MAC Endpoint Technical Overview

Overview

Websense® MAC Web Endpoint is designed to provide a seamless experience to end users for authenticating and directing traffic to the Websense Cloud Security infrastructure. The endpoint is available for Cloud Web Security customers, and has native support Intel-based MACs running OS X 10.6 or higher. It has been designed to consume minimal CPU, memory, and disk resources.

System Requirements

Browsers

Fully supported browsers (please note that we will not be supporting Web Installation for the MAC OS X version of the endpoint).

- Safari 5.1 or higher
- Firefox 8.0 or higher
- Google Chrome 15 or higher

Operating systems

- MAC OS X v10.6
- MAC OS X v10.7

Footprint

- Installer: <2MB
- Hard disk space required: <10MB
- Memory usage: <2MB

Required network rules

In addition to the subnet access already required to access the Websense Cloud Security service, ports 80, 443, and 8080-8082 must be allowed to these subnets for the endpoint to be installed via the Web installation mechanism.

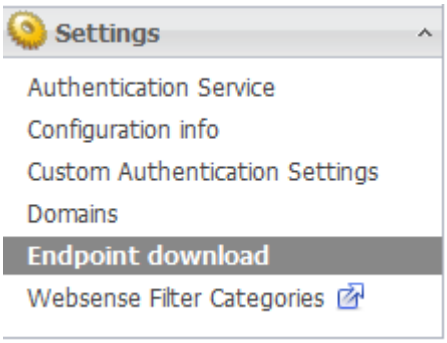
CIDR	Range	Subnet	Mask
85.115.32.0/19	85.115.32.0 - 85.115.63.255	85.115.32.0	255.255.224.0
86.111.216.0/23	86.111.216.0 - 86.111.217.255	86.111.216.0	255.255.254.0
116.50.56.0/21	116.50.56.0 - 116.50.63.255	116.50.56.0	255.255.248.0
208.87.232.0/21	208.87.232.0 - 208.87.239.255	208.87.232.0	255.255.248.0
86.111.220.0/22	86.111.220.0 - 86.111.223.255	86.111.220.0	255.255.252.0

CIDR	Range	Subnet	Mask
103.1.196.0/22	103.1.196.0 - 103.1.199.255	103.1.196.0	255.255.252.0
177.39.96.0/22	177.39.96.0 - 177.39.99.255	177.39.96.0	255.255.252.0

Installation

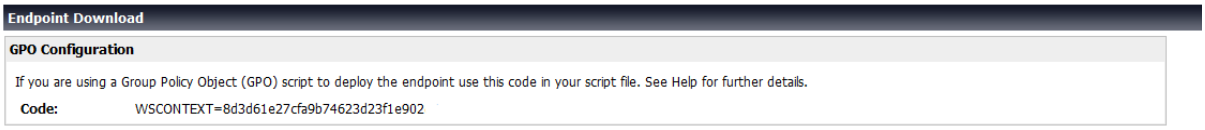
Early access program customers will have been sent a link to download the EAP MAC Endpoint package. This is not currently in the portal.

Before any of the Endpoints can be installed, you must first set an anti-tampering password. (For more information on this, see the TRITON Cloud Web Security Help guide).



Within the downloaded archive is the Websense Endpoint.pkg file along with a non-account specific HWSconfig.xml file, which needs to be edited before you can begin the install. It must also be in the same directory as the .pkg file for the endpoint to successfully install.

You need to get your account specific string which also resides on the same page as the Endpoint password you have just set.



Within the HWSConfig.xml file you will see a section like

<Context InitContext="" />

Inside the “” you need to copy and paste the string after WSCONTEXT=, so in this example it would be

<Context InitContext="8d3d61e27cfa9b74623d23f1e902" />

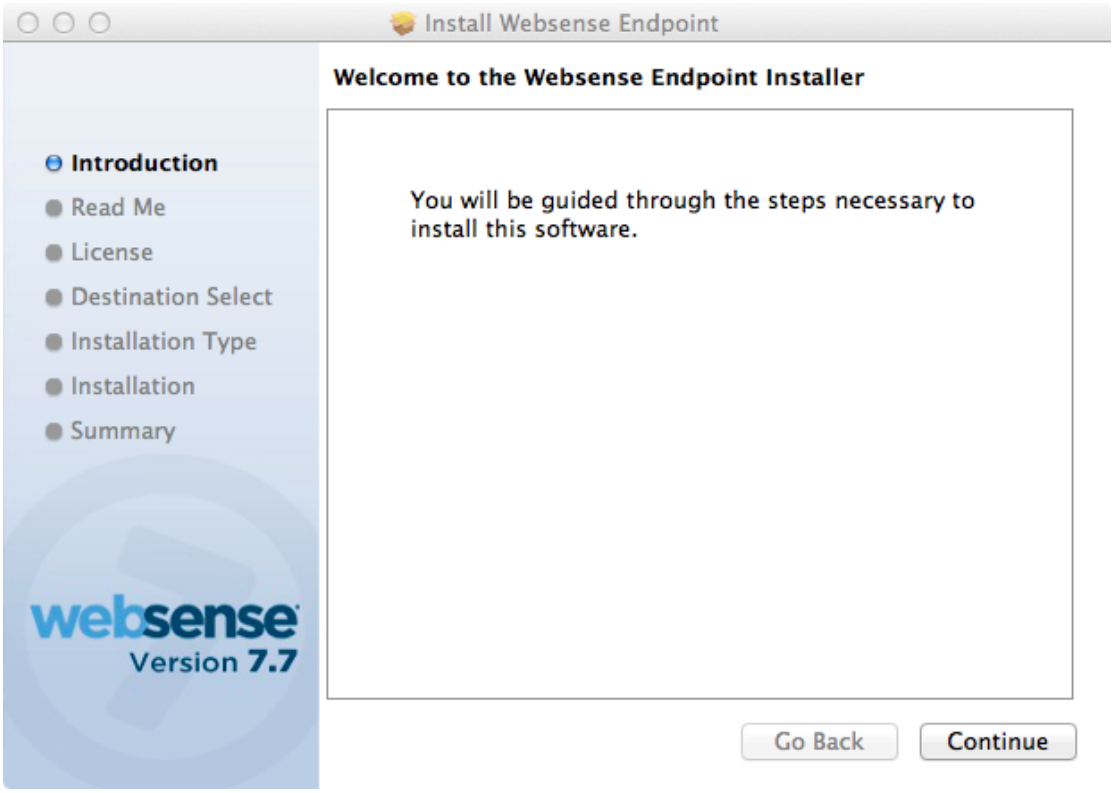
Please note that if you wish to use the Endpoint over port 80 for proxying and PAC file retrieval you will need to do two things before installing the Endpoint.

1. Request Websense Support to add the “Send HWS Endpoint to port 80” template to your account (you can choose to only add this to specific policies or globally).
2. Change the HWSconfig line from
   <PACFile URL="http://webdefence.global.blackspider.com:8082/proxy.pac" />
   to
   <PACFile URL="http://pac.webdefence.global.blackspider.com/proxy.pac " />

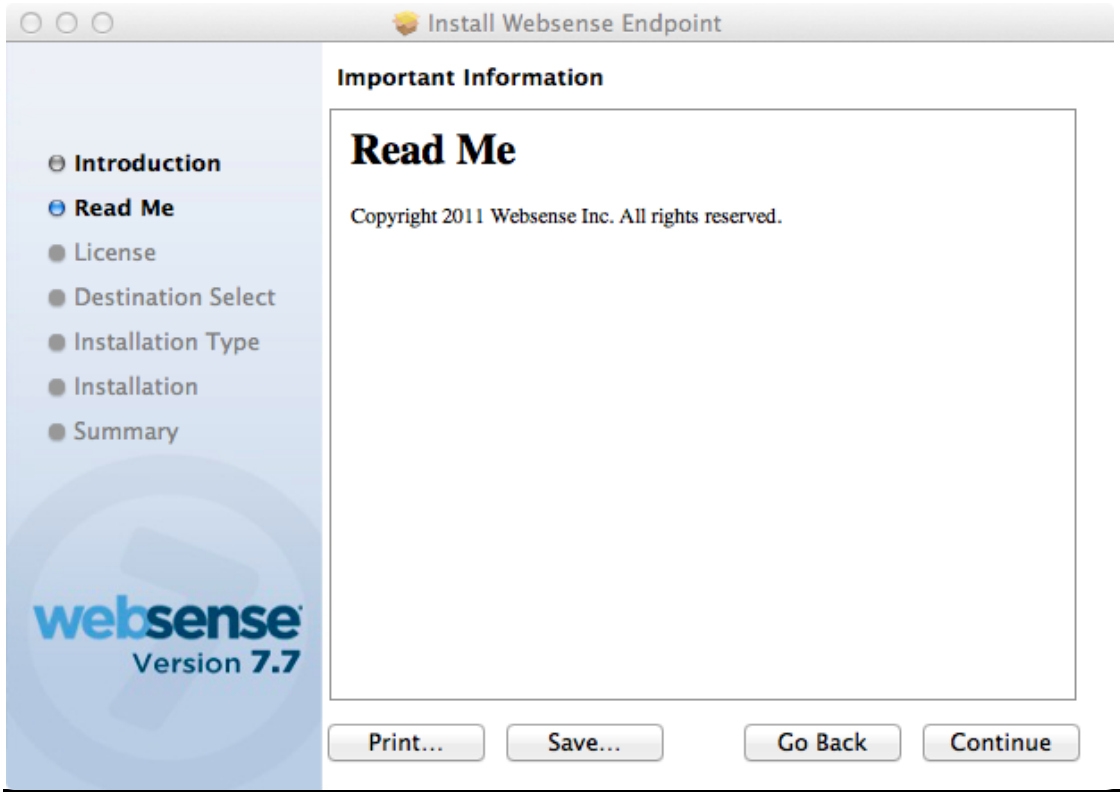
Please note that by applying this template you will also move any Endpoints already installed over to port 80 access of the service will are associated with any policies that this template applies to.

You are now ready to install the Websense MAC Endpoint.

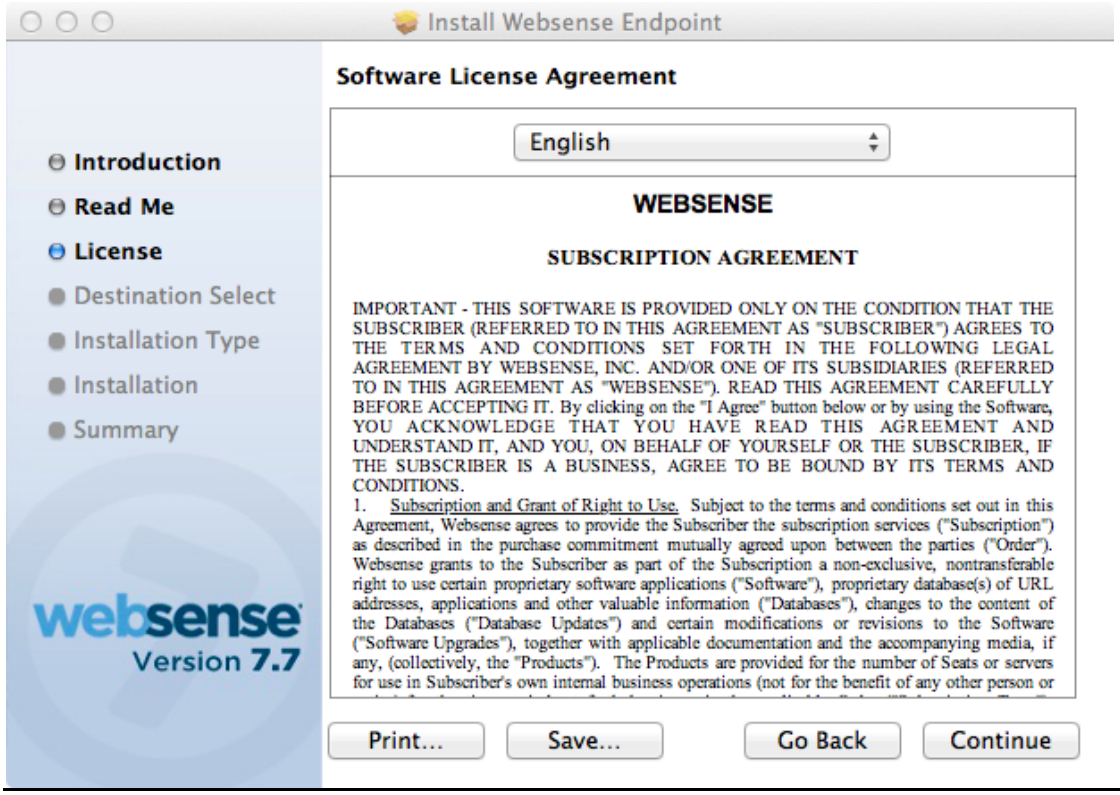
Running the Websense Endpoint.pkg file will show the following screen:



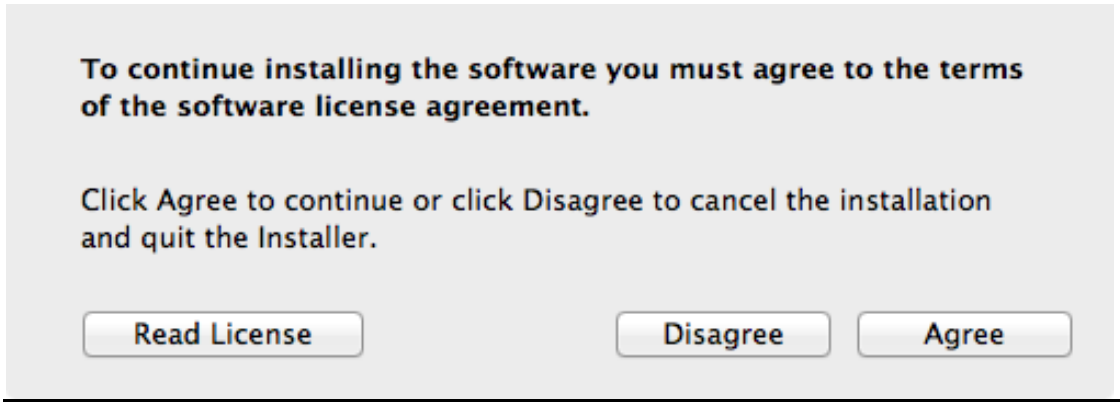
Click **Continue**.



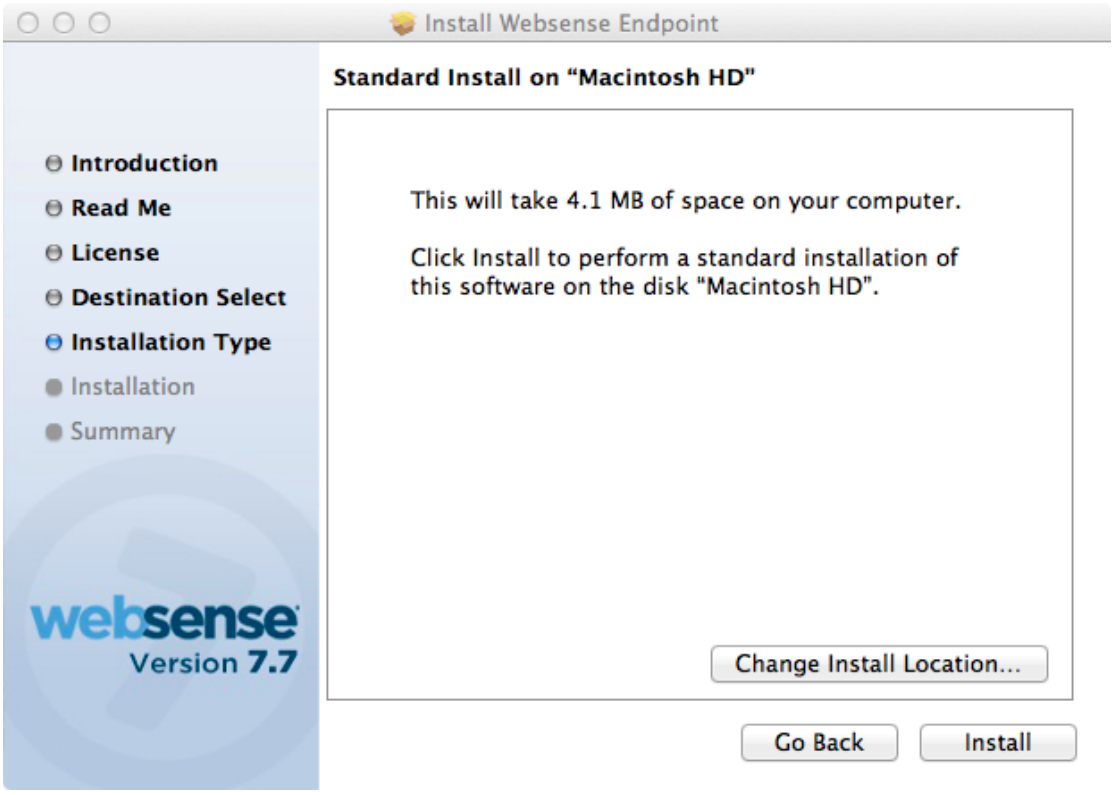
Click **Continue**.



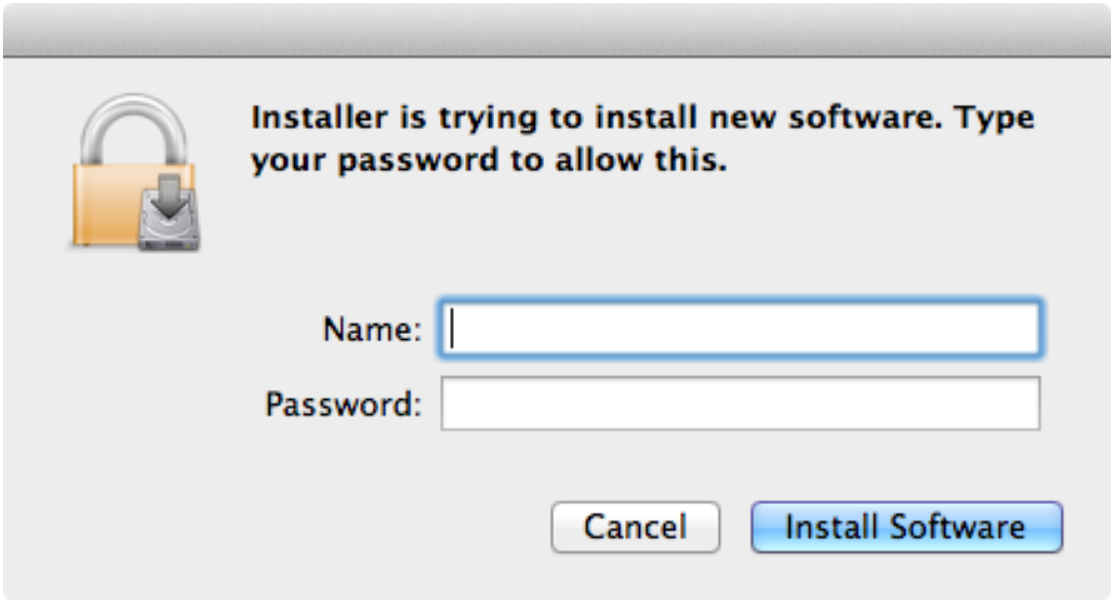
Click **Continue**.



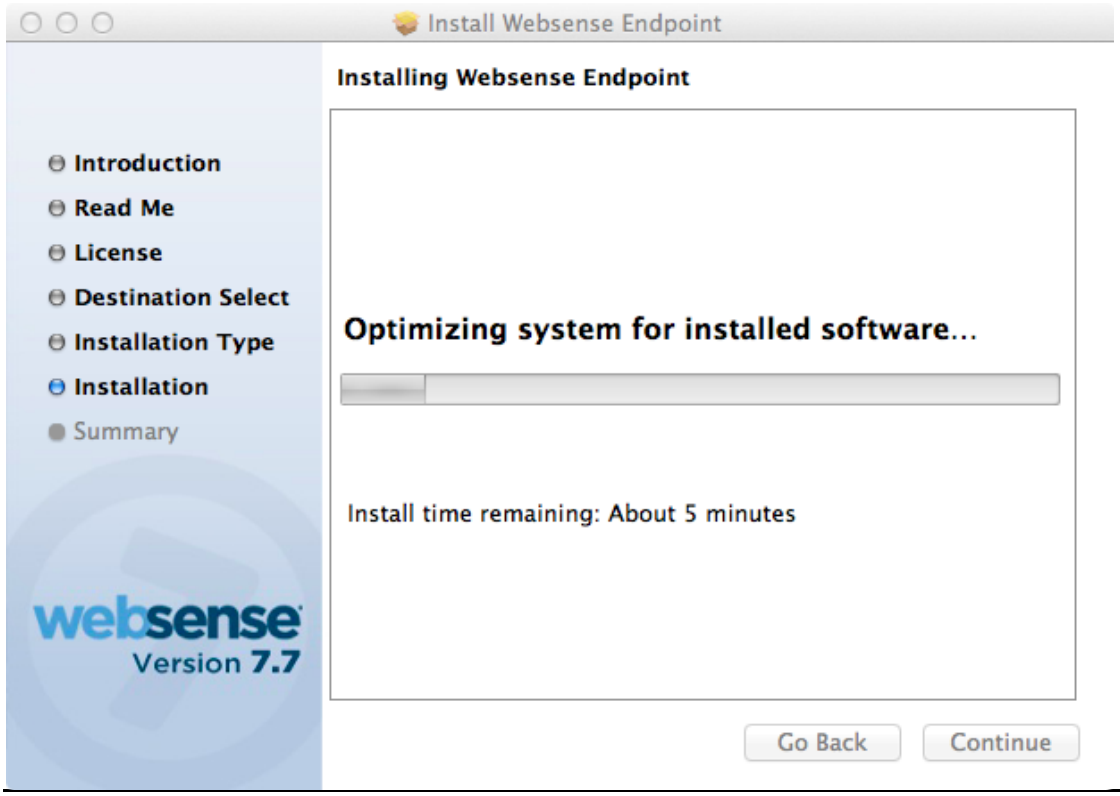
Click **Agree** if you agree with the license. Click **Disagree** to cancel the installation.



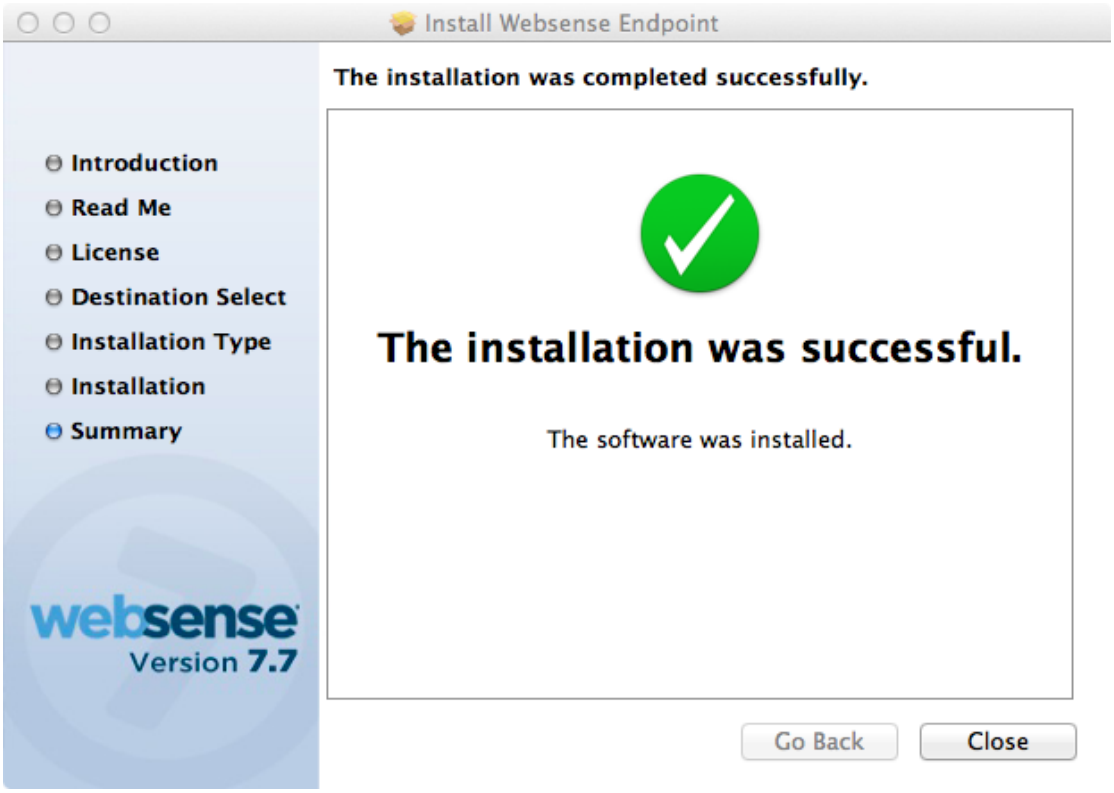
Click **Install**. Please note you must install the Websense Endpoint on the local hard disk. We do not support installation of the Endpoint on removable media.



Enter in a username and password of a user with administrator rights to install the software and click **Install Software**.

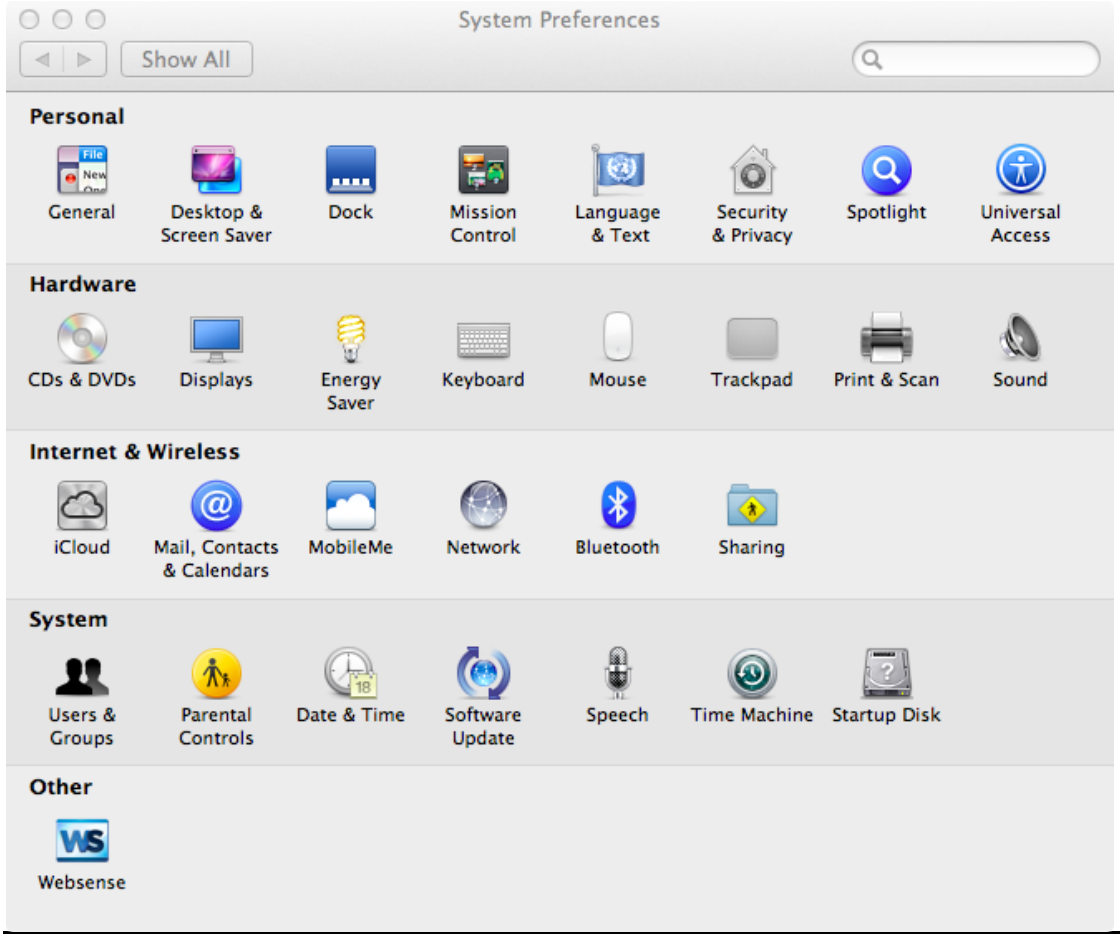


The installation will now proceed. If the installation fails here, it is usually because the HWSconfig.xml file is either not present or is in the incorrect format if you have edited it.

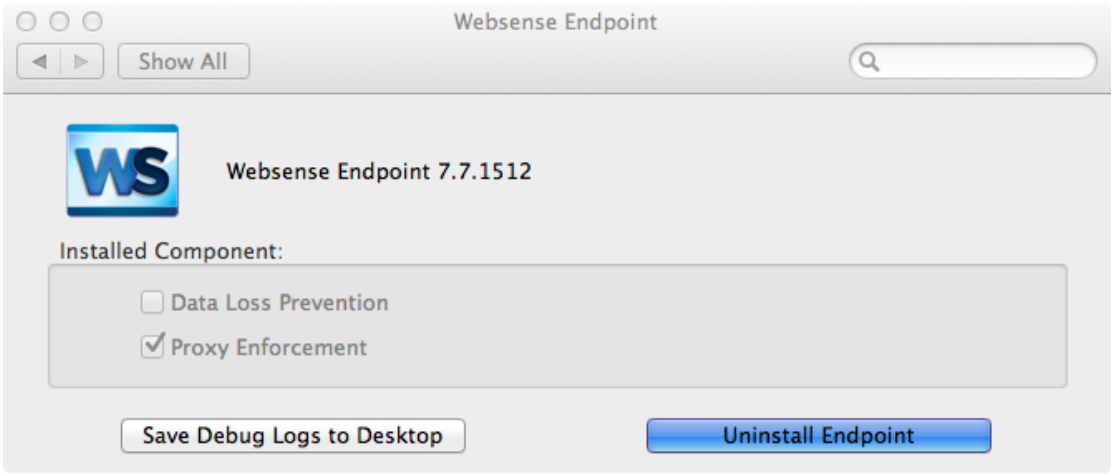


Upon successful installation this screen appears. Click **Close** to finish the installation.

You will now see a new settings screen in the System Preferences window:



Clicking on the Websense will bring up the following screen:



This application shows the installed Endpoint version and support Websense packages (Proxy Enforcement is used for the Web Endpoint).

You can do two other things here.

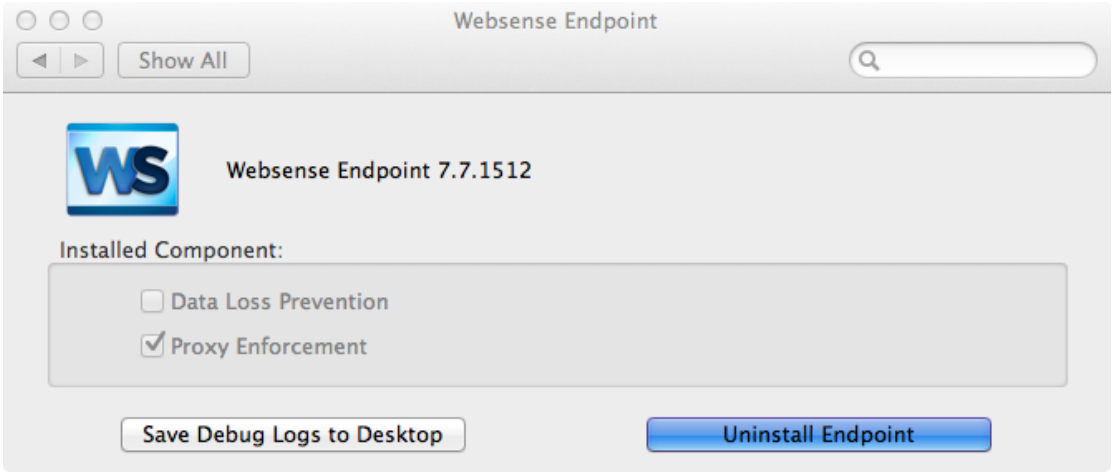
- Save Debug Logs to Desktop
- Uninstall Endpoint

Save Debug Logs to Desktop

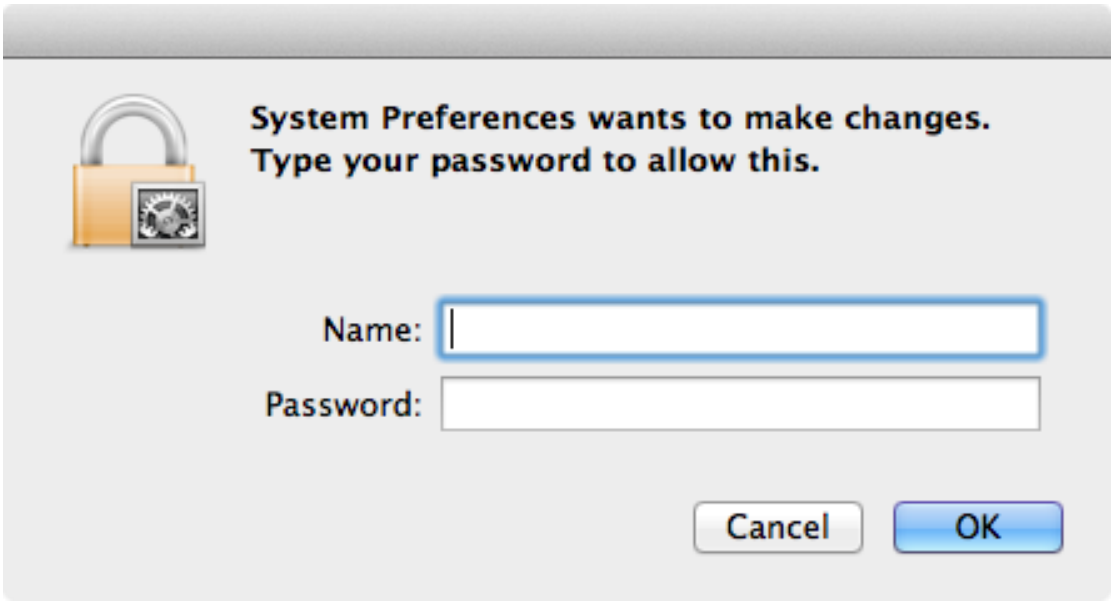
The Save Debugs logs is an important support tool and allows the Websense support team access to all the troubleshooting logs in one place. Clicking this button will create an archive file on the MAC desktop beginning with ClientInfo*.zip. Whenever you need to raise a support ticket with Websense support regarding the client, please make sure you include this zip file with the request, as this will greatly speed up the resolution of any issue you may find.

Uninstall Endpoint

Uninstallation of the Endpoint can be achieved either through the UI provided or via the command line (see the Command Line Features section).

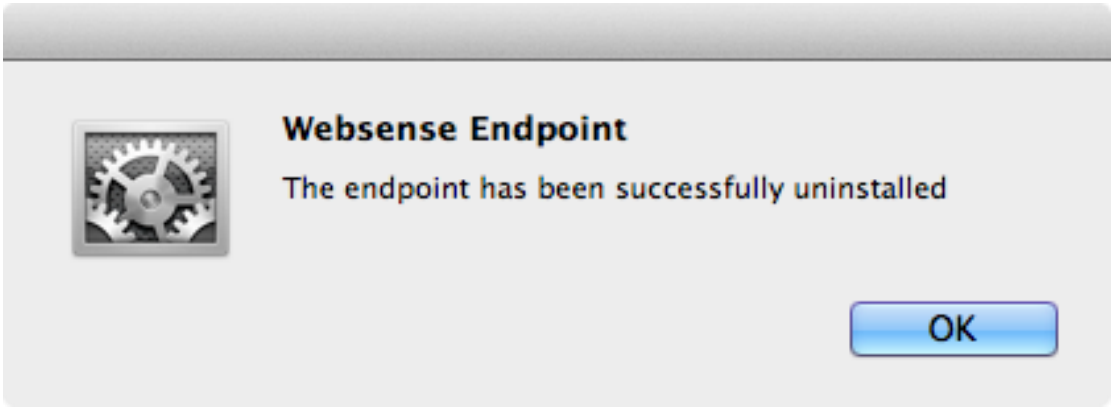


Clicking on **Uninstall Endpoint** will first pop up a window requesting a user/password combination which has administration rights.



Click on **OK** to continue to the next screen.

You will then have to enter the Endpoint anti-tampering password that was set in the cloud portal. Click on **OK** to start the uninstallation. Once the Websense Endpoint has finished uninstalling, the following screen appears:



Click on **OK** to finish the uninstallation.

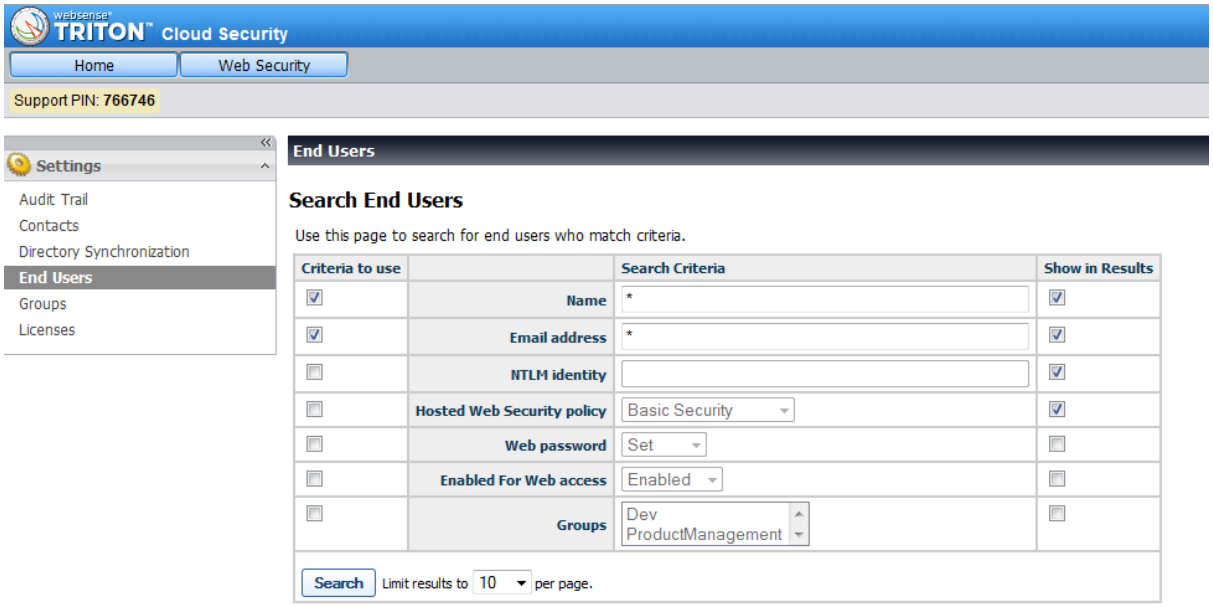
Using the MAC Endpoint with the Websense Cloud Web Security Service

When a MAC is logged into an active directory-based domain, the Web Endpoint will identify the user in the same way as the Windows Endpoint and return a user to the service of domain\user, which will also have been synced from your active directory using the Directory Sync client. No further setup should be required. However domain MAC users tend to be the exception to the rule, and most MACs are not using a domain login, but a local login instead. In this case the Endpoint formats the user details up to the Cloud Security service as

mac.local.[local_username] (e.g., if you were logged in as "Joe Bloggs," it would appear to the service as mac.local.joebloggs. Since these users will not have been synced to the service via the directory sync tool, there is some manual work to be done here.

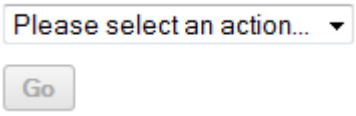
The Websense Cloud Web Security service will auto-register users on the service assuming the correct Endpoint WSCONTEXT string is being used. This gives users the "Basic Security" policy by default.

If you click on **Account Settings** in the cloud portal, then click on "End Users" in the menu, you will be taken to the following screen:

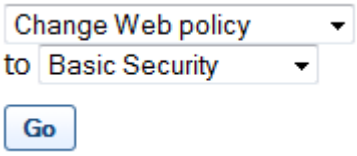


To search for all the locally logged on MAC users, change the name field to mac.local,* and click on **Search**.

You will now be shown a list of all of these users. To change the policy of a user, first select **Change Web Policy** from the **Please select an action**… dropdown.



Choose the policy you want to move the selected MAC users to.



Then select each of the displayed MAC users that you want to move, and click the **Go** button. The users will now be moved to the new policy, and this update will be live across the Websense cloud infrastructure within 60 seconds.

Please note that there are two MAC usernames that will be common across all of your MAC users.

- mac.local.root
- mac.local._softwareupdate

These users are used by installed software to get their updates from the internet. Websense recommends a fairly tight policy for these users as typically they would only need to access a few categories (Information Technology is the most common category it needs access to).

Command Line Features

How to stop the service

sudo wepsvc --stop

(You will need to first type the MAC administrator password to run the sudo command, then it will ask you for the service password, which is the default password unless changed in the portal for that account).

How to uninstall the service

sudo wepsvc --uninstall

(You will need to first type the MAC administrator password to run the sudo command, then it will ask you for the service password, which is the default password unless changed in the portal for that account).

Other Features

Running wepsvc –help will show you the following command switches.

--status --[wsdlp|wspxy]	display the status of the component
--start --[wsdlp|wspxy|all]	start the specified component
--stop --[wsdlp|wspxy|all] [--password pwd]	stop the specified component
--uninstall [--password pwd]	uninstall the endpoint
--enable-anti-tampering --[wsdlp|wspxy] [--password pwd]	enable anti-tampering feature of the component
--disable-anti-tampering --[wsdlp|wspxy] [--password pwd]	disable anti-tampering feature of the component
--dump-event-log --wsdlp	dump DLP event log
--collect-debug-dump	collect the related logs and save them on desktop

All this commands require them to be run as root, e.g. sudo wepsvc --status --wsxpy

Please note that to stop the product or disable the anti-tampering you must have both the MAC root password (on first run of sudo command) and the service password.

With the Web Endpoint please ignore the references to the DLP plug (wsdlp) since this is only applicable for the DLP client or the unified client.