Table of Contents

Overview

Most commonly, Agents are used to secure devices that leave the traditional local network boundary, for example, when a user takes their office laptop computer home with them. Historically, devices that were taken outside of the enterprise network would have required the use of a VPN with default routes to backhaul all data to the location where the physical gateway(s) and other services resided to ensure that the security policy was applied consistently. As drivers for VPN diminish (adoption of cloud SaaS solutions replace locally hosted services), residential bandwidth throughput increases and price decreases, cloud secure web gateway have become a more attractive option.

VPNs may still be used for any locally hosted services that have not yet been migrated to the cloud, but all internet traffic can egress through the commodity Internet Service Provider and still be secured using iboss' distributed cloud gateways. The other common use case for deploying security agents is in circumstances where no local gateway is desired or necessary. An example use case for this is a satellite office or retail store.

Licensing Requirements

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

Prerequisites and Guidelines

At least one local or cloud gateway with Mobile Agent licenses enabled.

While it is possible to backhaul data to a local gateway, it is highly recommended to redirect mobile endpoint traffic to cloud gateways.

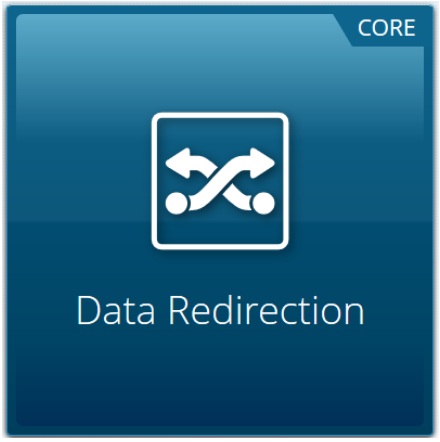
It is recommended to leverage the inherent fault tolerance of the iboss distributed gateway platform by ensuring that more than one cloud gateway be used to secure mobile devices.

Preparing the Web Gateway

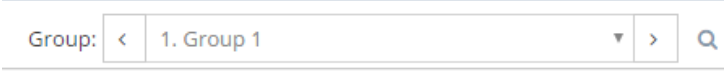
The instructions for configuring Windows Mobile Client consist of preparing the web gateway to support offsite web security, decrypting traffic, and identifying the logged in user.

Login to https://ibosscloud.com

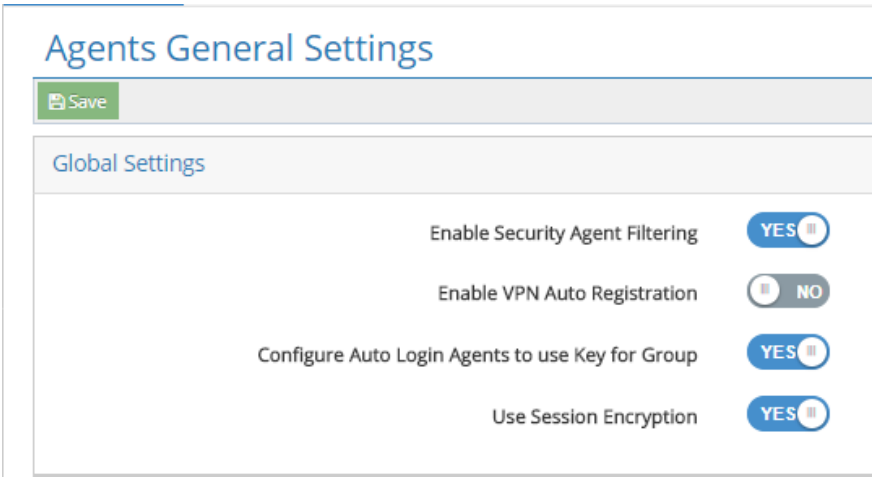
Navigate to **Data Redirection > Agents**



Select the Default group, 1, from the group selection drop-down and choose the filtering group you are deploying the Windows Agent to.



Enable Security Agent Filtering for the filtering groups you intend to support and click Save.



Setting	Description
Use session Encryption	This toggle will activate the service.
Enable VPN Auto Registration	This toggle is not necessarily required (the toggle shown above demonstrates this disabled) but is an optional step for use with VPN mode.
Configure Auto Login Agents to use Key for Group	Switching this toggle to "Yes" causes users to be placed into groups based on the security key (parameter in the agent MSI setup file) rather than the group name.
Use session Encryption	When this feature is enabled AES encryption will be used. All new agent registrations will be encrypted (when enabled) and all existing sessions that

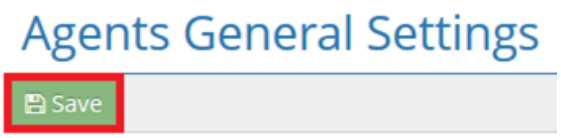
	are not encrypted will still function properly.

Define a custom security key. Note this key as it will be necessary for agent configuration in later steps.

Select your LDAP server from the "Extract Group From LDAP" setting.

Note: *If you do not have a centralized directory or prefer to decouple NetID SSO from the directory, skip this step as Gen. 4 agents do not support this*

Save the settings



Steps Specific to Gen. 4 Agent Setup

Option 1- Windows Agent via SAML and Proxy

The Generation 4 Windows agent accelerates proxy data redirection by automatically configuring the proxy settings on the workstation and injecting proxy authentication information and SAML authentication cookies into the proxy requests.

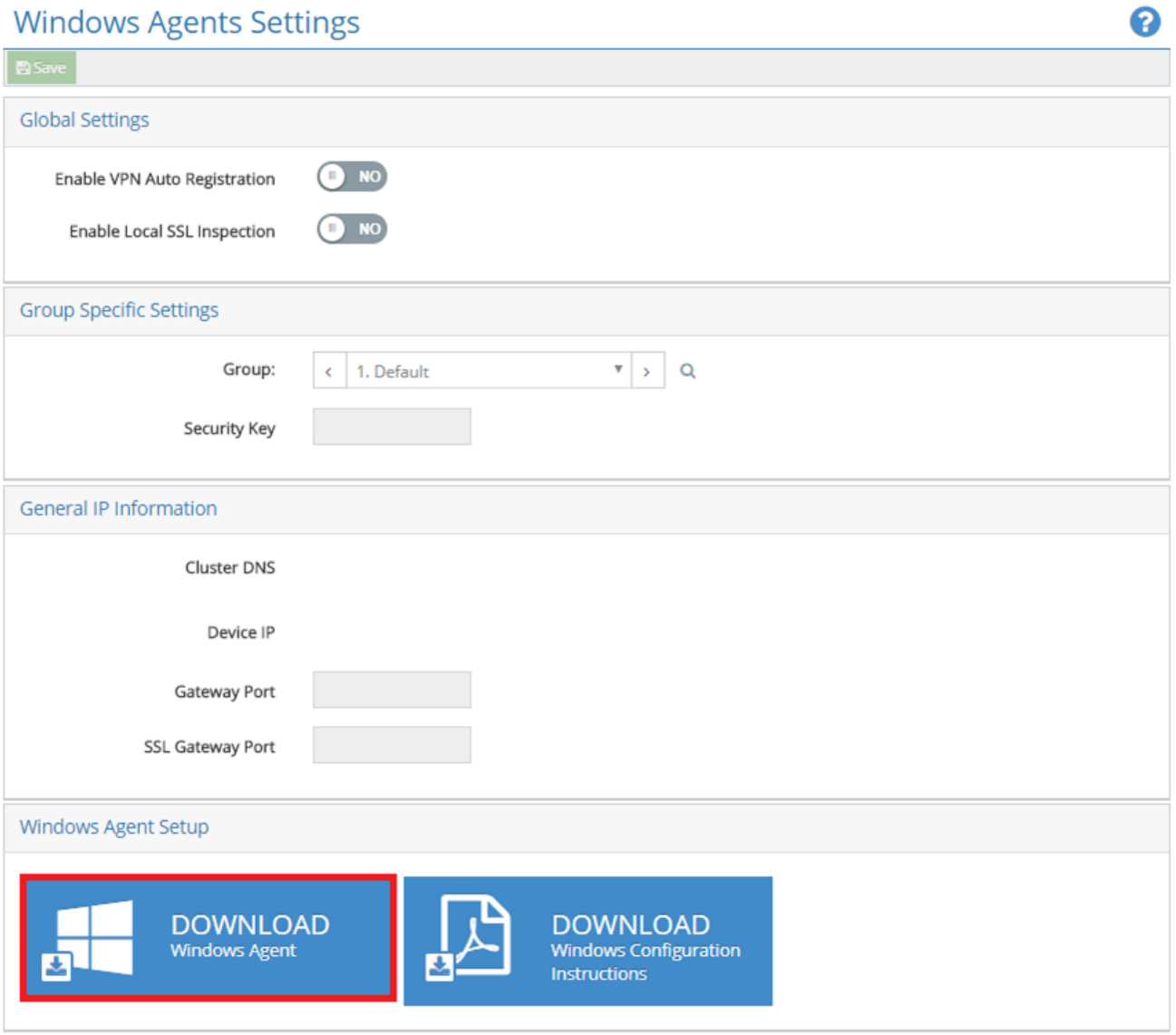
Note: *Proxy-based filtering will still work without agents but the agents will speed up the performance and reduce the number of logins the user will need to enter.*

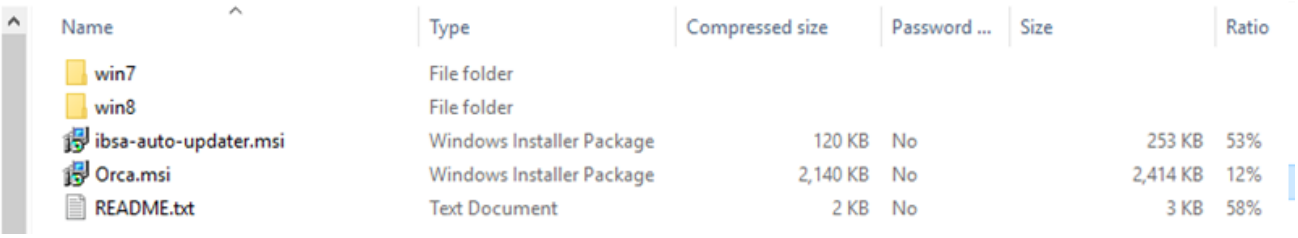
Web Gateway Setup Information

The Web Gateway must be configured to proxy with SAML-based authentication. To do this, log in to iboss Cloud and navigate to **Data Redirection > Proxy > User Authentication Method > SAML**. Click the **Save** when finished to preserve these settings.

Agent Setup

The **Download Windows Agent** button will allow you to download the installation and configuration files for the Windows Mobile Client Agent.





Name	Type	Compressed size	Password ...	Size	Ratio
win7	File folder				
win8	File folder				
ibsa-auto-updater.msi	Windows Installer Package	120 KB	No	253 KB	53%
Orca.msi	Windows Installer Package	2,140 KB	No	2,414 KB	12%
README.txt	Text Document	2 KB	No	3 KB	58%

Extract the archive from the Windows 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). The latest installation files are always available via the 'Download Agent' button.

Select the OS that you would like to use (taking care to select the appropriate 32- or 64-bit installer).

Note: *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*

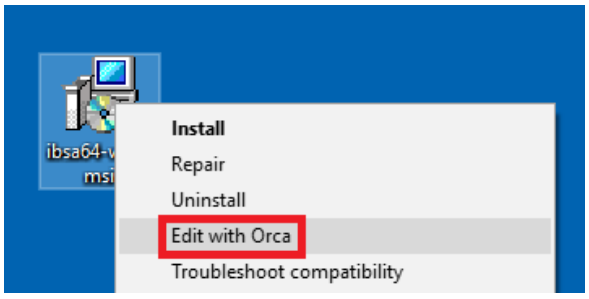
Save the .msi to your desktop for quick access in the next steps.

The Windows agent is configured through the system registry. The MSI file used to install the Windows agent may be pre-configured to set the desired values using an MSI editing tool such as Orca.

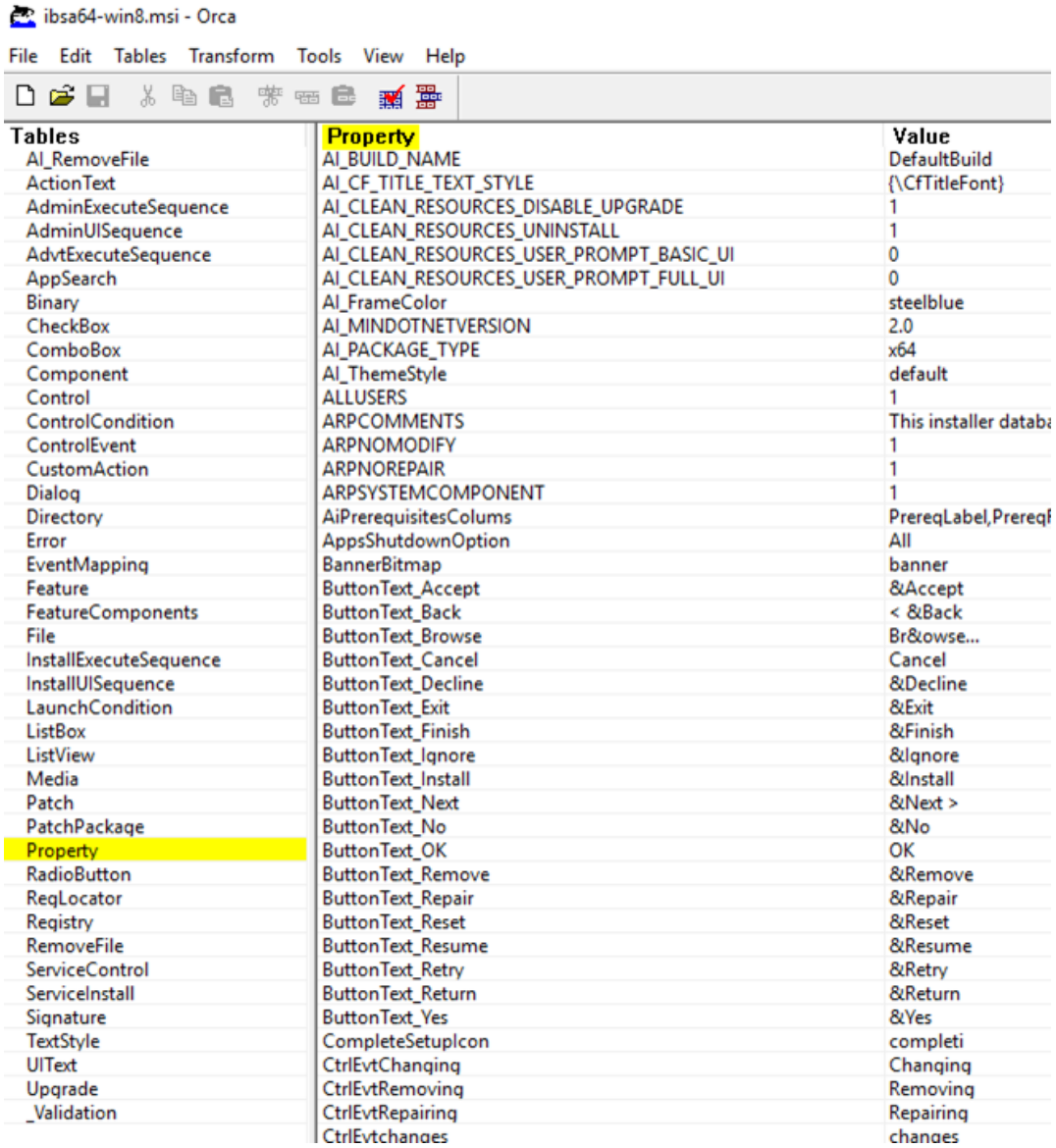
Installing and Using Orca

Name	Type	Compressed size	Password ...	Size	Ratio
win7	File folder				
win8	File folder				
ibsa-auto-updater.msi	Windows Installer Package	120 KB	No	253 KB	53%
Orca.msi	Windows Installer Package	2,140 KB	No	2,414 KB	12%
README.txt	Text Document	2 KB	No	3 KB	58%

Orca is a widely available tool used for editing the properties .msi files. Once Orca is installed on the system, you can use it to modify the .msi file that you just downloaded. Right click on the extracted file and choose **Edit with Orca** as shown here.



This will bring up the interface shown below.

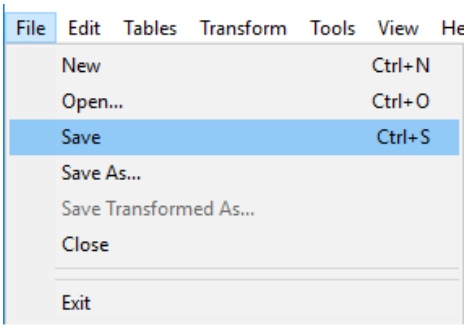


Click on "Property" in the list of tables, then click on Property at the head of the table to organize it alphabetically. Edit the appropriate parameters (explained below) by typing in the corresponding field in the "Value" column.

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

Parameter	Description
PARAM_RUNTIME_MODE	Set to “gen4_saml”
PARAM_GATEWAY_HOST	Enter the Web Gateway address or cluster address here. E.g. cluster1-swg.ibosstest.com
PARAM_GATEWAY_PORT	Enter the proxy port (available on the Proxy page under Settings). The default is 8009.
PARAM_PROXY_MONITOR_INTERVAL	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 update them.
PARAM_PROXY_OVERRIDE	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 *ibosstest.com. Multiple server names must be separated by semi-colons.
PARAM_SAML_SESSION_COOKIE	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. If set in Orca and deployed to multiple workstations, all users would be deployed similarly.

After the necessary parameters have been edited in Orca, save the file by clicking **File > Save**.



Once you have modified the installer, install the appropriate .msi (either ibsa32.msi or ibsa64.msi) on your computer by double-clicking the installer and following any prompts.

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

This completes the install of the agent in SAML Proxy Mode.

Option 2- Windows Agent Auto-Login Mode

The Generation 4 Windows agent accelerates proxy-based redirection by automatically configuring the proxy settings on the workstation and injecting cookies into traffic that will authenticate the endpoint and gateway to each other. Auto-Login mode allows iboss Agents and endpoints to be automatically registered and secured by a configured gateway without the need for manual input of login credentials.

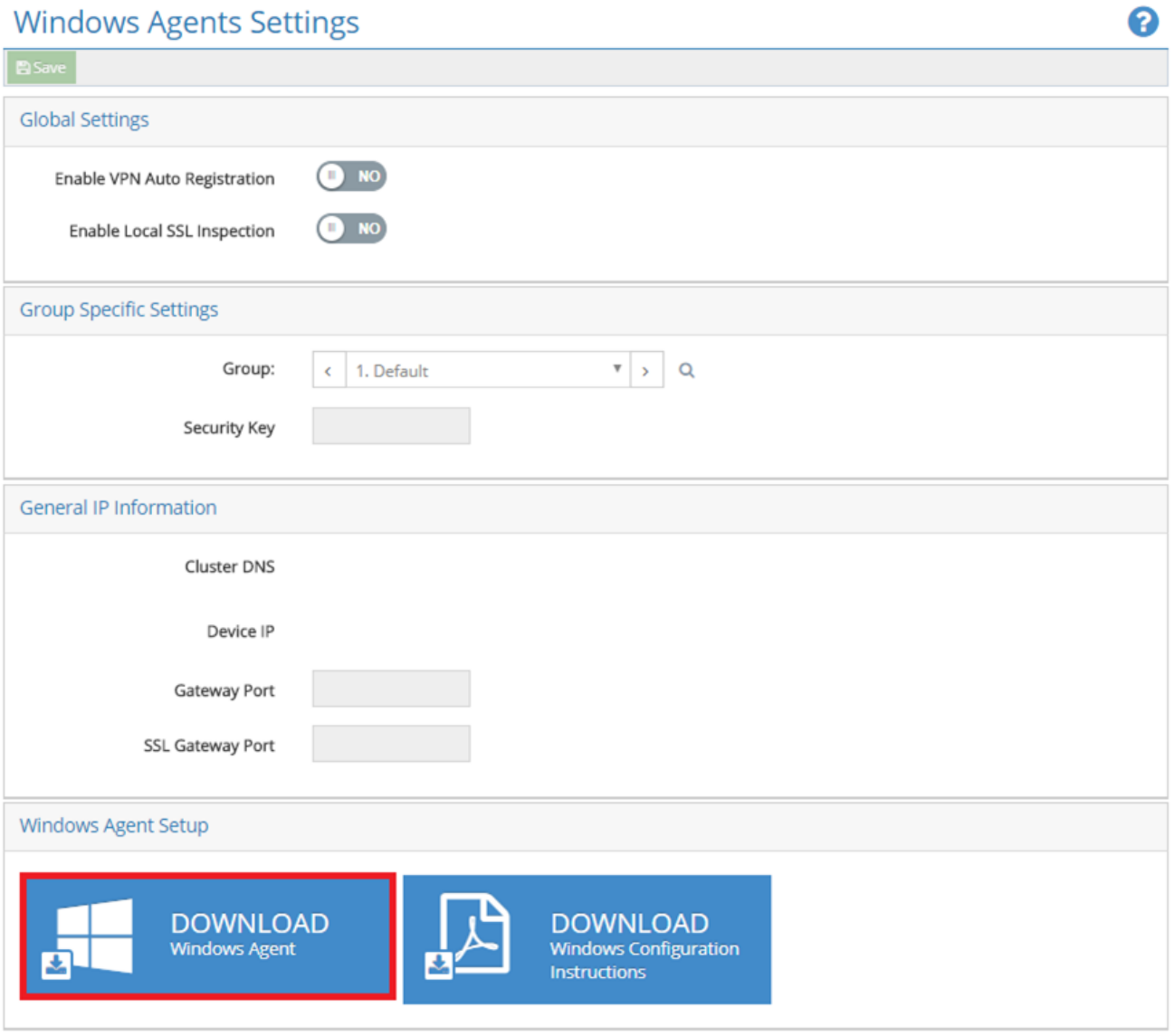
Note: *The Auto Login Proxy configuration requires the use of Agents to work.*

Web Gateway Setup Information

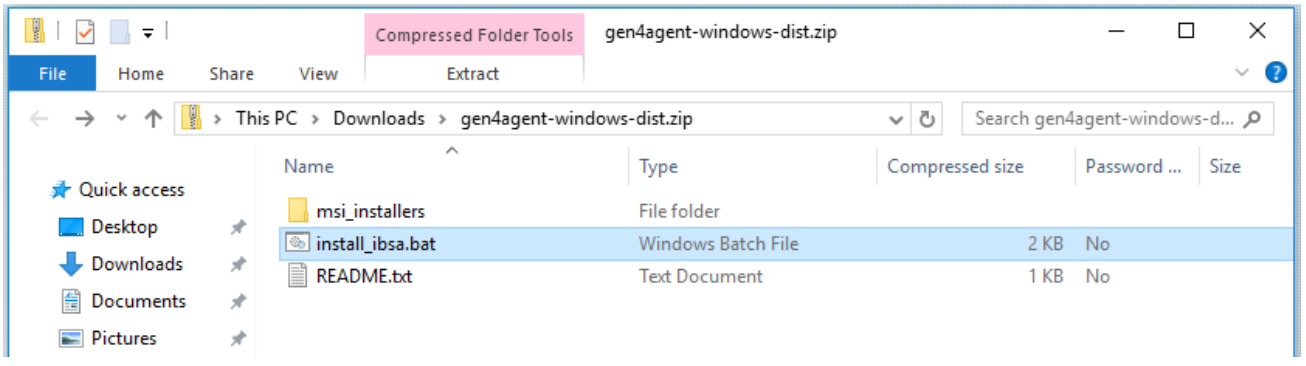
The Web Gateway must be set to use a proxy data redirection method, with the "User Authentication Method" set to Auto-Login Agents. to do this, log into your iboss Cloud Account and navigate to **Data Redirection > Proxy > Enable Proxy Settings** (if not already active) **>User Authentication Method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

Agent Setup

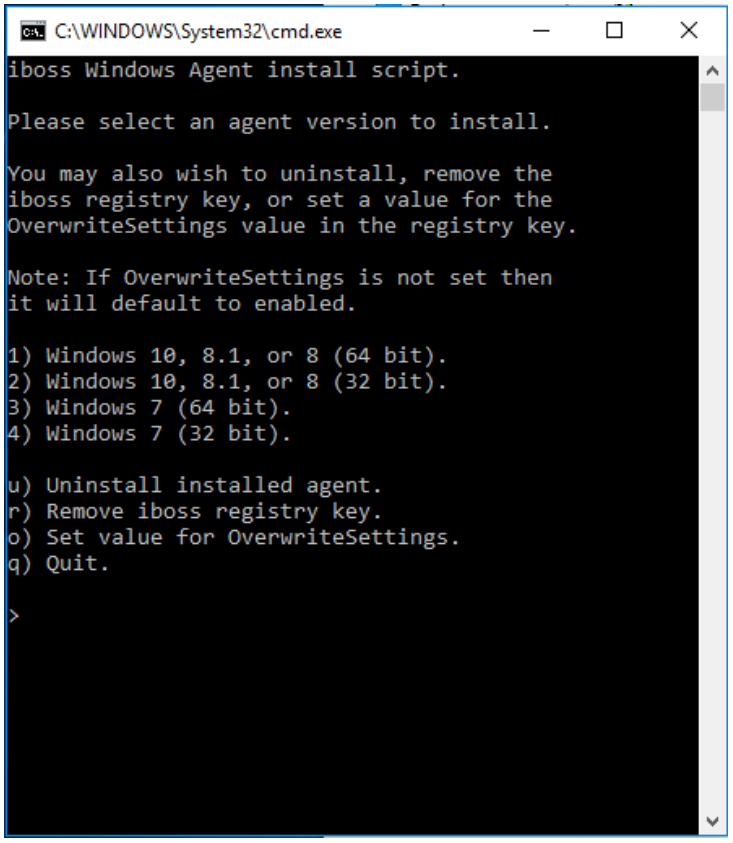
The **Download Windows Agent** button will allow you to download the installation and configuration files for the Windows Mobile Client Agent.



It will appear on your computer compressed into a .zip file. Extract the contents of the file and save to your preferred location.



In this folder, right-click the file called **install_ibsa.bat > Run as an Administrator** certifying that you are sure you want to run the file. The batch file will be presented to you as shown below.



If this is the first time an iboss agent is being installed on this device, enter a number 1-4 corresponding to the windows version present on the device.

If this device has had another version of the iboss agent previously installed on it, enter the "u" command to fully uninstall any agents on the device, followed by the "r" command to remove the iboss registry key. After this, enter a number 1-4 corresponding to the windows version present on the device.

Within a few minutes, your device will now direct all web traffic (unless otherwise specified) to the gateway/cluster from which the agent was downloaded. All applicable policy is now being applied.

To verify that the agent is running, you can navigate to your computer's "Services" interface (Search "Services" from the Start menu) and check to see that "IBSA" (iboss Security Agent) is present and running. To ensure the parameters of the agent have been correctly set, open up your computer's Registry Editor (search "regedit" from the start menu) and navigate through the registry path **Computer > HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > iboss Security Agent > Parameters**. The address of the web gateway cluster will display in the "GatewayHost" parameter, the "RuntimeMode" parameter will be "gen4_auto", and the "Version" parameter will be "4.0.0". If you edit any of the parameters in the Registry Editor, be sure to restart the IBSA service.

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.

In the event that the agent does not detect any groups pertinent to the device, the device will 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.

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

This completes the install of the agent.

Acquiring Group Information

At the initial startup of the agent or upon 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.

Steps Specific to Gen. 2/Gen. 3 Agent Setup

The parameters below must be entered via the Registry Editor or Orca when setting up the Gen. 2/Gen. 3 Agent. Of all the properties, there are only a few which need to be changed to match your network configuration.

Parameter	Description
PARAM_GATEWAY_HOST	This should be the IP Address (or DNS Hostname) 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 translated via NAT 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.

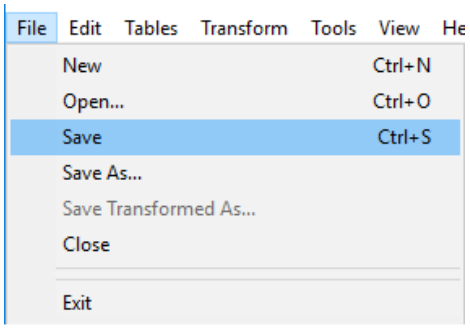
If you will be using the agent to perform LOCAL network SSL content inspection (NOT REQUIRED for mobile filtering/security or SSL blocking), the following options should be set (available in gen3 agents only):

Parameter	Description
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 Gen. 3 installers only. A restart is required when moving from a Gen. 2 agent to a Gen. 3 agent. This option can be used if moving between Gen. 2 and Gen. 3 is necessary.

After the necessary parameters have been edited in Orca, save the file by clicking **File > Save**.



Once you have modified the installer, install the appropriate .msi (either ibsa32.msi or ibsa64.msi) on your computer by double-clicking the installer and following any prompts.

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

This completes the install of the agent.

Additional References

Legacy Windows and Mac Agent Documentation

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.*