iboss Security Agents

iboss Newtork Security

www.iboss.com

Table of Contents

Table of Figures

1 iBoss Security Agent

1.1 Overview

The iBoss security agent is used to provide filtering for computers that will connect to the Internet from outside of an enterprise network that is monitored by the Enterprise iBoss. In addition, the iboss security agent can be used as a local network security agent to provide data inspection of SSL encrypted content.

Note: SSL content inspection is available on the generation 3 (gen3) Windows agent only. SSL filtering/blocking is available by default on both the Windows and Mac agents regardless of the SSL content inspection additional feature. The additional SSL content inspection feature allows for the logging and blocking of links within SSL encrypted pages. The SSL content inspection feature is NOT required to block SSL/HTTPs requests and log accesses to those destinations.

The agent can be used for both mobile security and local SSL/Encryption data inspection or for either local or mobile use depending on your requirements.

The Agent is very lightweight, easy to install and transparent to the user.

1.2 Key Features

- **Installation may be pushed to the client via your usual deployment method**
- **Intelligently determines if client is on enterprise or remote network**
- **Accounts for VPN configurations**
- **Monitoring and reporting available from the Enterprise Reporter**
- **Versions for Windows, Mac, iPad and iPod**
  (please see separate iBoss Browser Filter manual for iPad & iPod)

1.3 Additional Key Features of Gen 2 Windows Mobile Agent

- **Full SSL decryption allows the agent to fully filter and monitor the internal content of encrypted sites accessed via https.**
- **Google image scrubbing cleans image results from Google image searches based on configured policy**
- **Google translation filtering filters websites when accessed via Google Translation services**
- **Gen3 - Local Network SSL inspection agent capability allows for inspection of SSL encrypted content while on local network. This provides expanded social media controls and reporting of links within HTTPS pages.**

2 Getting Started

This section describes the activities necessary to enable filtering on a mobile client.

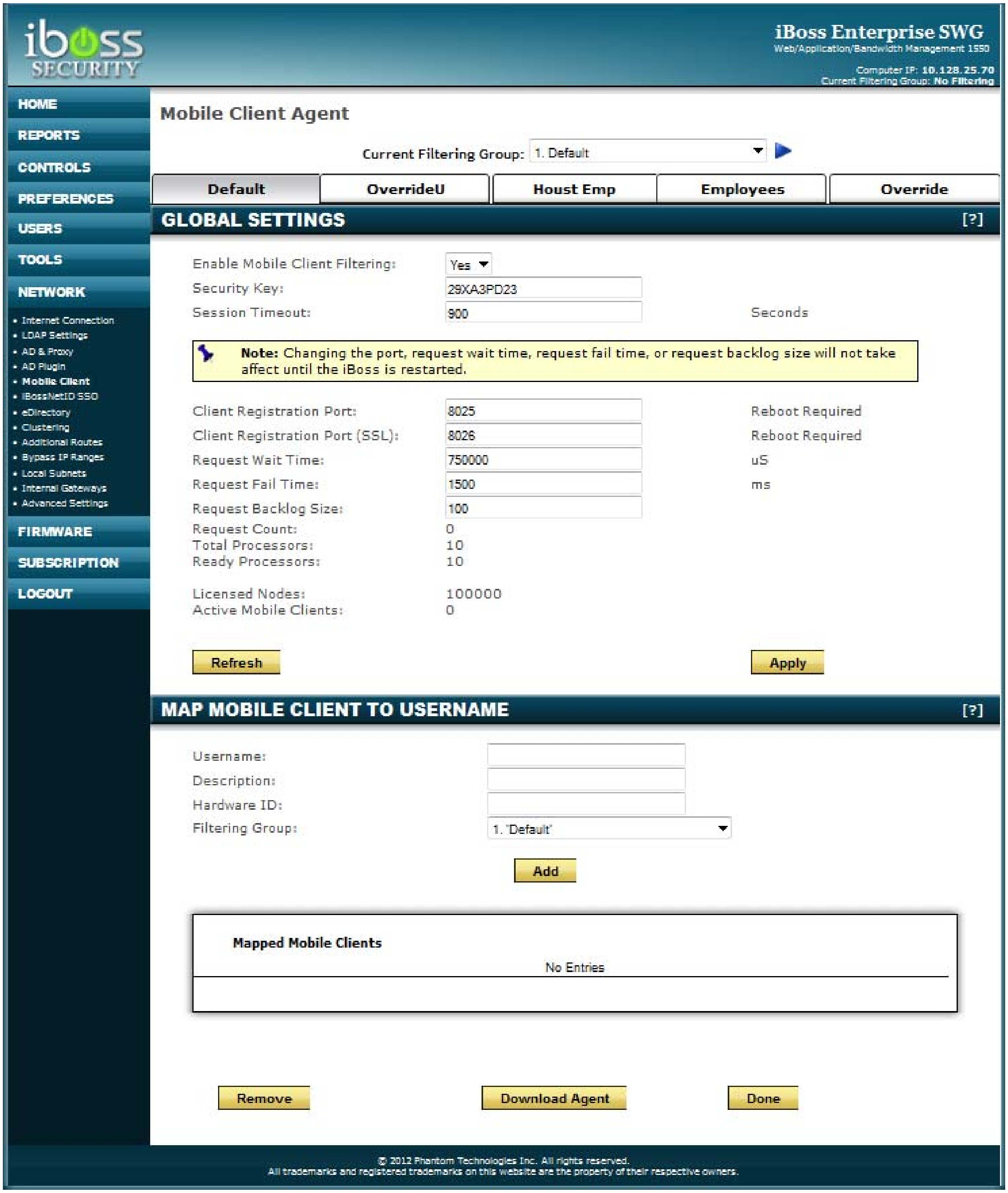
2.1 Overview

Filtering for the Mobile Client Agents is achieved by exchanging Internet access data with the iBoss Enterprise for filter policy comparison. A secondary connection informs the iBoss of username, IP, and hardware ID. A decision is made according to assigned policy and the mobile client is directed to allow the Internet connection or replace with a block page.

The Agent detects computer network configuration events and modifies its behavior as appropriate. On the local enterprise network it allows normal operation as any other client. If connected to an offsite network (café, home, airport, …) the agent switches mode and establishes connection to the Enterprise iBoss to continue filtering based on the filtering policy assigned for mobile use.

2.2 iBoss Configuration

Mobile Client Agent configuration is performed via the menu option:
Network→Mobile Client Agent



Computer IP: 10.128.25.70
Current Filtering Group: No Filtering

Mobile Client Agent

Current Filtering Group: 1. Default

GLOBAL SETTINGS

Enable Mobile Client Filtering: Yes
Security Key: 29XA3PD23
Session Timeout: 900 Seconds

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

Client Registration Port: 8025 Reboot Required
Client Registration Port (SSL): 8026 Reboot Required
Request Wait Time: 750000 uS
Request Fail Time: 1500 ms
Request Backlog Size: 100
Request Count: 0
Total Processors: 10
Ready Processors: 10

Licensed Nodes: 100000
Active Mobile Clients: 0

MAP MOBILE CLIENT TO USERNAME

Username:
Description:
Hardware ID:
Filtering Group: 1. 'Default'

Mapped Mobile Clients

No Entries

© 2012 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Figure 1 - iBoss Mobile Client Configuration

2.2.1 Global Settings

The global settings section contains configuration settings that apply across all registered Mobile Client connections.

`Enable Mobile Client Filtering:` Must be 'Yes' for any clients to connect
`Security Key:` any alphanumeric string (Should change from default)
`Session Timeout:` Seconds for a client to timeout if not refreshed

```
Client Registration Port:       |
Client Registration Port (SSL): |
Request Wait Time:              | Please do not change these without
Request Fail Time:              | contacting support.
Request Backlog Size:           |
```

`Request Count:` Number of client connection requests received
`Licensed Nodes:` Max concurrently connected clients
`Active Mobile Clients:` Current number of non-timed out sessions

Select to save this configuration. These settings will be applied to newly received connections.

2.2.2 Mapping Mobile Clients

Individual clients may be mapped to Filter Groups by either Hardware ID or User. This will override the Filter Group assigned at installation time.

2.2.3 Additional Configuration

The IP 208.70.74.2 should be on the Allowlist and marked as global if 'ID Theft' is enabled. The mobile client accesses this IP to determine On or Off Net.

2.3 Network Preparation

The iBoss Mobile Agent requires connectivity to the Enterprise iBoss while on a remote network. Usually this is via a port-forward from the public IP of a firewall to the internal IP of the iBoss.

2.3.1 Most Common Configuration

A port forward on the firewall for:

- UDP port 53 for DNS (Only Required for Windows Mobile Gen 1). Do not forward this port if you are using the Gen2 Windows Mobile Client
- TCP port 8025 and 8026 (default) for a data channel conveying registration information
-

A web server accessible from off-network to provide the block page (contact iBoss Support for assistance with this if one is not readily available).

2.3.2 Alternate Scenarios

If your network topology is more complicated you will need to consult with iBoss support. As we find solutions for these situations we will document them in the Knowledgebase.

2.4 Mobile Client Agent Installation

The Mobile Client installation files are downloaded via the ‘Download Agent’ button in the iBoss Enterprise interface;
Network→Mobile Client

Download and extract the archive. The archive contains both Windows and Mac folders with the relevant files in another archive file.

NOTE: It is assumed that the mobile user will not have permissions to alter the network configuration or registry of the mobile client.

2.4.1 Windows (Gen 1)

NOTE: The Gen 2 Windows Mobile Client is recommended. Installation of this client is described in the next section.

Extract the archive from the Windows Gen1 folder. The archive contains a Windows Installation file (.msi) and a registry update file (.reg). Installation may be done manually or pushed via the publishing feature of Windows Server (http://support.microsoft.com/kb/816102).
Note: The latest installation files are always available via the 'Download Agent' button.

1. Modify the following for all Filter Groups used for mobile filtering;
   Preferences→Block Pages→DNS BLOCK RESPONSE IP = 208.70.74.33

2. Modify the registry update file with site-specific data as described below.

reg-param-settings.reg

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\iBossMobileClient\Parameters]
"LogLevel"=dword:00000001
"RemoteDnsServerIp"=""
"RemoteRegIp"=""
"OutsideNetworkIp"=""
"SecurityKey"=""
"ResolutionDelaySeconds"=dword:00000002
"UseRemoteDnsIfInterfaceEnabled"="sonicwall"
"FilteringMethod"="DNS"
"UseLocalDnsIfInterfaceEnabled"=""
"DoNotSetDnsOnAdapters"=""
"RegistrationIntervalMillis"=dword:000493e0
"ResolutionVersionParam"=dword:00000003
```

Minimum configuration:
RemoteDnsServerIp: The public IP for access to the iBoss DNS while NOT on local net.
RemoteRegIp: Usually the same as RemoteDnsServerIp.
OutsideNetworkIp: Public IP to which private addresses are NATed.
(a range can be specified as 1.23.45.100-1.23.45.200)
SecurityKey: The Security Key of the Filter Group from iBoss Mobile Client configuration.

3. Import the modified registry settings by double-clicking the file or using regedit.
4. Install the Mobile Agent by double-clicking the .msi file or right-clicking and select install.

2.4.2 Windows (Gen2/Gen3) - Recommended

Extract the mobile client from the windows->gen3 folder. This folder contains 3 core files:

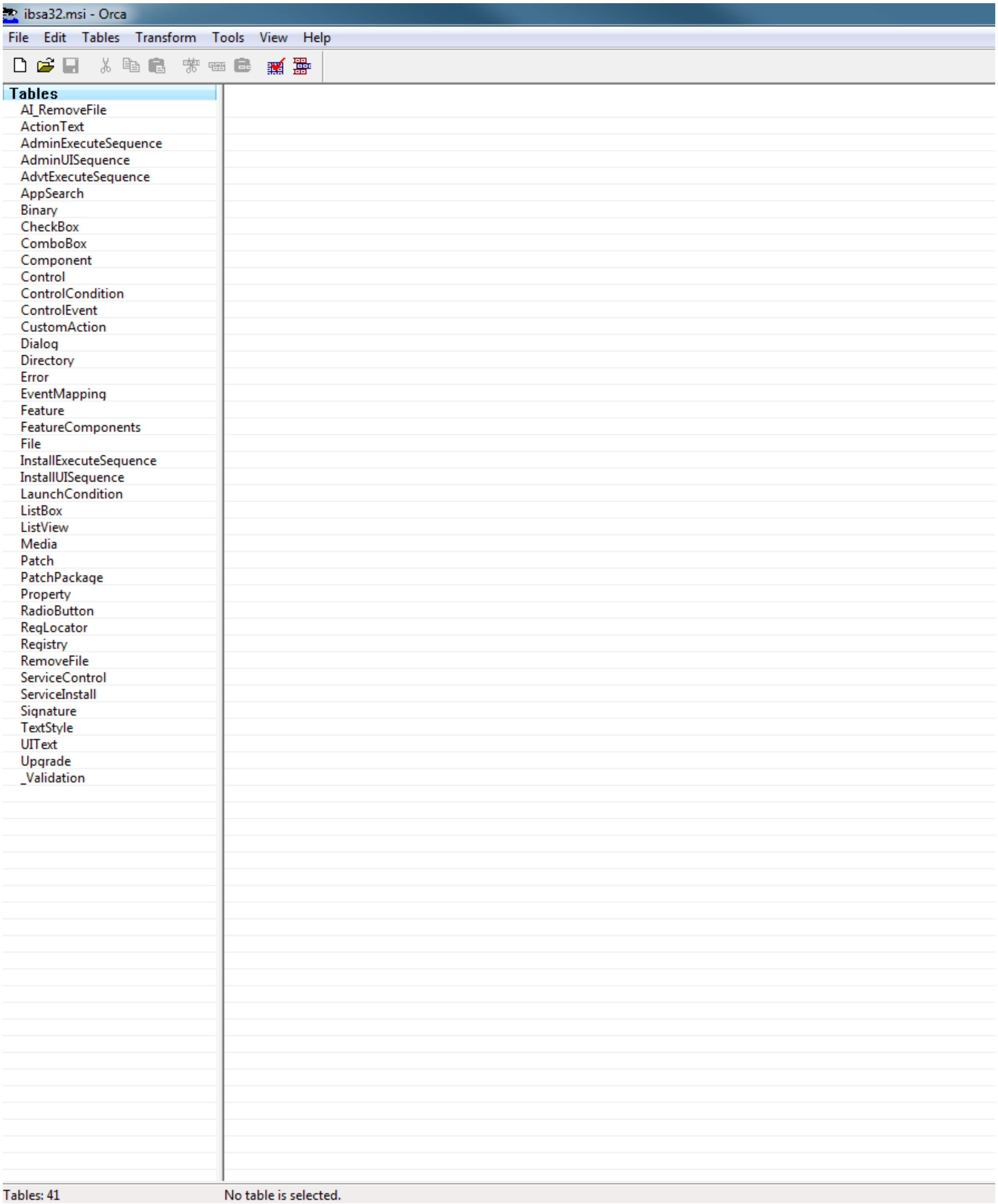
1. ibsa32.msi (Installer for 32-bit systems)
2. ibsa64.msi (Installer for 64-bit systems)
3. Orca.msi (Microsoft tool for modifying .msi installers to customize for your environment)

NOTE: Under the gen3 installer folder, you'll find a win7 and win8 install folder. The win7 installer folder is compatible with all Windows versions up to and including Windows 7. The win8 installer folder is compatible with Windows 7 and above including Windows 8.

If you do not have Orca installed on your system, install this on the computer that will be used to prepare the installers. Orca is not required on the computer that will be filtered by the mobile client. It is only used on the computer that will prepare the installers.

Once Orca is installed on the system, modify both the ibsa32.msi installer and ibsa64.msi installers. To do this, right click on ibsa32.msi installer and select the new menu option "Edit with Orca". This option is only available after Orca is installed on your system.

This will bring up the dialog below:



Tables

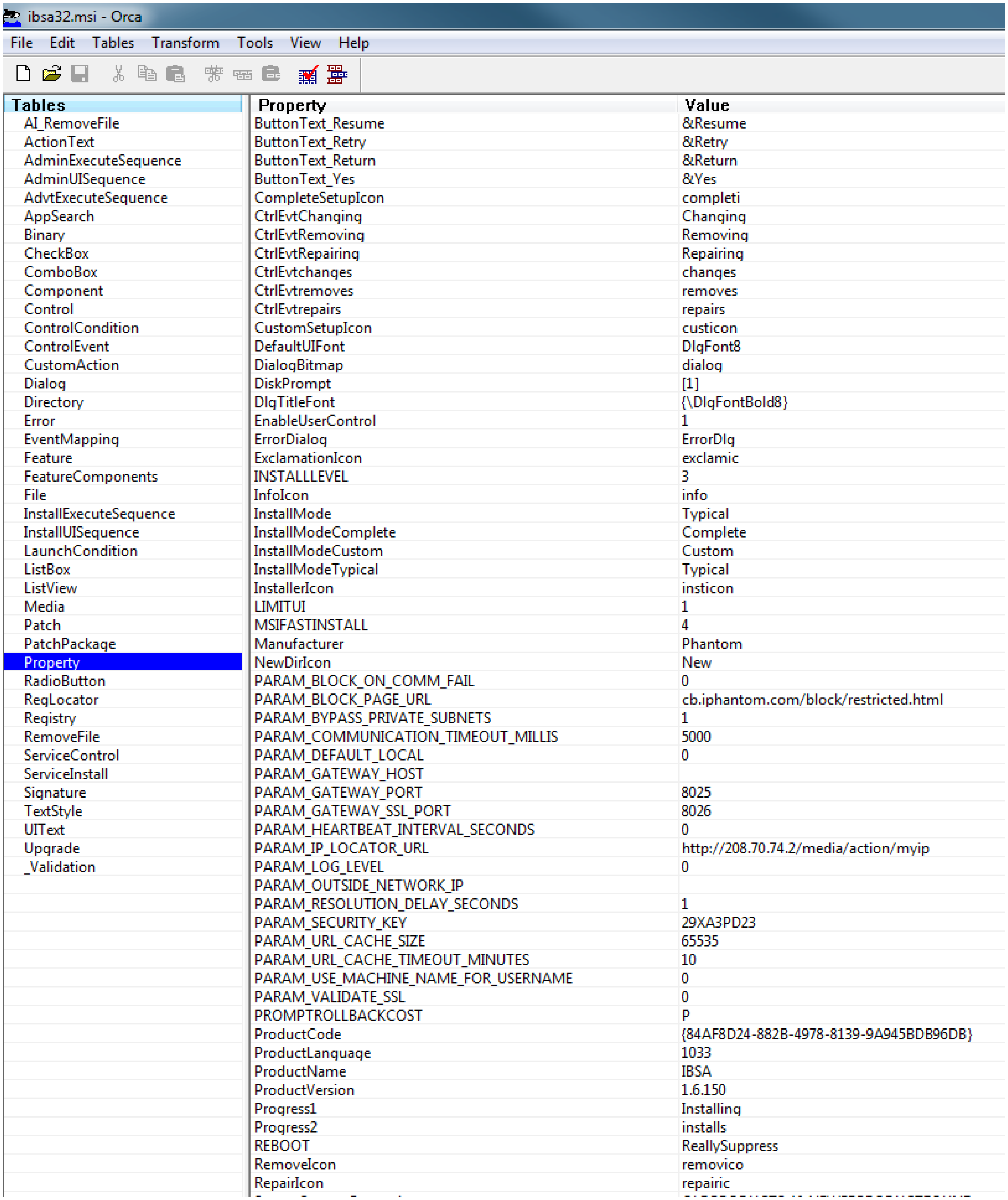
AI_RemoveFile
ActionText
AdminExecuteSequence
AdminUISequence
AdvtExecuteSequence
AppSearch
Binary
CheckBox
ComboBox
Component
Control
ControlCondition
ControlEvent
CustomAction
Dialog
Directory
Error
EventMapping
Feature
FeatureComponents
File
InstallExecuteSequence
InstallUISequence
LaunchCondition
ListBox
ListView
Media
Patch
PatchPackage
Property
RadioButton
RegLocator
Registry
RemoveFile
ServiceControl
ServiceInstall
Signature
TextStyle
UIText
Upgrade
_Validation

Tables: 41   No table is selected.

Figure 2 – Orca

This allows you to modify the actual file contents of the ibsa32.msi installer.

Select “Property” from the tree menu on the left. Then sort the right display contents by Property name by clicking on the Property column at the top of the right window pane. Scroll down to the section of properties tagged with the label name PARAM_.



Tables

- AI_RemoveFile
- ActionText
- AdminExecuteSequence
- AdminUISequence
- AdvtExecuteSequence
- AppSearch
- Binary
- CheckBox
- ComboBox
- Component
- Control
- ControlCondition
- ControlEvent
- CustomAction
- Dialog
- Directory
- Error
- EventMapping
- Feature
- FeatureComponents
- File
- InstallExecuteSequence
- InstallUISequence
- LaunchCondition
- ListBox
- ListView
- Media
- Patch
- PatchPackage
- Property
- RadioButton
- RegLocator
- Registry
- RemoveFile
- ServiceControl
- ServiceInstall
- Signature
- TextStyle
- UIText
- Upgrade
- _Validation

Property	Value
ButtonText_Resume	&Resume
ButtonText_Retry	&Retry
ButtonText_Return	&Return
ButtonText_Yes	&Yes
CompleteSetupIcon	completi
CtrlEvtChanging	Changing
CtrlEvtRemoving	Removing
CtrlEvtRepairing	Repairing
CtrlEvtchanges	changes
CtrlEvtremoves	removes
CtrlEvtrepairs	repairs
CustomSetupIcon	custicon
DefaultUIFont	DlgFont8
DialogBitmap	dialog
DiskPrompt	[1]
DlgTitleFont	{\DlgFontBold8}
EnableUserControl	1
ErrorDialog	ErrorDlg
ExclamationIcon	exclamic
INSTALLLEVEL	3
InfoIcon	info
InstallMode	Typical
InstallModeComplete	Complete
InstallModeCustom	Custom
InstallModeTypical	Typical
InstallerIcon	insticon
LIMITUI	1
MSIFASTINSTALL	4
Manufacturer	Phantom
NewDirIcon	New
PARAM_BLOCK_ON_COMM_FAIL	0
PARAM_BLOCK_PAGE_URL	cb.iphantom.com/block/restricted.html
PARAM_BYPASS_PRIVATE_SUBNETS	1
PARAM_COMMUNICATION_TIMEOUT_MILLIS	5000
PARAM_DEFAULT_LOCAL	0
PARAM_GATEWAY_HOST	
PARAM_GATEWAY_PORT	8025
PARAM_GATEWAY_SSL_PORT	8026
PARAM_HEARTBEAT_INTERVAL_SECONDS	0
PARAM_IP_LOCATOR_URL	http://208.70.74.2/media/action/myip
PARAM_LOG_LEVEL	0
PARAM_OUTSIDE_NETWORK_IP	
PARAM_RESOLUTION_DELAY_SECONDS	1
PARAM_SECURITY_KEY	29XA3PD23
PARAM_URL_CACHE_SIZE	65535
PARAM_URL_CACHE_TIMEOUT_MINUTES	10
PARAM_USE_MACHINE_NAME_FOR_USERNAME	0
PARAM_VALIDATE_SSL	0
PROMPTROLLBACKCOST	P
ProductCode	{84AF8D24-882B-4978-8139-9A945BDB96DB}
ProductLanguage	1033
ProductName	IBSA
ProductVersion	1.6.150
Progress1	Installing
Progress2	installs
REBOOT	ReallySuppress
RemoveIcon	removico
RepairIcon	repairic

Figure 3 - Windows Installer Properties

There are many configurable options for the mobile client. Of all the properties, there are only a few properties which need to be changed to match your network configuration.

PARAM_GATEWAY_HOST	This should be the IP Address (or DNS Host name) of the iBoss as visible by mobile computers when OUTSIDE of your network. This IP must be publically accessible on TCP ports 8025 and 8026.
PARAM_SECURITY_KEY	Change this to match the security key on the iBoss Mobile Client configuration page that corresponds to the filtering group you would like the mobile client filtered by when outside of your network.
PARAM_OUTSIDE_NETWORK_IP	The public IP Address (or addresses) of the local network to which the private IP Addresses are NAT'd when on the local network. Enter single IPs or IP ranges in the following format (38.50.10.5,38.50.10-7-38.50.10.12). If there is only one public IP, enter it by itself.

In addition, if you will be using the agent to perform LOCAL network SSL content inspection (NOT REQUIRED for mobile filtering/security or SSL blocking), the following options should be set (available in gen3 agents only):

PARAM_LOCAL_GATEWAY_HOST	(gen3) This should be the local IP Address of the iboss as seen on the local network.
PARAM_LOCAL_GATEWAY_SECURITY_KEY	(gen3) Change this to match the security key on the Mobile Client/Local SSL Inspection configuration page for "Local SSL Agent Security Key". This key is not group specific.
PARAM_LOCAL_SSL_AGENT	(gen3) Set this to 1 if the agent will be used for local SSL inspection. If the agent will only be used for mobile filtering/security, leave this set to 0 and do not enter values for any of the values in this section
PARAM_ALWAYS_LOCAL	(gen3) Set this to 1 if the agent will ONLY be used for local SSL inspection and will not be used for mobile security.

The rest of the properties are optional and are typically not modified.

If you would like the agent to perform a system reboot after detecting an upgrade, set the following property:

PARAM_RESTART_AFTER_UPGRADE = 1

This option is available on gen3 installers only. A restart is required when moving from a gen2 agent to a gen3 agent. This option can be used if moving between gen2 and gen3 is necessary.

Save the MSI installer. This creates the custom installer for your network. Repeat the steps for the 64-bit installer.

Once you have modified the installer, install the ibsa32.msi (or ibsa64.msi for 64-bit systems) on the mobile computer by double clicking the installer.

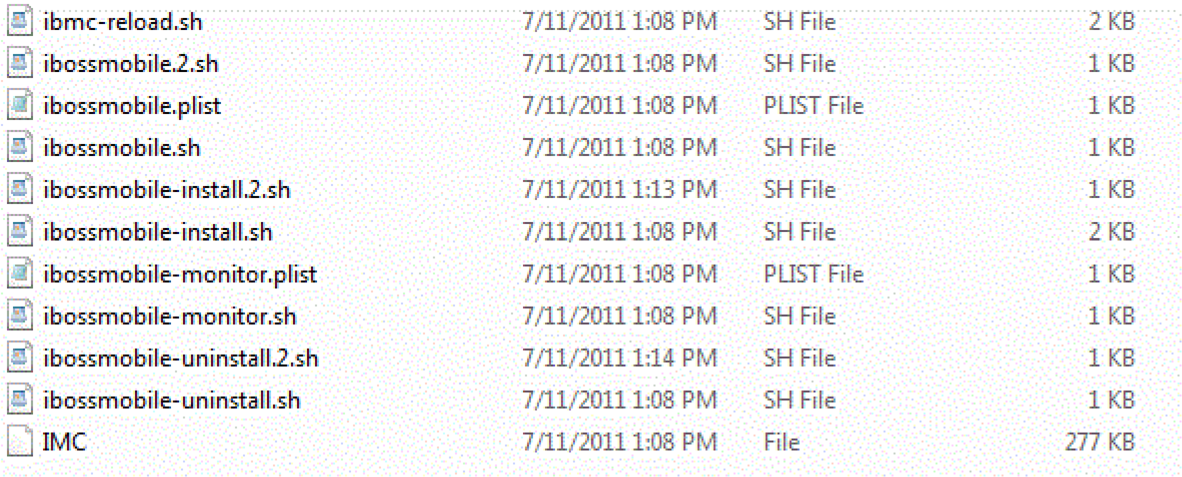
You can also push the installer via Active Directory. Make sure that the 64-bit installer is used for 64-bit systems and 32-bit installer is used for 32-bit systems.

This completes the install of the mobile agent/local SSL inspection agent.

Installing the Mac Agent

Installing the Mac agent involves downloading the agent onto the Mac computer, extracting the compressed files to a directory, adjusting settings through one or more of the files extracted, then running the installer. An install and uninstall script are provided which handles configuring and fully removing the plugin from the system. You must have the "root" password to the system in order to install the agent which runs under root privileges.

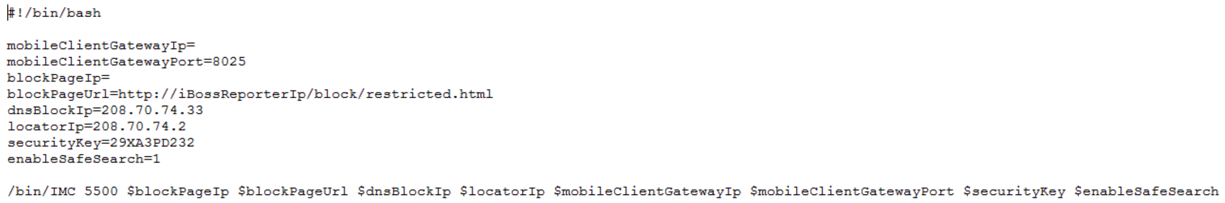
Download and extract the files from the file ibossmobile.tar.gz onto the Mac computer. The extracted files will contain a folder labeled installpack which contains two directories, 10.5 and 10.6. Depending on the Mac OS, you will want to use the files from either the 10.5 or 10.6 directory. For Snow Leopard (Mac OSX 10.6.x), use the 10.6 folder. The following files should be present:



ibmc-reload.sh	7/11/2011 1:08 PM	SH File	2 KB
ibossmobile.2.sh	7/11/2011 1:08 PM	SH File	1 KB
ibossmobile.plist	7/11/2011 1:08 PM	PLIST File	1 KB
ibossmobile.sh	7/11/2011 1:08 PM	SH File	1 KB
ibossmobile-install.2.sh	7/11/2011 1:13 PM	SH File	1 KB
ibossmobile-install.sh	7/11/2011 1:08 PM	SH File	2 KB
ibossmobile-monitor.plist	7/11/2011 1:08 PM	PLIST File	1 KB
ibossmobile-monitor.sh	7/11/2011 1:08 PM	SH File	1 KB
ibossmobile-uninstall.2.sh	7/11/2011 1:14 PM	SH File	1 KB
ibossmobile-uninstall.sh	7/11/2011 1:08 PM	SH File	1 KB
IMC	7/11/2011 1:08 PM	File	277 KB

Figure 4 - Mac Mobile Agent Files

The ibossmobile-install.sh file is the installer while the ibossmobile-uninstall.sh is used to uinstall the agent. ibossmobile-install.2.sh and ibossmobile-uninstall.2.sh should not be used and are present for special circumstances. After extracting the files, you will want to open and modify two files, namely ibossmobile.sh and ibmc-reload.sh. Start by opening and modifying the file ibossmobile.sh. A snapshot of this file is shown below:



```
#!/bin/bash

mobileClientGatewayIp=
mobileClientGatewayPort=8025
blockPageIp=
blockPageUrl=http://iBossReporterIp/block/restricted.html
dnsBlockIp=208.70.74.33
locatorIp=208.70.74.2
securityKey=29XA3PD232
enableSafeSearch=1

/bin/IMC 5500 $blockPageIp $blockPageUrl $dnsBlockIp $locatorIp $mobileClientGatewayIp $mobileClientGatewayPort $securityKey $enableSafeSearch
```

Figure 5 - Mac Mobile Client Settings - ibossmobile.sh

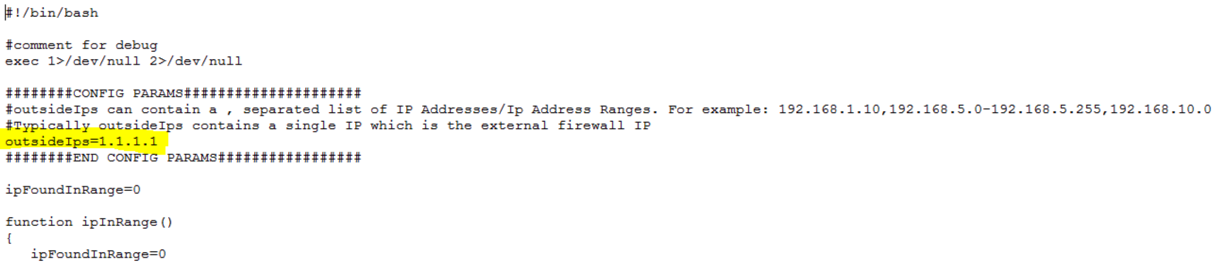
The table below describes the settings in this file that must be modified:

Setting	Description
mobileClientGatewayIp	This is the IP Address of the iBoss which will be the filtering service for the mobile client. This address must be accessible from the Internet. If the iBoss is behind a firewall, you must allow access to the iBoss from the outside IP of the network where the iBoss resides (via an access rule on the firewall or by port forwarding the outside IP to the local IP of the iBoss).
mobileClientGatewayPort	This port defaults to 8025. This is the port that is configured on the Mobile Client settings page on the iBoss under the global section.
blockPageIp	This is the IP address of the server that is hosting the block page. If you do not have a publicly available block page, use the block page hosted by iBoss Web Filters (208.70.74.18).
blockPageUrl	This is the URL to the block page. The host portion of the URL should match the IP address configured for blockPageIp. If you are using the block page hosted by iBoss Web Filters, enter http://208.70.74.18/block/restricted.html.
dnsBlockIp	This should contain an IP address that hosts a block page whenever a DNS based block redirect is sent by the mobile client. When a page is blocked by DNS, the browser will make a web request for the index page at this IP which should contain a block page. The default 208.70.74.33 is the default hosted page.
locatorIp	This IP is used by the agent to determine whether the client is local on the network (being actively filtered directly by the iBoss appliance) or remote (being filtered by the mobile agent). Leave the default IP of 208.70.74.2.
securityKey	This key should match the security key on the iBoss Web

	Filter Mobile Client page for the group who's filtering rules you want to apply while this computer is off the network. On the Mobile Client page, each filtering group tab is associated with a security key. By matching this security key with the correct group, the iBoss will apply the filtering rules for that corresponding group while the computer is off the network.
enableSafeSearch	Indicates you would like the mobile agent to enforce safe search on Google, Yahoo, Youtube, and Bing while the computer is off the network.

Once you have configured the settings above, save the ibossmobile.sh file.

Next, you will want to adjust the settings in the file ibmc-reload.sh which is shown below:



```
#!/bin/bash

#comment for debug
exec 1>/dev/null 2>/dev/null

########CONFIG PARAMS#####################
#outsideIps can contain a , separated list of IP Addresses/Ip Address Ranges. For example: 192.168.1.10,192.168.5.0-192.168.5.255,192.168.10.0
#Typically outsideIps contains a single IP which is the external firewall IP
outsideIps=1.1.1.1
########END CONFIG PARAMS#################

ipFoundInRange=0

function ipInRange()
{
   ipFoundInRange=0
```

Figure 6 - Mac Mobile Client Settings - ibmc-reload.sh

The only setting in this file you will need to adjust is the "outsideIps" setting. The IP address (or IP Addresses) entered for this field indicate the outside IP of the local network as seen from the outside when the computer is on the local network. For example, if your computer was on the local network being filtered by the iBoss appliance directly and you were to visit a website like http://www.whatismyip.com, the IP Address that shows on this website would be the value entered here. If your network owns more than one public IP that may appear from clients surfing on the local network, you can enter them all by using a comma. Ranges of IPs can also be entered by using a dash "-". For example, to include a range from 38.189.22.50 to 38.189.22.70, just enter the value 38.189.22.50-38.189.22.70 into this field. Use a comma to separate one or more IPs or IP ranges. Once you are done editing this file, save and close the file.

Now run the installer script ibossmobile-install.sh to install the mobile client agent. Rebooting is required for the mobile agent to take affect and you will be prompted for the root password when running the installer if you have not become root via the super user command (su - root).

Once the agent is installed, it will automatically detect whether you are on the local network being filtered directly by the iBoss appliance or remote in which case the mobile agent will provide filtering.

Understanding How the Mac Mobile Agent Works

The Mac Mobile Agent filters by intercepting packets from all interfaces as the flow from the Mac Computer. It then performs reassembly of the streams and sends DNS queries and URL requests to the iBoss Web Filtering appliance for classification. The iBoss Appliance applies the filtering rules with the associated group whose security key (under the Mobile Client page) matches the one configured in the ibossmobile.sh file. The iBoss then logs the request in real-time and responds with either an indication that the page should be allowed or blocked in which case the agent either allows the page or presents the block page.

Once the agent is installed, it creates a file under the /bin/ directory called ibmc_im. This file (whose initials stand for iboss mobile client is mobile) contains a single value of either 1 or 0. A value of 1 indicates that the agent thinks the computer is currently mobile (off the main network). A value of 0 indicates that the agent thinks the computer is currently on the main network in which case the agent does not provide any filtering and relies on the iBoss appliance on the main network to perform all of the filtering. When testing, this value should accurately reflect either 1 or 0 when moving on and off the network.

Troubleshooting the Mac Mobile Client

There are a number of reasons the Mac Mobile Client may not work properly. This section describes troubleshooting steps to diagnose the problem.

1. Check to make sure the agent is properly detecting when the computer is on and off the network.

An improper setting for the setting outsideIps in ibmc-reload.sh will prevent the agent from properly determining when the computer is off the network. The agent relies on this setting to determine whether the computer is on or off the network so that it will filter only when the computer is off the network.

First check the file /bin/ibmc_im using the more command. Ideally you should have already become super user by running the command:

```
su - root
```

an entering the root password. Once you are logged in as root using the above command, run the command:

```
more /bin/ibmc_im
```

You should see either a value of 0 or 1 depending on whether you are on or off the network. If you are on the primary network, you should see a value of 0 (in which case no filtering will be applied by the mobile agent). If you are off the network you should see a value of 1 in which case the mobile agent is providing filtering. Move on and off the network and notice the value of this file change properly.

If the value is not correct, open the file ibmc-reload.sh and adjust the value of outsideIps to reflect all of the outside (publicly visible) IPs of the main network.

2. Check to make sure the iBoss is accessible from outside the network.

The mobile client must communicate with the iBoss while it's filtering a computer off of the main network. It typically does this via TCP requests on port 8025. The mobile agent will send these TCP requests while outside the local network to the IP Address that is configured in the file ibossmobile.sh under the setting mobileClientGatewayIp.

If the value set for mobileClientGatewayIp is not correct, the agent will not be able to communicate with the iBoss and surfing off of the network will either be extremely slow or you will not be able to surf at all. The first thing you will want to do is check the value of mobileClientGatewayIP in the file ibossmobile.sh and make sure it is correct.

If the iBoss is behind a firewall or NATing firewall, the mobile agent will not be able to communicate with the iBoss while off the network because the firewall will prevent this communication. With a NATing firewall, you will want to configure a port forwarding rule that forwards traffic destined for the outside IP on port 8025 to the local IP of the iBoss. This will allow the mobile client to communicate with the iBoss while off of the network. Confirm that the firewall allows communication with the iBoss via TCP port 8025 from outside of the network.

3. Confirm that the iBoss Mobile Agent is running.

The mobile agent runs under a process named IMC. To confirm that this process is running, run the command:

```
ps -ef | grep IMC
```

You should see the mobile agent running as an active process with results similar to below:

```
0   98   1  0   0:09.49  ??       0:10:37       /bin/IMC 5500 38.104.122.22
http://38.104.122.22:8080/block/restriced.html 208.70.74.33 208.70.74.2 38.104.122.22
8025 29XA3PD232 1
0   6317    182   0    0:00.00  ttys000      0:00.01  grep IMC
```

If you only see the grep line above, this means the agent is not running and you should try running the uninstaller and then the installer again. Also, you may be installing the wrong version. If the Mac is on OSX 10.5, you should use the installer in the 10.5 directory.

4. Confirm the firewall rules are in place

The agent automatically configures the firewall rules in order to divert packets into the agent for filtering. Confirm that the rules are in place by running the following command:

```
ipfw list
```

You should run this command while being a root super user (via the command su - root). You should see something similar to the following:

```
00001 allow ip from any to 38.104.122.22 out
00002 allow ip from any to 38.104.122.22 out
00003 allow ip from any to 208.70.74.33 out
00004 allow ip from any to 208.70.74.2 out
00005 divert 5500 ip from any to any out
65535 allow ip from any to any
```

If you only see the rule:

```
65535 allow ip from any to any
```

then the firewall rules were not installed in place and something is wrong with the install. You may want to run the uninstaller and re-install the mobile agent.

When imaging a Mac using Casper, there have been cases where the image created is not an exact copy of the original. This causes the rules above to not be installed properly. A solution to this is to use the utility diskutil in Mac to create the image and then use Casper to restore the image onto the Mac receiving the image.

3 Troubleshooting

Clients will show up on the mobile client configuration page and on the 'Identify Computers & Users'. The strategy for troubleshooting filtering is similar to any other client. The strategy for troubleshooting network connectivity or port forwarding is not specific to the iBoss. (Mac clients may not appear in the Computers list - 11/21/2011)

General procedures for testing the Mobile Client:

- Contact iBoss Support for help in verifying accessibility of tcp port 8025 and 8026
- Use a DNS tool pointing to the external IP that is set up with a port forward to the iBoss (Only for Gen 1 Windows Mobile Client)
  (nslookup at Windows command prompt, dig in Mac Terminal)
- Change logging level to 1 or 2 to see what agent is determining.

Gen 1 Windows

From "on network":

- Ensure the client is using the appropriate DNS servers
  ('ipconfig /all' for Windows)
- Ensure interfaces are using DHCP (static IPs & DNS server config may not work).

From "Off network":

- Ensure full networking and Internet access is working with Mobile Client service stopped
  (renew IP info after stopping service)
- Ensure the DNS service is available from the location.
  Use DNS tools and point to public address.

Note the counters on the Mobile Client configuration page.

Please use one of the following for support:

Website Support: http://support.iboss.com/
Telephone Support: 1.877.PHANTECH (742.6832)
E-mail Support: support@iPhantom.com