Table of Contents

Overview Licensing Requirements Prerequisites and Guidelines Gen. 2/Gen. 3 Instructions Gen. 4 Mac Agent Instructions Configuration Example Troubleshooting Additional References

Overview

The iboss Mac Agent is used to provide filtering and protection for devices that will connect to the Internet from outside of an iboss-protected organization's network. In addition, the Mac Mobile Agent can be configured to provide data inspection, leveraging SSL Decryption.

Currently there are two options when providing filtering/protection via an agent for macOS devices:

Option 1 - Filtering the device by combining Proxy and NetID The agent settings can be configured and deployed via Apple Configurator, an MDM solution, or manually. The PAC Script is intelligent and can proxy when the device is off the network and route traffic directly through iboss when on-site. The NetID will transparently assist in identifying logged-on users when on and off the network. *Note: The iboss Mac Agent used on macOS 10.9.x and prior is not compatible with 10.10.x and above.*

Option 2 - Using the iboss Mac Agent in VPN Mode This will result in tunneling all traffic destined for the Internet via an iboss Gateway Node. Once again intelligence is built into the agent and platform to know when a user's device is either on or off the network.

Licensing Requirements

Core, Malware Defense, or Data Loss Prevention iboss Cloud subscription.

Prerequisites and Guidelines

At least one web gateway is required. There are no prerequisites to communicate with iboss Cloud.

Gen. 2/Gen. 3 Instructions

Login to https://ibosscloud.com

Option 1 – Mac Agent Configuration (Proxy and NetID Mode)

Navigate to the Data Redirection Module > Agents



Click on Mac Agents

Data Redirection	Home > Data Redirection > Agents > Mac Agents
- 🖽 Agents 🔷 🔨	Mac Agents Settings
- 😃 General	
- 😐 Windows Agents	Group Specific Settings
– 😐 Mac Agents	Group: < 1. Default v > Q
 Chromebook Agents 	Security Key 29XA3PD231
(Jecuity rey
	General IP Information
	Cluster DNS https://cluster122164- swg.ibosstest.com
	Device IP 210.1.91.146
	Gateway Port 8025
	SSL Gateway Port 8026
	Mac Agent Setup
	DOWNLOAD Mac Agent DOWNLOAD Mac Configuration Instructions

Download the **"Mac Agent"** and unzip the security agent files. Select 10.10-10.11 for any device using Yosemite OS or above.

Select "10.10-10.11"



Click and edit the "iboss.conf"



The parameters configured in iboss.conf control the overall operation and timing. The data configured should be immediately after the equal sign with no spaces anywhere on the line.

	iboss.conf ~	
<pre># Please refer to README.txt mobileNetIDiboss= localNetIDiboss= netIDKey=8H29DA6N31 outsideIps=1.1.1.1 ibossApplePort=8015 ibHeartBeat=300 defaultLocal=0 autoProxyURL= NIDDEBUG=0</pre>	in original installation	files for instructions

Item	Description
mobileNetIDiboss	The public IP or DNS name of the IP configured to forward to the iboss private IP.
localNetIDiboss	The private IP or DNS name of the iboss.
netIDKey	The Security Key from the iboss NetID SSO page corresponding to the profile which will become either the Filter Policy or have the LDAP lookup settings to determine the Filter Profile.
outsidelps	A list of the public IPs, comma separated, that your clients are NAT'd to while on-network.
ibossApplePort	The port in which the credentials are sent over transparently. There is rarely a reason to change this port. It would have to be changed on the iboss and firewall.
ibHeartBeat	The frequency in which this agent sends a heartbeat to the iboss registering the IP currently used by the device.
defaultLocal	Special case use. In case of certain failures this setting determines whether the agent reverts to working as if on local network (1) or mobile (0).
autoProxyURL	The URL of the PAC script used by auto-proxy. This script must be customized for your use.
NIDDEBUG	Special case use. 1=reload log, 2=reload and loop logging is directed to files under /var/log/ Console logging may also be enhanced.

Click on "User Single Sign On" then select "iboss NetID SSO"



Enable "Mac Registration Agent"

Select the filter group and copy the appropriate group security key and paste into the iboss.conf.

Optional: "**Extract Group From LDAP**" If the user is intending to extract the group from LDAP it is recommended to push all mobile clients out with the 'Default' security key and enable extract group from LDAP. Otherwise deploy the agent with the appropriate key.

W Oser single sign-On *	ibossNetID Single Sign-On Agent	9
- 🗇 BYOD	Save & Download SSO Agent	
 		Group: < 1. Default V > Q
 A LDAP Settings 	Groups Specific Settings	
- 🌣 AD Plugin	Enable Mac Registration Agent	YES
■ Google SSO	chable mac registration Agent	
🤗 iboss NetID SSO	Enable ibossNetID Agent	
eDirectory		
· · · · · · · · · · · · · · · · · · ·	Group Security Key	BH290AbN31
	Default Group	The group associated with this key
	Extract Group From LDAP	None *
	Query LDAP Only For Logins To Domain	
	ibossNetID Session Timeout	300
	ibossNetID Replay Window	10800
	ibossNetID Source IP Verification	YES
	Gateway Hosts	38.96.13.177

Next, Configure the Proxy. Click on **Data Redirection > Proxy**



Enable Proxy Settings

Set "Filtering Method" to Proxy Mode

Set "User Authentication Method" to Mobile Devices (Source IP Based)

7/31/2018

Save Actions -			
NS Settings			
	Proxy Port	8009	
	DNS Host	https://cluster17-swg.ibosscioud.com	
ettings			
	Enable Proxy Settings	YES	
	Filtering Method	Proxy Mode	٣
	NTLM Authentication Port	8008	
	User Authentication Method	Mobile Devices (Source IP Based)	*
	Unidentified User Group Action	Use Default Filtering Group	*
	Default Landing Page	www.google.com	
	Enable Inline Provy		

Note: a PAC script is needed and you will need to host it somewhere that you have access to edit such as a Webserver.

Option 2 - Mac Agent Configuration (VPN Mode)

CORE

Click on Data Redirection > IPsec Tunnels

Switch the IPsec Settings Enable toggle to "Yes"



Navigate to the Data Redirection > Agents



Switch the Global Settings Enable Security Agent Filtering toggle to "Yes"



Click on + New Local Subnet/IP Range

Add your Public IP Address in the "IP Address" field followed by the "Subnet Mask" field for either your single Public IP Address or your Range/Subnet. *Note:* This helps to make the agent aware of when users are on or off the organizations network.

Add Local Subnet/IP Range 😮		>
Type *	Subnet	\$
IP Address	1.1.1.2	
Subnet Mask	255.255.255.255	

Click Save

Navigate to the Users, Groups & Devices Module > Users & Devices



Click on Add Device



Set "Device Type" to Mobile Device via IPsec Tunnel

Next specify a name for your macOS Devices in the "Device Name" field.

Then leave both "IPsec Username" and "IPsec Password" fields empty.

For the "IP Addresses to Allocate" field, you will need to specify enough IP Address for at least 1 per device. **Note:** It is recommended to allocate more IP addresses than there are devices when creating a static device for the Mac Agent.

"Apply Filtering"	by assigning a	a filtering group t	o the Mac o	devices that v	will be utilizing	the Mac Agent	, then Click
on Add Device							

Add Device	×
Device Type	Mobile Device via IPSec Tunnel \$
Device Name	Mac/OSX Devices
IPSec Username	
IPSec Password	
IP Addresses to Allocate	200
Apply Filtering	Group 25 \$
Device Overrides User	YES
Note	
Video Recording	
viceo recording	
Q Identify Me	× Cancel 🗈 Add Device

You can now download the Mac Agent profile by selecting the **blue computer monitor icon** from the "Actions" column button next to the entry you just created under **Groups > Static Devices**

Static Devices	Dynamic Devices	Users			
Actions - +	Show Search 📔 Clear	All High Risk Locks			10 ‡
Device Nar	ne Group Nam	e IP Address 👻	MAC Address	Logged In?	Actions
Mac/OSX D	evices Default (#1)	10.50.0.109 (IP	Sec	-	🖉 🗰 o 🖵 🖪

This profile can then be deployed either by Apple Configurator, an MDM solution, or manually on to the device. To install the profile manually, run the .mobileconfig file on the chosen device.

Click Continue



Click Install. You will then see that the profile has been successfully installed onto the device.

	Promes	C Search
ser Profiles	ikaan Oomaa tiraan ay	
ibossConnect ipsec 2 settings	Profile	PN Configuration
	iboss Cybersecurit	y Unsigned
	Description This profile pr the ibossConr	rovisions the device with nect ipsec profile
	Installed Feb 10, 2017,	11:46 AM
	Settings Certificate	
	VPN Service	
	DETAILS	
	Certificate	
	Description The ibossCon	nect ipsec certificate

Gen. 4 Mac Agent Instructions

This generation has added the option for Auto-Login mode (Option 2 below), which allows iboss Agents/Endpoints to be automatically registered and filtered with a configured server without entering any login information.

Setup for this version is a very similar process to the Gen. 2/Gen. 3 setup. You will instead select the Gen. 4 agent from the zipped agent file you download from the platform, set different parameters in the json-based configuration file and choose an authentication method.

To begin, click this button located in "Mac Agent Setup" section in Data Redirection > Agents > Mac Agents



Open the resulting file and navigate to **iboss Security Agent Sep 2017 > iboss Macintosh OS X Agent >** Install the **gen4agent.pkg**

• • •	🥪 Install GEN IV Agent
	Welcome to the GEN IV Agent Installer
 Introduction Destination Select Installation Type Installation Summary 	You will be guided through the steps necessary to install this software.
ί <mark>bψss</mark> °	Go Back Continue

н

	🥪 Install GEN IV Agent	
	Standard Install on "Macintosh HD"	
 Introduction Destination Select Installation Type Installation Summary 	This will take 30.9 MB of space on your computer. Click Install to perform a standard installation of this for all users of this computer. All users of this comp able to use this software.	s software uter will be
 Introduc Destinat Installat 	Go Back Installer is trying to install new software. Enter your password to allow this. User Name: Developer Decouverd	Install oftware r will be
 Installati Summar Summar 	Password: Cancel Install Software	
	Go Back	Install

Once the agent is installed it must be configured with the values listed under the Option 1 or 2 sections (debending on preference) below.

Option 1- Mac Agent via SAML and Proxy

The Generation 4 agent accelerates proxy-based filtering by automatically configuring the proxy settings and injecting proxy authentication information and SAML authentication cookies.

Note: Proxy based filtering will still work without agents but the agents will speed up the performance and reduce the number of logins the user will need to enter.

Troubleshooting Note: To support this functionality it was necessary to require Basic Authentication on the proxy server. If the client is configured manually (without the agent) then it will be necessary to enter this information. The username is "ibss" and password is "ibss" also.

Web Gateway Setup Information

The Web Gateway must be configured to proxy with SAML-based authentication (**Data Redirection > Proxy > User Authentication Method > SAML**).

Mac Agent Setup

The Mac Agent is configured through a json-based configuration file which is generated as part of installation under /var/root/config.json.

The following values are used to configure Gen. 4 Proxy mode:

Parameter	Description		
RuntimeMode	Set to "gen4_saml"		
GatewayHost	Enter the web gateway or cluster address here e.g. cluster1-swg.ibosstest.com		
GatewayPort	Enter the proxy port (available on the Data Redirection > Proxy page under "Settings"). The default is 8009.		
ProxyMonitorInterval	This value (in milliseconds) controls how often the proxy settings will be checked by the agent (default and minimum is 1000 ms). If the settings are found to be different from wha is configured in the registry then the agent will set them back.		
ProxyOverride	These are addresses that will bypass the proxy server. At a minimum every Web Gateway in the cluster MUST be added e.g. cluster1 contains the Web Gateway cn643828021-cnc6116.ibosstest.com. Separate multiple server names with with semi-colons.		
SAMLSessionCookie	Optional, if a SAML session cookie is known ahead of time then it can be specified here and the user would not need to log in. If unused then set to null.		
AutoProxyURL	The URL of the PAC script used by auto-proxy. This script must be customized for your use.		

Option 2- Mac Agent Auto-Login Mode

Generation 4 Agent accelerates proxy-based filtering by automatically configuring the proxy settings and injecting proxy authentication information.

Note: Proxy based filtering will still work without agents but the agents will speed up the performance and reduce the number of logins the user will need to enter.

Troubleshooting Note: To support this functionality it was necessary to require Basic Authentication on the proxy server. If the client is configured manually (without the agent) then it will be necessary to enter this information. The username is "ibss" and password is "ibss" also.

Web Gateway Setup Information

The Web Gateway must be set to use a proxy data redirection method, with the "User Authentication Method" set to Auto-Login Agents. to do this, log into your iboss Cloud Account and navigate to **Data Redirection > Proxy > Enable Proxy Settings** (if not already active) **>User Authentication Method > Auto Login Agents**). Click the **Save** when finished to preserve these settings.

Mac Agent Setup

The mac agent is distributed as a package (gen4agent.pkg). After the user double clicks on this package, the software is installed under /Applications/iboss/gen4agent/ and the iboss agent application is started.

The Mac Agent is configured through a json-based config file, which is generated as part of installation under /var/root/config.json.

The fields WebSecurityKey, GatewayHost, and GatewayPort will be automatically populated with the appropriate key, host, and port for the cluster from which the agent was downloaded.

If you check your Proxy settings through either your computer or your browser, you will notice that traffic is being directed to a proxy- the same iboss web gateway cluster address will appear here as well.

The user needs to edit this file and provide at least the WebSecurityKey, GetwayHost and GetwayPort. Then, iboss gen4agent needs to be reloaded with the following command:

"/Applications/iboss/gen4agent/reconfigure.sh reload"

The following values can be used to manually configure Gen. 4 Proxy mode:

Parameter	Description		
RuntimeMode	Set to "gen4_auto"		
GatewayHost	Enter the SWG or cluster address here e.g. cluster1-swg.ibosstest.com		
GatewayPort	Enter the proxy port (available on the SWG Proxy page under Settings). The default is 8009.		
ProxyMonitorInterval	This value (in milliseconds) controls how often the proxy settings will be checked by the agent (default and minimum is 1000 ms). If the settings are found to be different from what is configured in the registry then the agent will set them back.		
ProxyOverride	These are addresses that will bypass the proxy server. Separate multiple server names separated by white space.		
SAMLSessionCookie	okie In auto mode, this field is not being utilized.		
AutoProxyURL	The URL of the PAC script used by auto-proxy. This script must be customized for your use.		

Note:

- To stop the service: /Applications/iboss.app/gen4agent/reconfigure.sh unload
- To start the service: /Applications/iboss.app/gen4agent/reconfigure.sh load
- To restart the service: /Applications/iboss.app/gen4agent/reconfigure.sh reload
- Log file is generated under: /Applications/iboss.app/gen4agent/logs

It is best to restart the iboss agent service each time any of the above parameters is manually adjusted.

Acquiring Group Information

At the initial startup of the agent or upon a a user-changed event, the agent checks whether the device is joined to a domain and if the current user is a domain user. If so, it retrieves the group information from the domain controller. If the computer is not joined to a domain or the user is logging into a local account on a domain-joined computer, then the group information will be retrieved from the local user groups.

In the event that the agent does not detect any groups pertinent to the device, the device will fall into your default group and appear in the table under **Users, Groups & Devices > Users and Devices**. From here the device can be moved from the default group to an appropriate one.

Configuration Example

Gen. 2/Gen. 3, Option 1 - Mac Agent Configuration (Proxy and NetID Mode)

These instructions are for installing on a single client.

Edit ibossconf and set the following:

```
# Please refer to README.txt in original installation files for instructions
mobileNetIDiboss=EXTERNAL_IP_OF_IBOSS
localNetIDiboss=LOCAL_IP_OF_IBOSS
netIDKey=SECURITY_KEY_OF_GROUP
outsideIps=List IP's in the NAT pool (comma seperated. dashes are permitted for range)
ibossApplePort=8015
ibHeartBeat=300
defaultLocal=0
autoProxyURL=http://web.mydoamin.com/mobile/mobilepac
NIDDEBUG=0
```

Execute ./install.command on the device to install the agent. A reboot is recommended.

To deploy this package to additional Mac clients, it is only necessary to replicate the 7 files that get placed in the system's folders and ensure the proper owner, group and permissions:

-rw-rr	1 root	wheel	636 May 28 20:44 /Library/LaunchDaemons/iboss.netid.plist
-rw-rr	1 root	wheel	762 May 28 20:44 /Library/LaunchDaemons/iboss.setPAC.plist
-rwx	1 root	wheel	1943 May 28 20:44 /bin/iboss.netid.sh
-rwx	1 root	wheel	4852 May 28 20:44 /bin/iboss.setPAC.sh
-rw-rr	1 root	wheel	12762 May 29 13:24 /var/log/iboss.netID.log
-rw-rr	1 root	wheel	282157 May 29 13:24 /var/log/iboss.setPAC.log
-rw-rr	1 root	wheel	949 May 28 20:44 /etc/iboss.conf

Gen. 2/Gen. 3, Option 2 - Mac Agent Configuration (VPN Mode)

You can open the .mobileconfig file in a text editor, as it is just an XML profile describing the automatically populated VPN configuration.



Navigate to System Preferences > Network on your Mac to display the newly created VPN interface.

Troubleshooting

For Gen. 2/Gen. 3, Option 1 - Mac Agent Configuration (Proxy and NetID Mode)

To troubleshoot Mac Mobile Client when in Proxy and NetID mode, it is recommended to try the following:

- 1. Validate the iboss.conf configuration
- 2. Check file permissions and ensure they have the proper rights.
- 3. Uninstall and reinstall the agent.
 - To remove the mobile client but leave the debug script logging for review:
 - ./install.command kill
 - To completely remove the mobile client including the debug logging:
 - ,/install.commad un

For Gen. 2/Gen. 3, Option 2 - Mac Agent Configuration (VPN Mode)

To troubleshoot the Mac Agent when in VPN mode it is recommended to try the following:

- 1. Verify the what Public IP Address from which the Mac is connecting.
- 2. Check Network Settings on the Mac to be sure that the VPN interface is present.
- 3. Check whether the Profile has been installed correctly on the Mac.
- 4. Open the .mobileconfig file in a text editor to establish whether its connecting to your Gateway Node.
- 5. Check IPsec logs under Data Redirection > IPsec Tunnels > Actions

Additional References

Configuring NetID SSO

Mac Agent Configuration Guide -- iboss Support

Note: This article was last updated in conjunction with the iboss version 9.0.90.200 firmware (released 09/26/2017). You may be using a different version of firmware than the one featured in this article.