Directory Plug-in.



Active Directory Plugin

GLOBAL SETTINGS

Enable AD Plugin: Yes
Security Key: XS832CF2A

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

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

ACTIVE DIRECTORY INFO

Name: Description: IP Address: Default Filtering Group: 1. 'Default'

AD Plugin Servers

Name: AD
Ip: 10.128.30.36 Default Group: 1
Request Count: 0 Successful: 0 Unsuccessful: 0
□ Remove

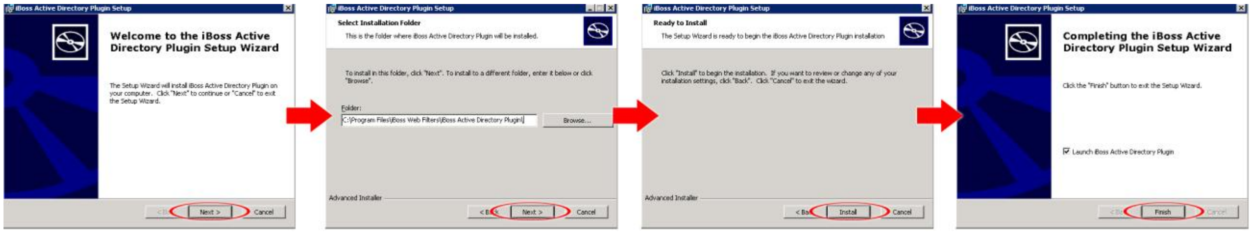
2. In the global settings section, enable the Active Directory plug-in interface by selecting Enable in the "Global Settings" section and clicking the "Apply" button.

3. Each Active Directory server will need to be added to the Active Directory servers list on this page. The iBoss only allows registered servers to communicate and send authentication information.

   Add each Active Directory server to the list by setting the Active Directory server name and IP Address and clicking the "**Add**" button. Repeat this process for each server on the network.

4. Now click the "**Download AD Plug-in**" button from the domain controller on this page to download the plug-in to the server. Extract and install the plug-in on the Active Directory server.

NOTE	Microsoft .NET Framework is required for the plug-in. If your server does not have .NET 2.0 or greater installed, the installation may fail while attempting to start the plug-in service. If this occurs, download and install the .NET Framework 2.0 from Microsoft. This does NOT require a server reboot.



Welcome to the iBoss Active Directory Plugin Setup Wizard

The Setup Wizard will install iBoss Active Directory Plugin on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Select Installation Folder

This is the folder where iBoss Active Directory Plugin will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\iBoss Web Filters\iBoss Active Directory Plugin\

Ready to Install

The Setup Wizard is ready to begin the iBoss Active Directory Plugin installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

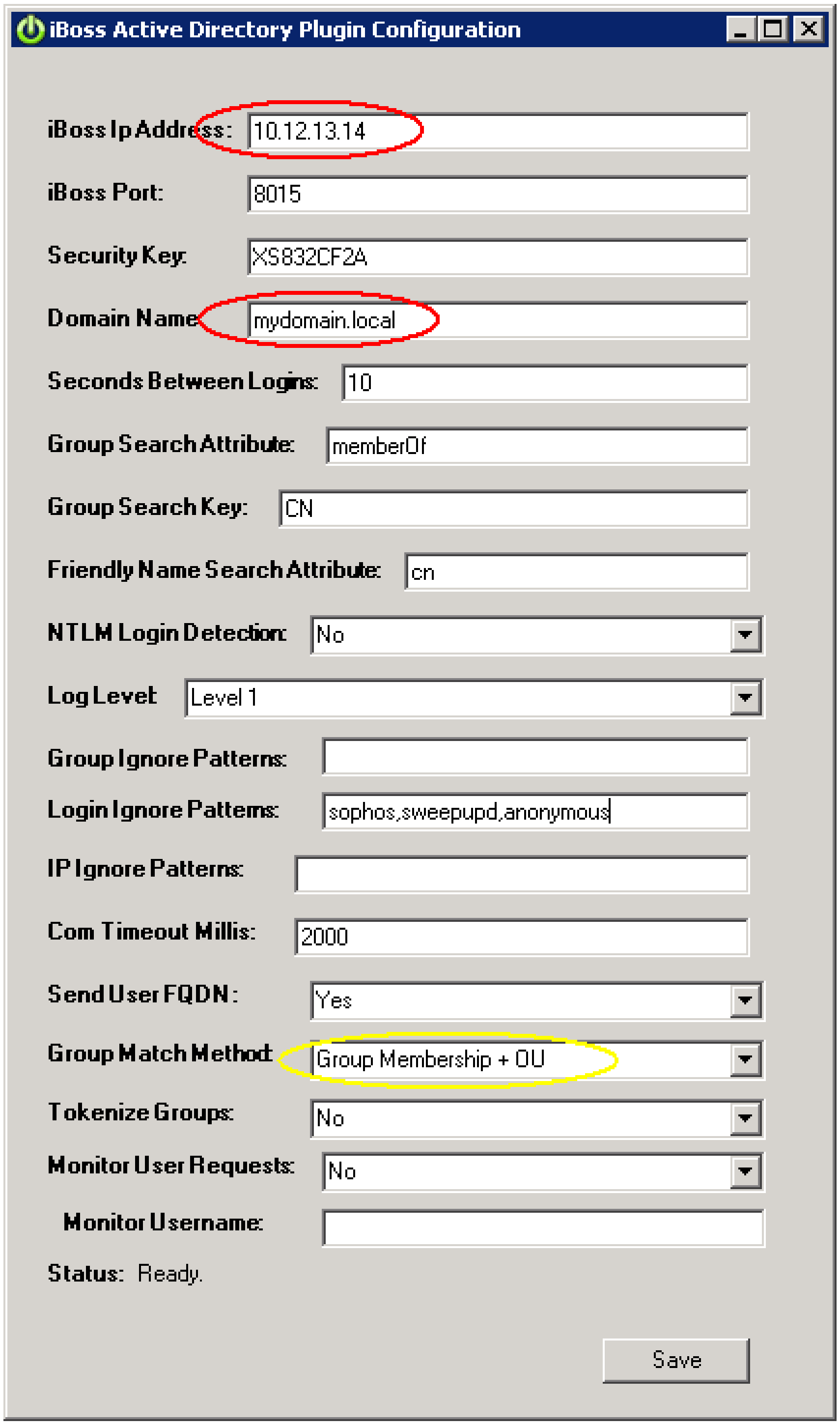
Completing the iBoss Active Directory Plugin Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

☑ Launch iBoss Active Directory Plugin

Figure 25 - AD Plug-in Installation

The plug-in configuration interface will appear after the install. You can access this interface anytime afterwards via your Programs menu.



iBoss Active Directory Plugin Configuration

iBoss Ip Address: 10.12.13.14

iBoss Port: 8015

Security Key: XS832CF2A

Domain Name: mydomain.local

Seconds Between Logins: 10

Group Search Attribute: memberOf

Group Search Key: CN

Friendly Name Search Attribute: cn

NTLM Login Detection: No

Log Level: Level 1

Group Ignore Patterns:

Login Ignore Patterns: sophos,sweepupd,anonymous

IP Ignore Patterns:

Com Timeout Millis: 2000

Send User FQDN: Yes

Group Match Method: Group Membership + OU

Tokenize Groups: No

Monitor User Requests: No

Monitor Username:

Status: Ready.

Figure 26 - Minimum Configuration of the Active Directory Plug-in

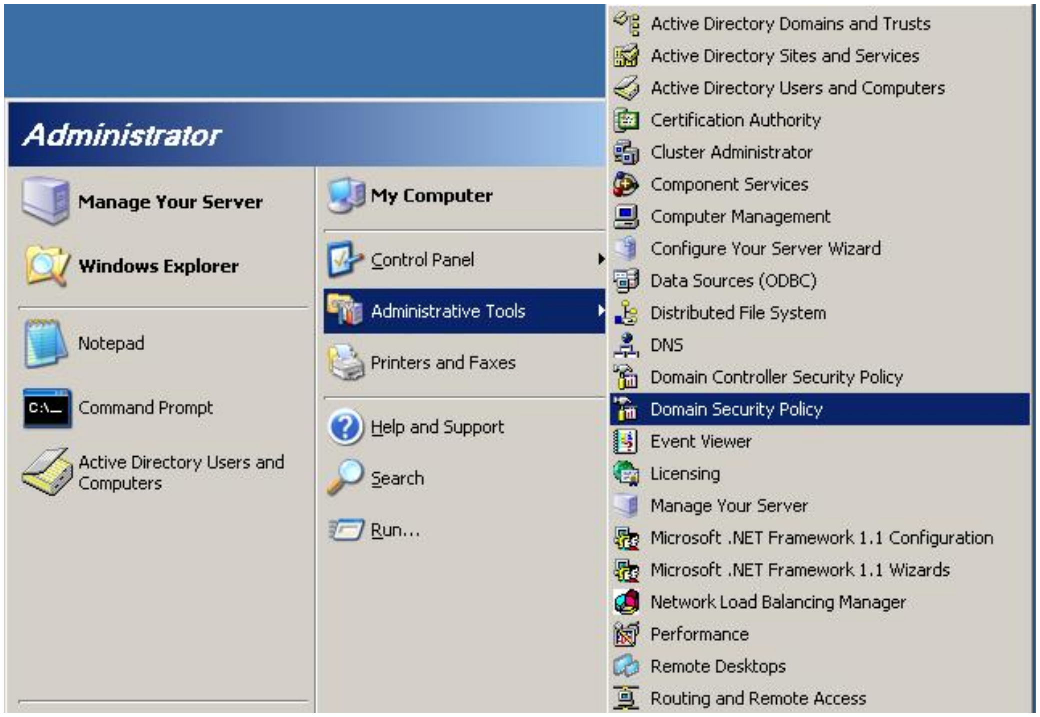
Most of the default settings are adequate. The settings that need to be changed are:

iBoss IP Address	Enter the IP Address of the iBoss
Domain Name	Enter the domain name for your network
Group Match Method	Select whether group, OUs or both are being used

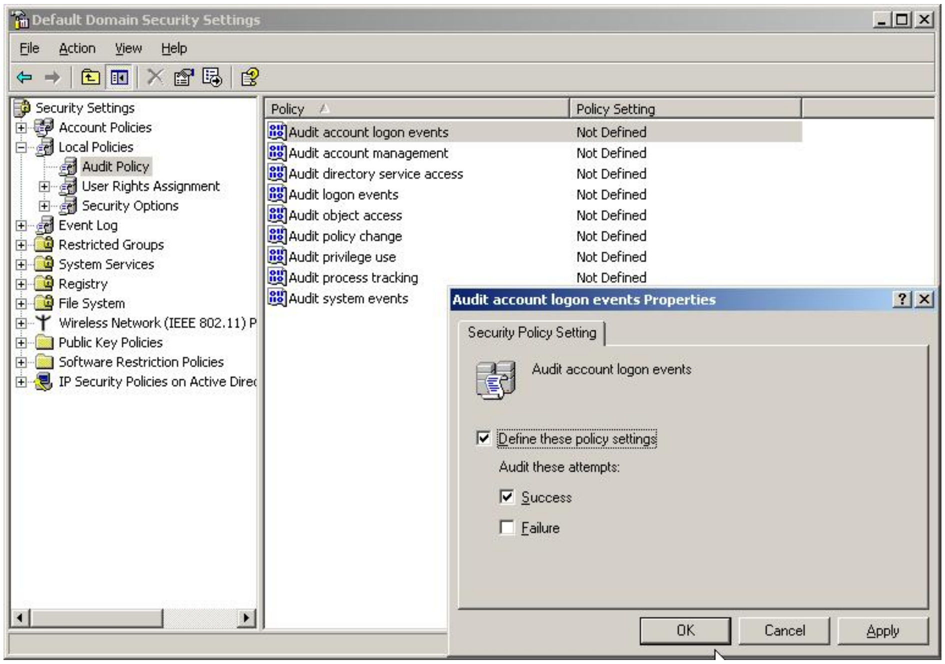
Once the settings are adjusted, click the Save button and close the window by clicking the "**X**" on the top right corner of the window.

The "**Domain Controllers Security Policy**" needs to be adjusted so that successful logon events are audited and logged by the domain controller. Configuring this policy varies depending on whether your network uses Active Directory 2003 or 2008 server.

For 2003 servers, Go to Administrative Tools→ Domain Controller Security Policy.



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



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

Audit account logon events Properties

Security Policy Setting

Audit account logon events

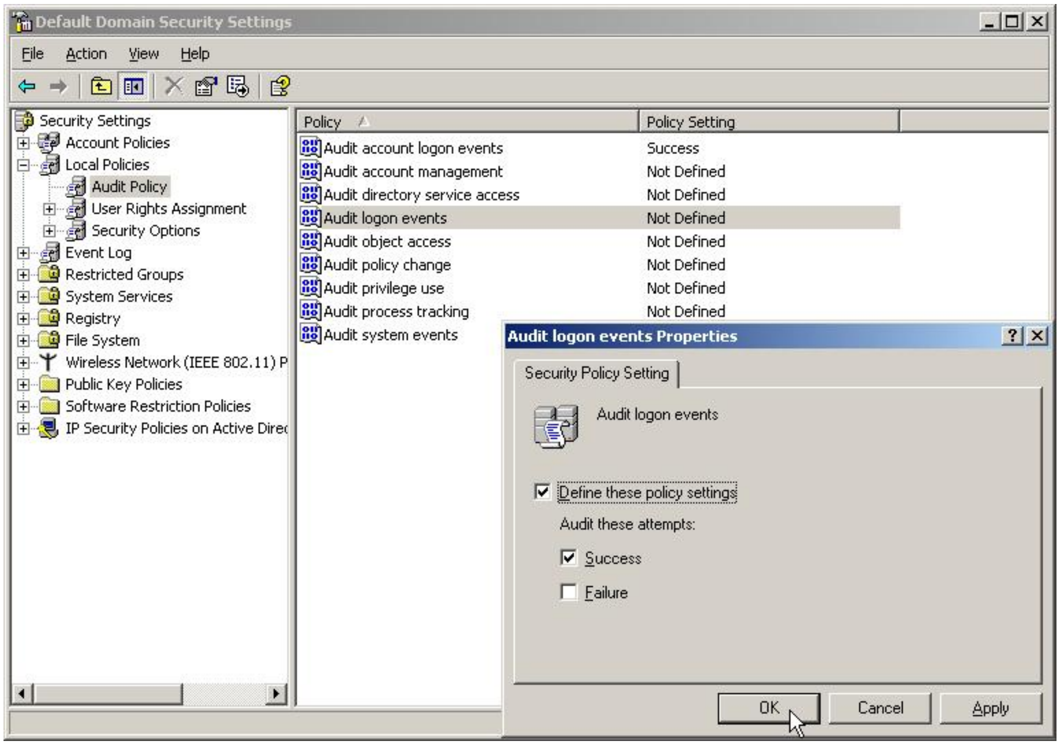
☑ Define these policy settings

Audit these attempts:

☑ Success

☐ Failure

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



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

Audit logon events Properties

Security Policy Setting

Audit logon events

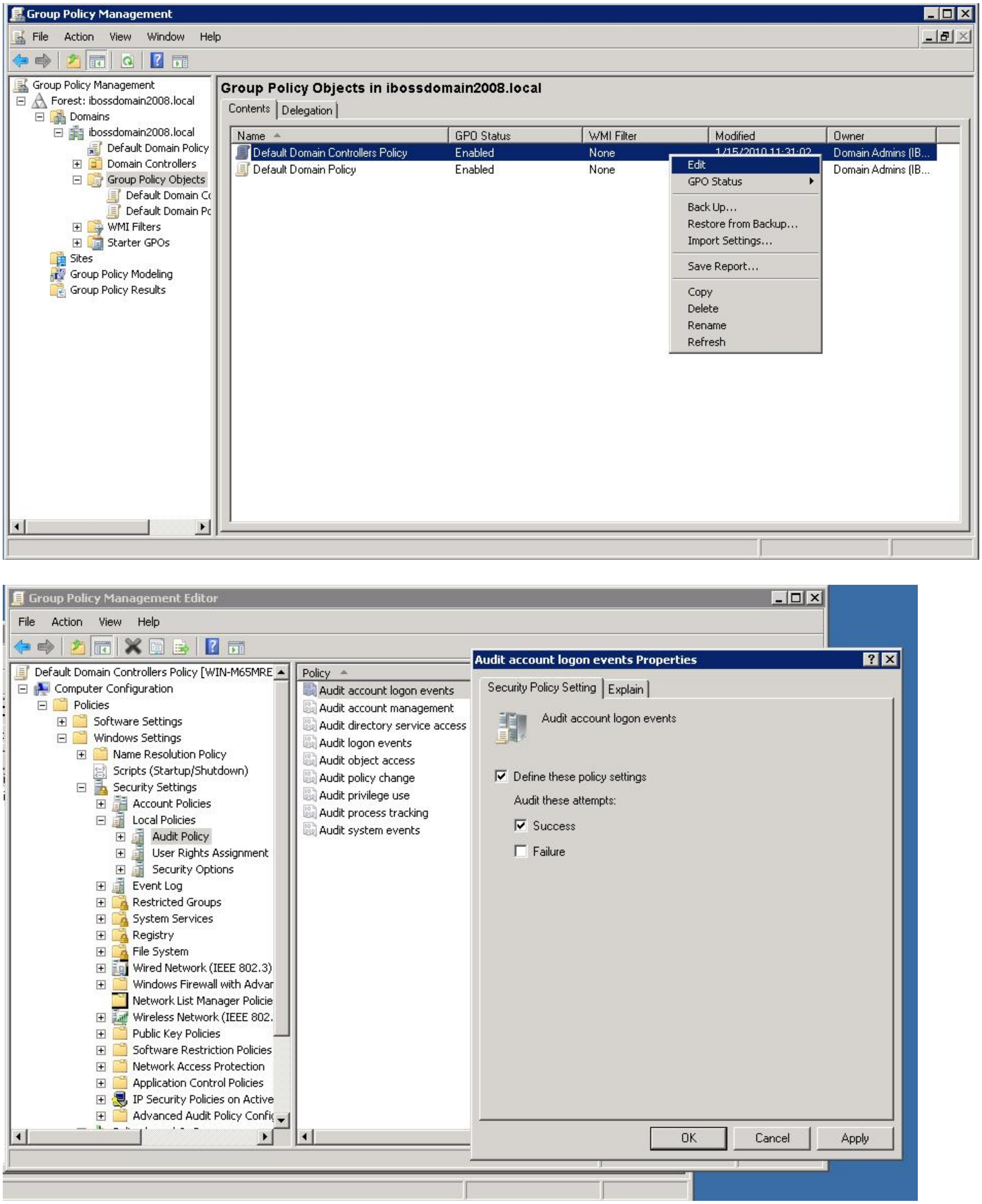
☑ Define these policy settings

Audit these attempts:

☑ Success

☐ Failure

For 2008 servers, open your Group Policy Editor under Administrative Tools, go to Group Policy Objects and locate the Default Domain Controllers Policy. Right click this policy and select “**Edit**”.



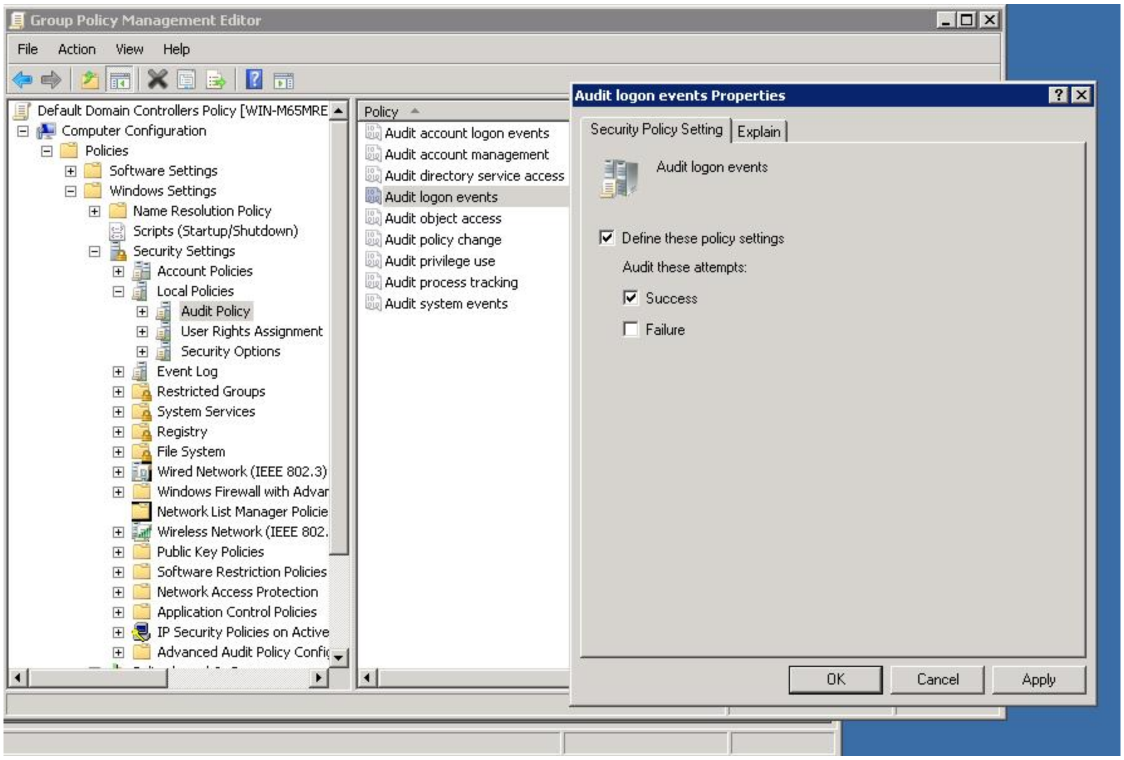
☑ Define these policy settings

Audit these attempts:

☑ Success

☐ Failure

Figure 27 - 2008 Audit account logon events



☑ Define these policy settings

Audit these attempts:

☑ Success

□ Failure

Figure 28 - 2008 Audit logon events

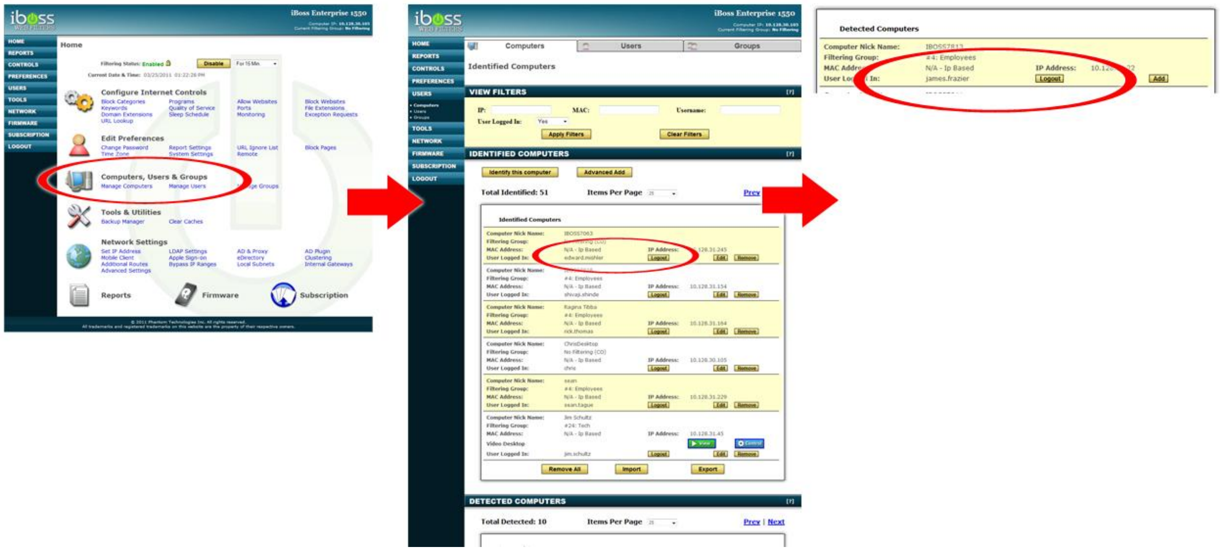
Expand under Computer Configuration→ Policies → Windows Settings → Security Settings → Local Policies→ Audit Policy → "**Audit account logon events Settings**" & "**Audit logon events**". Double click the first option **Audit account logon events** and make sure the checkbox for **Define these policy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

Once your default domain controller policy has been updated to reflect auditing of successful logon events, the Active Directory plug-in should start sending login events to the iBoss. If there are users currently logging into the network, you can confirm this via the Active Directory Plug-in page.

Navigate back to the iBoss. Under the registered Domain Controller in the Active Directory plug-in page, you should see requests coming from the Domain Controller if there are active users logging into the network. Refresh the page and confirm that there are requests being sent by the plug-in to the iBoss by checking the request count for the domain controller.

If the request count does not appear to be increasing immediately, you may want to wait for the policy to take effect as well as for users to log onto the network. It may take a few minutes for the configured Default Domain Controller Policy to take effect.

Once the plug-in is installed on each domain controllers, users should begin to appear in the Home→Identify Computers & Users page.



Filtering Status: Enabled — For 15 Min.
Current Date & Time: 03/25/2011 01:22:26 PM

© 2011 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Identified Computers

IP: MAC: Username:
User Logged In: Yes

Total Identified: 51 Items Per Page 25

Identified Computers

Computer Nick Name: IBOSS7063
Filtering Group: No Filtering (C0)
MAC Address: N/A - Ip Based IP Address: 10.120.31.245
User Logged In: edward.mishler

Computer Nick Name: IBOSS7016
Filtering Group: #4: Employees
MAC Address: N/A - Ip Based IP Address: 10.120.31.154
User Logged In: shivaji.shinde

Computer Nick Name: Ragina Tibba
Filtering Group: #4: Employees
MAC Address: N/A - Ip Based IP Address: 10.120.31.164
User Logged In: nick.thomas

Computer Nick Name: ChrisDesktop
Filtering Group: No Filtering (C0)
MAC Address: N/A - Ip Based IP Address: 10.120.30.105
User Logged In: chris

Computer Nick Name: sean
Filtering Group: #4: Employees
MAC Address: N/A - Ip Based IP Address: 10.120.31.229
User Logged In: sean.tague

Computer Nick Name: Jim Schultz
Filtering Group: #24: Tech
MAC Address: N/A - Ip Based IP Address: 10.120.31.45
Video Desktop
User Logged In: jim.schultz

Total Detected: 10 Items Per Page 25

Detected Computers

Computer Nick Name: IBOSS7813
Filtering Group: #4: Employees
MAC Address: N/A - Ip Based IP Address: 10.120.31.22
User Logged In: james.frazier

3.6 Integrating with eDirectory

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.

3.6.1 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

3.6.2 Overview

The iBoss can integrate with eDirectory with two different modes. Only one of the two modes is 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

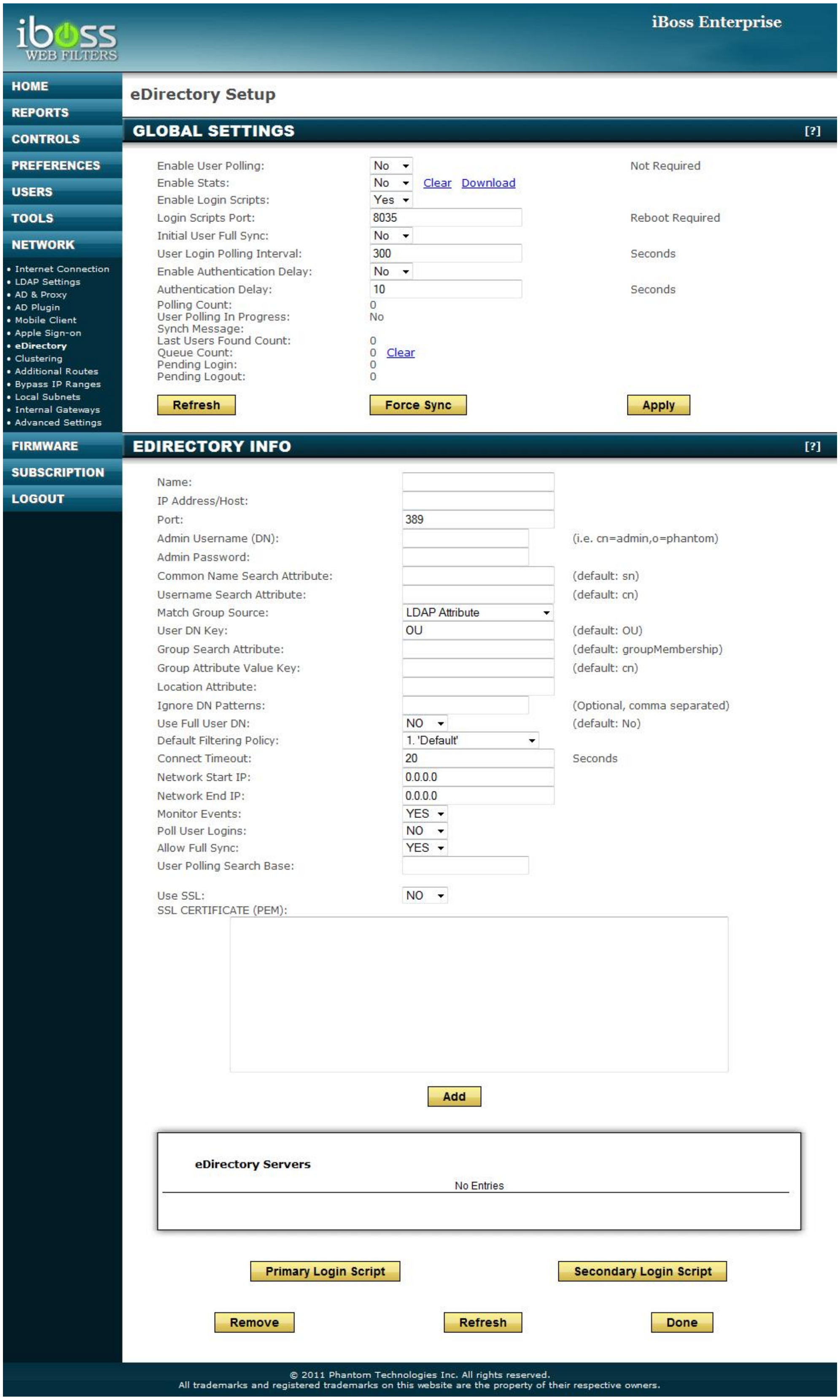
In this mode, the iBoss monitors login and logout events sent by the eDirectory server in real-time. As users login and logout of their workstations, eDirectory sends these events and iBoss uses them to associate the user with the workstation and apply dynamic filtering policy depending on which user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

3.6.3 iBoss Configuration

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



eDirectory Setup

GLOBAL SETTINGS

Enable User Polling:	No	Not Required
Enable Stats:	No	
Enable Login Scripts:	Yes	
Login Scripts Port:	8035	Reboot Required
Initial User Full Sync:	No	
User Login Polling Interval:	300	Seconds
Enable Authentication Delay:	No	
Authentication Delay:	10	Seconds
Polling Count:	0	
User Polling In Progress:	No	
Synch Message:		
Last Users Found Count:	0	
Queue Count:	0	
Pending Login:	0	
Pending Logout:	0	

EDIRECTORY INFO

Name:		
IP Address/Host:		
Port:	389	
Admin Username (DN):		(i.e. cn=admin,o=phantom)
Admin Password:		
Common Name Search Attribute:		(default: sn)
Username Search Attribute:		(default: cn)
Match Group Source:	LDAP Attribute	
User DN Key:	OU	(default: OU)
Group Search Attribute:		(default: groupMembership)
Group Attribute Value Key:		(default: cn)
Location Attribute:		
Ignore DN Patterns:		(Optional, comma separated)
Use Full User DN:	NO	(default: No)
Default Filtering Policy:	1. 'Default'	
Connect Timeout:	20	Seconds
Network Start IP:	0.0.0.0	
Network End IP:	0.0.0.0	
Monitor Events:	YES	
Poll User Logins:	NO	
Allow Full Sync:	YES	
User Polling Search Base:		
Use SSL:	NO	
SSL CERTIFICATE (PEM):		

eDirectory Servers

No Entries

© 2011 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 29 - iBoss eDirectory Settings

3.6.4 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.

3.6.4.1 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.

3.6.4.2 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.

3.6.4.3 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.

3.6.4.4 User Polling In Progress

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

3.6.4.5 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.

3.6.5 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.

3.6.5.1 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.

3.6.5.2 Ip Address/Host

The IP Address or host name of the eDirectory server.

3.6.5.3 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.

3.6.5.4 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.

3.6.5.5 Admin Password

The password for the admin user specified above.

3.6.5.6 Common Name Search Attribute

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

Default: sn

3.6.5.7 Username Search Attribute

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

Default: cn

3.6.5.8 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

3.6.5.9 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

3.6.5.10 Location Attribute

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

3.6.5.11 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.

3.6.5.12 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.

3.6.5.13 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

3.6.5.14 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.

3.6.5.15 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.

3.6.5.16 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.

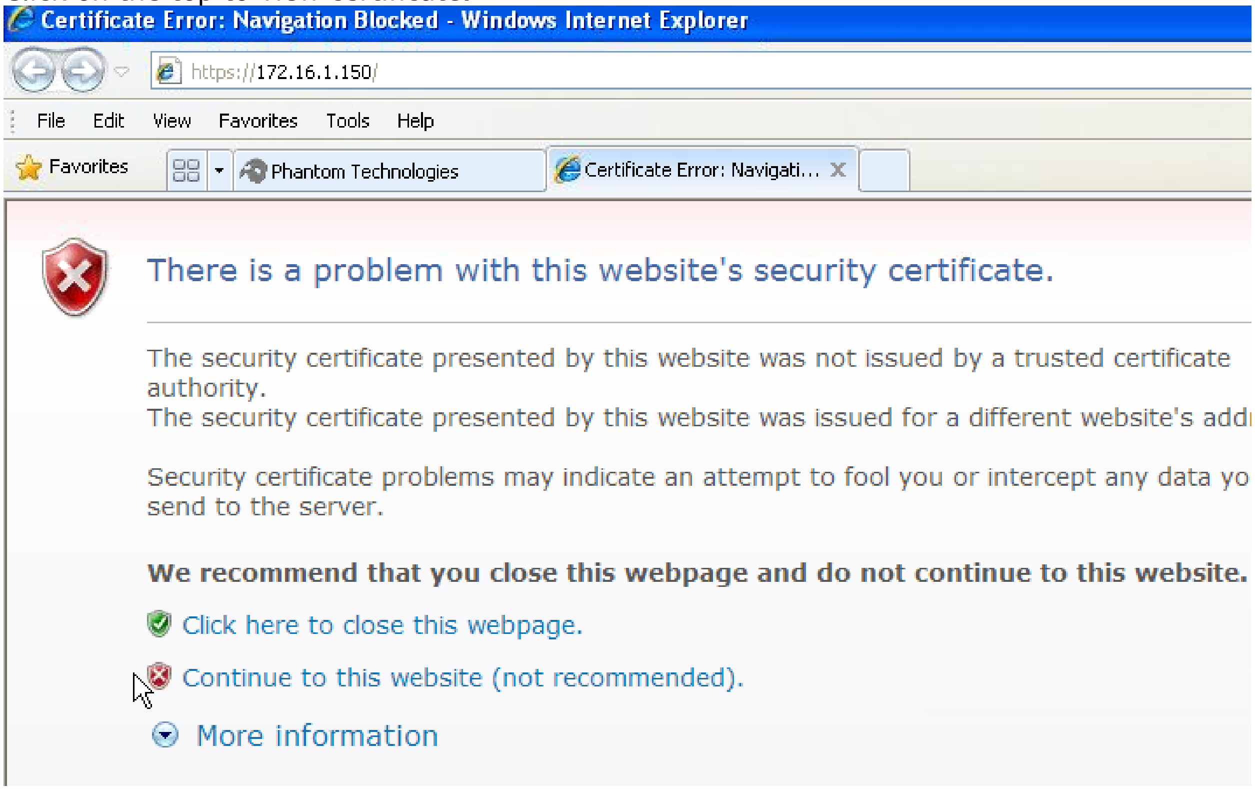
3.6.5.17 User Polling Search Base

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).

3.6.5.18 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**"

Obtaining the SSL certificate, go to https://IPADDRESS click on Continue to this webpage. Click on the top to view certificate.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://172.16.1.150/
File
Edit
View
Favorites
Tools
Help
Favorites
Phantom Technologies
Certificate Error: Navigati...

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's add

Security certificate problems may indicate an attempt to fool you or intercept any data yo send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

3.6.6 Add The Server

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

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

4 Conclusion

The iBoss should be configured with baseline settings after completion of the steps in this deployment diagram.

Please note that by default, the iBoss will not block any web content, but will archive all accesses. All filter settings are configured via the Home→Internet Controls menu.

Please refer to the iBoss Enterprise Manual for detailed explanations of the iBoss settings and configuration.