

Mobile Client Agent

iBoss Web Filters

Copyright © Phantom Technologies Inc.. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in chemical, manual or otherwise, without the prior written permission of Phantom Technologies Inc.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

www.iBossWebFilters.com

Table of Contents

TABLE OF FIGURES	3
1 MOBILE CLIENT AGENT.....	4
1.1 OVERVIEW	4
1.2 KEY FEATURES	4
2 GETTING STARTED	4
2.1 OVERVIEW	4
2.2 iBOSS CONFIGURATION.....	5
2.2.1 <i>Global Settings</i>	6
2.2.2 <i>Mapping Mobile Clients</i>	6
2.2.3 <i>Additional Configuration</i>	6
2.3 NETWORK PREPARATION	6
2.3.1 <i>Most Common Configuration</i>	6
2.3.2 <i>Alternate Scenarios</i>	7
2.4 MOBILE CLIENT AGENT INSTALLATION.....	7
2.4.1 <i>Windows</i>	7
2.4.2 <i>Mac</i>	11
3 OPERATION	12
4 TROUBLESHOOTING	13

Table of Figures

Figure 1 - iBoss Mobile Client Configuration	5
--	---

1 Mobile Client Agent

1.1 Overview

The iBoss Mobile Client 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. 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 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**

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

iBoss Enterprise SWG
Web/Application/Bandwidth Management 1550
Computer IP: 10.128.25.70
Current Filtering Group: No Filtering

Mobile Client Agent
Current Filtering Group: 1. Default

Default OverrideU Houst Emp Employees Override

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

Refresh Apply

MAP MOBILE CLIENT TO USERNAME [?]

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

Add

Mapped Mobile Clients
No Entries

Remove Download Agent Done

© 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 (Gen 2) - Recommended

Extract the mobile client from the windows->gen2 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)

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:



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	Property	Value
AI_RemoveFile	ButtonText_Resume	&Resume
ActionText	ButtonText_Retry	&Retry
AdminExecuteSequence	ButtonText_Return	&Return
AdminUISequence	ButtonText_Yes	&Yes
AdvtExecuteSequence	CompleteSetupIcon	completi
AppSearch	CtrlEvtChangingq	Changingq
Binary	CtrlEvtRemovingq	Removingq
CheckBox	CtrlEvtRepairingq	Repairingq
ComboBox	CtrlEvtchanges	changes
Component	CtrlEvtremoves	removes
Control	CtrlEvtrepairs	repairs
ControlCondition	CustomSetupIcon	custicon
ControlEvent	DefaultUIFont	DlgFont8
CustomAction	DialogBitmap	dialogq
Dialog	DiskPrompt	[1]
Directory	DlgTitleFont	{\DlgFontBold8}
Error	EnableUserControl	1
EventMapping	ErrorDialog	ErrorDlg
Feature	ExclamationIcon	exclamic
FeatureComponents	INSTALLLEVEL	3
File	InfoIcon	info
InstallExecuteSequence	InstallMode	Typical
InstallUISequence	InstallModeComplete	Complete
LaunchCondition	InstallModeCustom	Custom
ListBox	InstallModeTypical	Typical
Listview	InstallerIcon	insticon
Media	LIMITUI	1
Patch	MSIFASTINSTALL	4
PatchPackage	Manufacturer	Phantom
Property	NewDirIcon	New
RadioButton	PARAM_BLOCK_ON_COMM_FAIL	0
ReqLocator	PARAM_BLOCK_PAGE_URL	cb.iphantom.com/block/restricted.html
Registry	PARAM_BYPASS_PRIVATE_SUBNETS	1
RemoveFile	PARAM_COMMUNICATION_TIMEOUT_MILLIS	5000
ServiceControl	PARAM_DEFAULT_LOCAL	0
ServiceInstall	PARAM_GATEWAY_HOST	
Signature	PARAM_GATEWAY_PORT	8025
TextStyle	PARAM_GATEWAY_SSL_PORT	8026
UIText	PARAM_HEARTBEAT_INTERVAL_SECONDS	0
Upgrade	PARAM_IP_LOCATOR_URL	http://208.70.74.2/media/action/myip
_Validation	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-4978-8139-9A945BD896DB}
	ProductLanguage	1033
	ProductName	IBSA
	ProductVersion	1.6.150
	Progress1	Installing
	Progress2	installs
	REBOOT	ReallySuppress
	Removelcon	removico
	Repairlcon	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.

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

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.

2.4.3 Mac

!!NOTE: iBoss firmware version must be at least 6.0.12.0

!!NOTE: An alternate package is available that does not use Login Hooks.

Extract the archive from the Mac folder. The archive contains several files which are currently changing frequently as development incorporates different configurations.

In general, you need to edit ibossmobile.sh and ibmc-reload.sh with your local information, then run the "-install" script as root (sudo) from the installation folder. The installation can be run manually or pushed via whichever methods you normally use (i.e. Casper).

ibossmobile.sh or
iboss.mobile.agent.sh

```
#!/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
cacheSize=50000
```

mobileClientGatewayIp: The public IP for access to the iBoss DNS while NOT on local net.
blockPageIp: use 208.70.74.18 unless there is a local address to substitute.
blockPageUrl: You may use the above blockPageIp for the iBossReporterIp
securityKey: The Security Key of the Filter Group from iBoss Mobile Client configuration.

ibmc-reload.sh or
iboss.mobile.reload.sh

```
#####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
defaultLocal=1
#####END CONFIG PARAMS#####
```

outsideIps: This is the address(es) that the public Internet may see as the client IP when it is on the LOCAL net (NATed IPs). Typically this is the outside address of the firewall. If there are additional addresses they may be listed as described in the comments.
defaultLocal: This determines whether the filter agent defaults to local access if the iBoss is not accessible.

3 Operation

At computer bootup (service start) the Agent attempts to determine if it resides on the local LAN or remote.

- If on local LAN:
Computer is allowed to operate as normal.
- If remote:
Agent will filter Internet access based on responses from the Enterprise iBoss filter policy previously assigned.
- If remote but a VPN interface is detected:
There are two options for special handling of this. The "UseLocal..." and "UseRemote..." options look for VPN interface names.

4 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.iphantom.com/>

Telephone Support: 1.877.PHANTECH (742.6832)

E-mail Support: support@iPhantom.com