websense®
ESSENTIAL INFORMATION PROTECTION™

Web Endpoint Technical Overview

Overview

Websense® 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 both Web Security Gateway Anywhere and Cloud Web Security customers, and has native support for both 32-bit and 64-bit Windows operating systems. It has been designed to consume minimal CPU, memory, and disk resources.

System Requirements

Fully supported browsers (including proxy manipulation and Web installation)

- Internet Explorer 7, 8, and 9 (32-bit and 64-bit)
- Firefox 3.x (32-bit), Firefox 4, 5, 6 and 7

Please note that all browsers are supported for the Network Filter and proxy manipulation aspect of the endpoint.

Operating systems

- Windows XP with SP 2 or higher, 32-bit, 64-bit
- Windows Vista with SP1 or higher, 32-bit, 64-bit
- Windows 7 (including SP1), 32-bit, 64-bit

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.

Supported Protocols

Websense Web Endpoint supports the following protocols:

- HTTP
- HTTPS
- FTP over HTTP

User Identification

The endpoint appends two additional headers into each HTTP request. One header tells us the version of the agent that is installed; the other is an encrypted token which tells us who the user is, so we can apply the right policy for the end user and correctly log the data against that end-user. These headers do not include any domain passwords or other security information, meaning that there is no security risk in using the endpoint.

The headers are then stripped from the requests by the Websense Cloud Security or hybrid proxy.

Modes of Operation

The endpoint has two modes of operation

- Proxy manipulation
- Network Filter

Proxy manipulation

For supported browsers, the endpoint will manipulate the proxy settings in real-time. It does this for several reasons:

1. If the endpoint detects it is in an area of the corporate LAN which you want to route out via the Web Security Gateway Anywhere appliance proxy, it will set the proxy to this.
2. If the endpoint detects it is somewhere where you should not use the Web Security Gateway Anywhere appliance proxy, it will set the proxy to the Websense Cloud Security service.
3. If the endpoint detects it is at a hotspot, which the user has not yet fully signed into, it will remove the proxy settings until the gateway has successfully opened up.

Network Filter

The Network Filter is a TDI-layer driver that sits in the network stack at a higher level than the VPN driver. It is important to defer to the VPN driver, since this lets customers decide if they want to use a full tunnel VPN (no Web traffic would go directly to the Websense Cloud Security infrastructure, but routes through the corporate VPN gateway first), or split tunnel (where they can exception HTTP/HTTPS traffic bound for the Internet).

With full tunnel VPNs, having the Web Endpoint ensures that all Web traffic is still analyzed and filtered when the end user does not bring up the VPN (as most end users don't do this even though they are supposed to). In split tunnel mode, as well as ensuring that all Web traffic is still analyzed and filtered when the end user does not bring up the VPN, this allows the HTTP/HTTPS traffic to be directed to the Websense Cloud Security infrastructure and have the same category filtering and similar analysis applied to it as if they were going through the on-premises Web Security Gateway Anywhere environment internally.

This results in a significantly faster browsing experience for the end user (with no extra latency from having to route through the corporate VPN), and significantly lower corporate WAN usage as well for organizations with a large roaming workforce.

Outside of the Web Security Gateway Anywhere appliance-supported corporate environment, the Network Filter inspects all of the packets. Any packet which is found to be HTTP or HTTPS is redirected to the Websense Cloud Security service with the relevant headers added to it to enable user identification. Note that unlike competitor products, the agent scans ALL ports to detect this traffic, not just the standard 80, 443, and 8080 ports.

Anti-Tampering

Even under the latest Windows operating systems there is still no way to make any application tamper-proof when the user has local administration rights on the PC. The endpoint does, however, have 5 key protections against tampering, which should thwart the majority of end users including those with local administration rights.

- Endpoint agent files and folders are protected from deletion
- Endpoint agent registry cannot be modified or deleted
- Endpoint agent process will automatically restart if it is stopped or killed
- SC command to delete Endpoint agent service is blocked
- Un-installation and stopping of service requires a password

Endpoint Installation

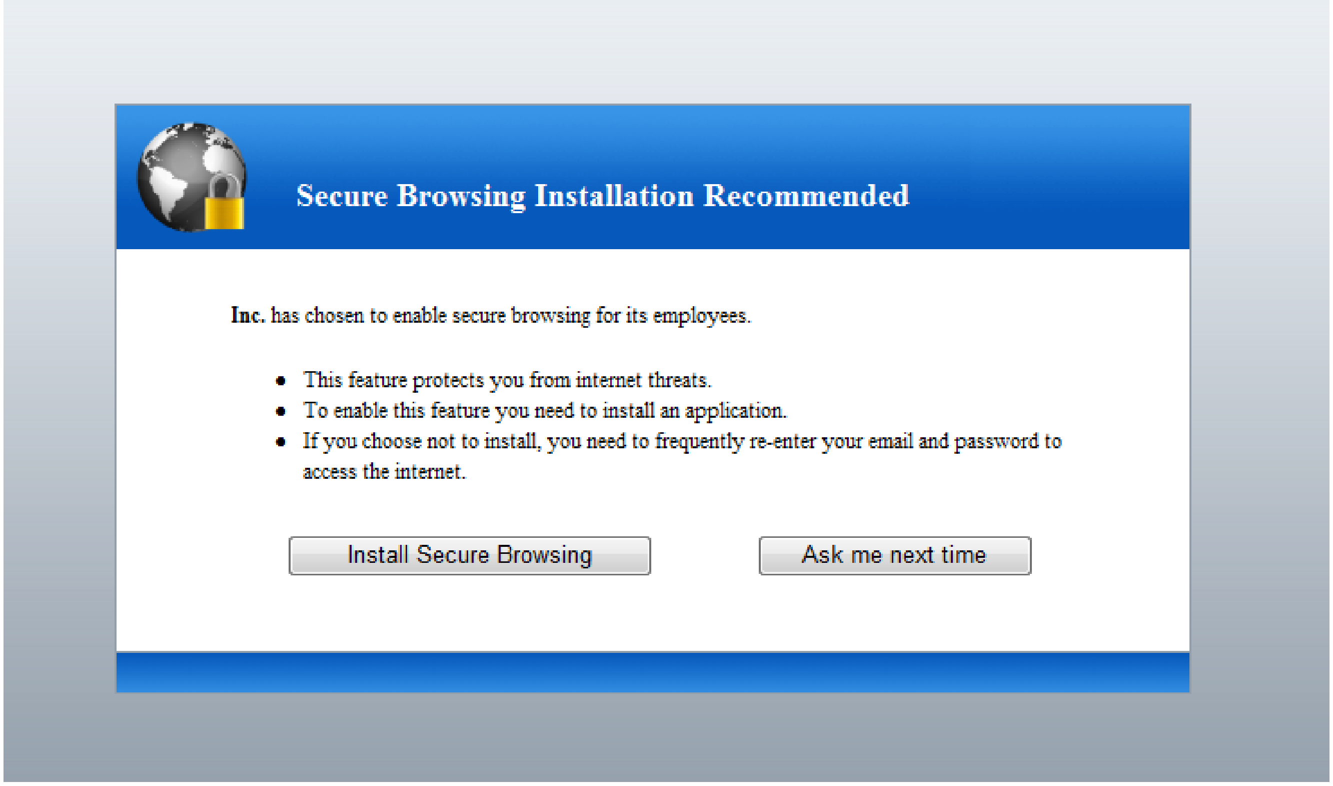
The endpoint can be deployed in a number of different ways.

- GPO installation (including silent install)
- Web installation
- EXE installation

Please note that local administrator rights are needed to install the endpoint in all of these cases.

Web Installation

If the administrator chooses to install the endpoint via the Web Installation, all of the end users will be shown the following screen, if the endpoint is not installed.



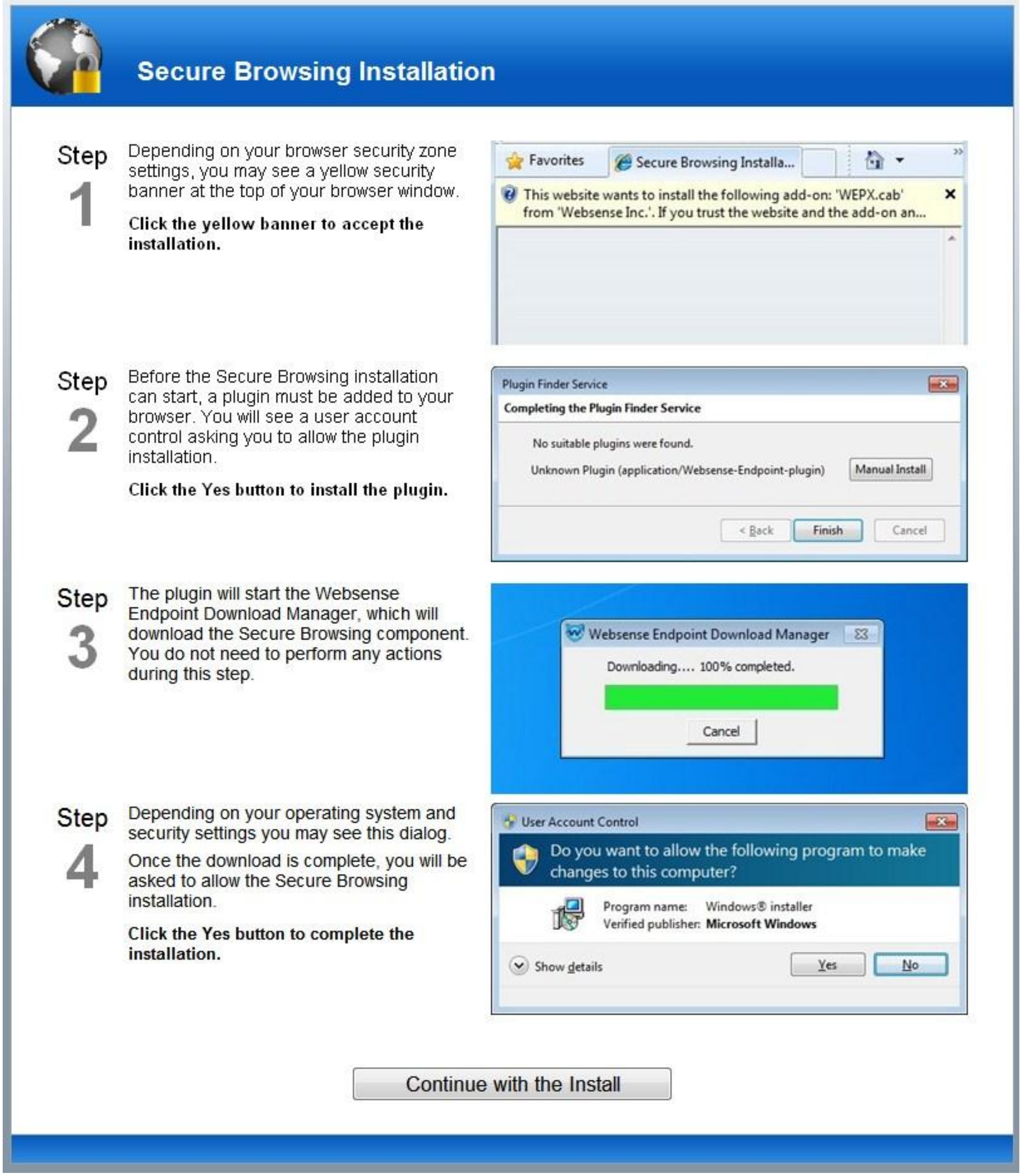
Secure Browsing Installation Recommended

Inc. has chosen to enable secure browsing for its employees.

- This feature protects you from internet threats.
- To enable this feature you need to install an application.
- If you choose not to install, you need to frequently re-enter your email and password to access the internet.

By clicking on the “Install Secure Browsing” button the end user will be taken to the next screen.

For Internet Explorer, you will see the following screen.



Secure Browsing Installation

Step 1

Depending on your browser security zone settings, you may see a yellow security banner at the top of your browser window.

Click the yellow banner to accept the installation.

This website wants to install the following add-on: 'WEPX.cab' from 'Websense Inc.'. If you trust the website and the add-on an...

Step 2

Before the Secure Browsing installation can start, a plugin must be added to your browser. You will see a user account control asking you to allow the plugin installation.

Click the Yes button to install the plugin.

Plugin Finder Service

Completing the Plugin Finder Service

No suitable plugins were found.

Unknown Plugin (application/Websense-Endpoint-plugin)

Step 3

The plugin will start the Websense Endpoint Download Manager, which will download the Secure Browsing component. You do not need to perform any actions during this step.

Websense Endpoint Download Manager

Downloading.... 100% completed.

Step 4

Depending on your operating system and security settings you may see this dialog.

Once the download is complete, you will be asked to allow the Secure Browsing installation.

Click the Yes button to complete the installation.

User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows® installer

Verified publisher: **Microsoft Windows**

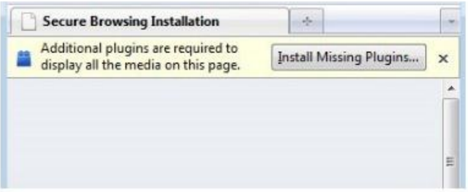
For Firefox 3.6 you will see the following screen.

Secure Browsing Installation

Step 1

A specialized plugin is required to proceed with the Secure Browsing installation.

Click the Install Missing Plugins button.

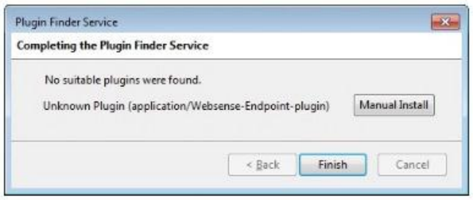

Secure Browsing Installation

Additional plugins are required to display all the media on this page.

Step 2

The Firefox Plugin Finder Service will offer the option to manually install the plugin.

Click the Manual Install button.


Plugin Finder Service

Completing the Plugin Finder Service

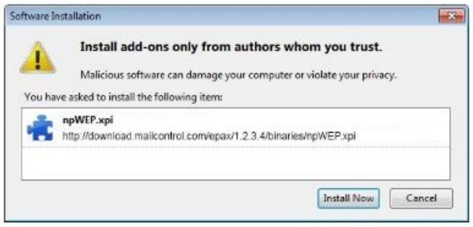
No suitable plugins were found.

Unknown Plugin (application/Websense-Endpoint-plugin)

Step 3

The Firefox Software Installation service will ask you to confirm the plugin installation.

Click the Install Now button.


Software Installation

Install add-ons only from authors whom you trust.

Malicious software can damage your computer or violate your privacy.

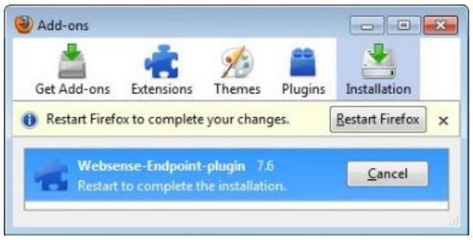
You have asked to install the following item:

npWEP.xpi
http://download.mailcontrol.com/epax/1.2.3.4/binaries/npWEP.xpi

Step 4

Firefox must be restarted to activate the plugin. After the restart, the installation will continue automatically.

Click the Restart Firefox button.

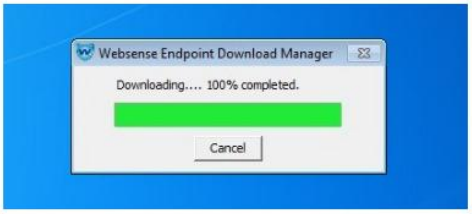

Add-ons

Restart Firefox to complete your changes.

Websense-Endpoint-plugin 7.6
Restart to complete the installation.

Step 5

The plugin will start the Websense Endpoint Download Manager, which will download the Secure Browsing component. You do not need to perform any actions during this step.


Websense Endpoint Download Manager

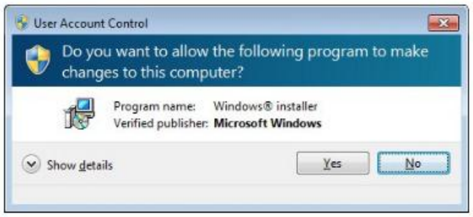
Downloading.... 100% completed.

Step 6

Depending on your operating system and security settings you may see this dialog.

Once the download is complete, you will be asked to allow the Secure Browsing installation.

Click the Yes button to complete the installation.


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows® installer
Verified publisher: **Microsoft Windows**

Continue with the Install

Please note that we detect whether the endpoint is 32 bit or 64 bit from the user-agent string. Since Firefox is 32 bit only, and IE defaults to using the 32 bit version on a 64bit machine, the downloaded file will be the 32-bit installer. The installer however, is just a wrapper, and must then download the full 32-bit or 64-bit package to install. This means even though a 32-bit wrapper is downloaded on 32-bit IE on Windows64, the wrapper will detect the OS is 64 bit and then download the 64-bit package for installation.

Endpoint Auto-Updates

The endpoint supports an auto-update feature, which can automatically deploy newer versions, without desktop administrators getting involved. This is OFF by default, and must be enabled by the portal administrator if required. We choose to turn this off by default as most organizations like to control the software on the desktop themselves and test newer versions before deploying them. There is nothing stopping organizations from switching this to ON once they have tested the new software, so all users (even field-based) get the latest endpoint installed. Once they have all updated, they can then switch it off again.

Please note that while an endpoint update is taking place (which can take several minutes), the end users will be unable to browse, but will be shown a Web page stating that the endpoint is updating. This page will continue to retry the originally-requested URL every 10 seconds until the endpoint has finished updating, and will then display the requested page correctly if the user is allowed to access this URL, or alternatively will display a block page.

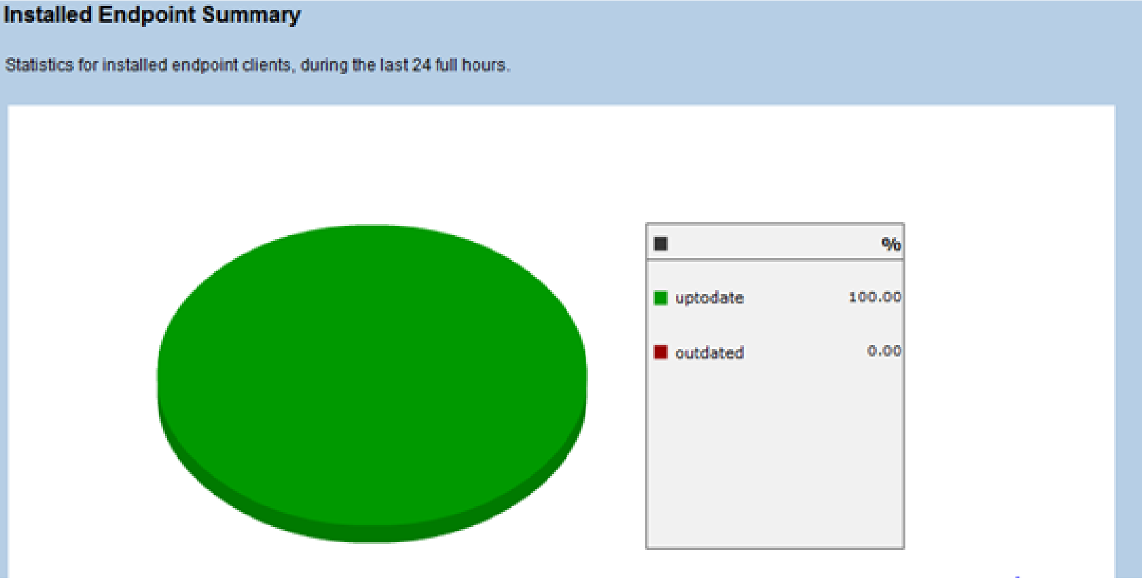
Anti-Tampering Password

Please note you can now set your own anti-tampering password on the Endpoint. For Web Security Gateway Anywhere customers, this is done at the install time as part of the msiexec install string. For Cloud Security customers, the password can be set in the cloud portal and the Endpoints will automatically update themselves with this password within the hour.

Reporting

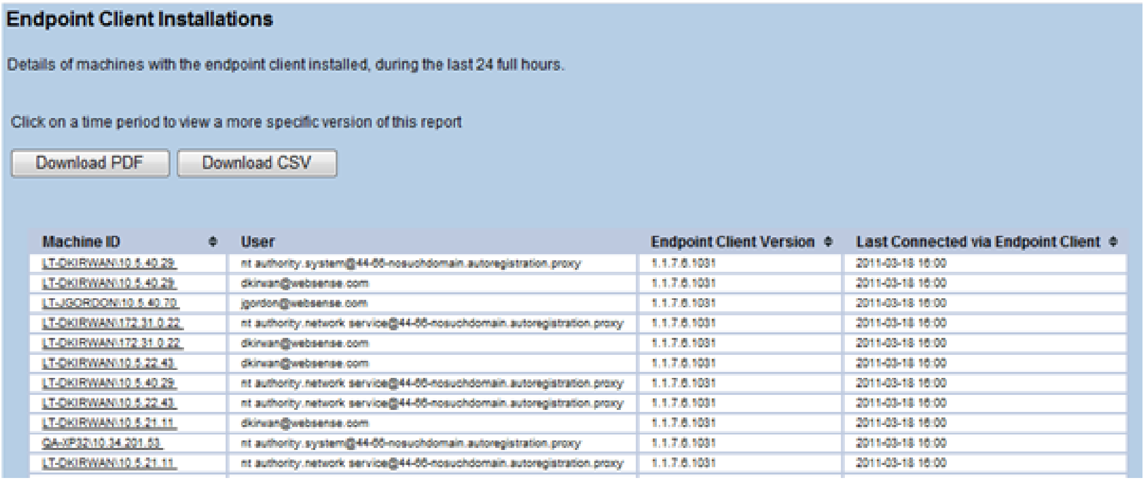
Websense has included an additional 3 reports for endpoints in the 7.6 release:

- **Installed Endpoint Summary -** Statistics for installed endpoints
- **Endpoint Client Installations -** Details of machines with the endpoint installed
- **Endpoint Users -** Details of all users who have browsed the Web using the endpoint



Installed Endpoint Summary

Statistics for installed endpoint clients, during the last 24 full hours.

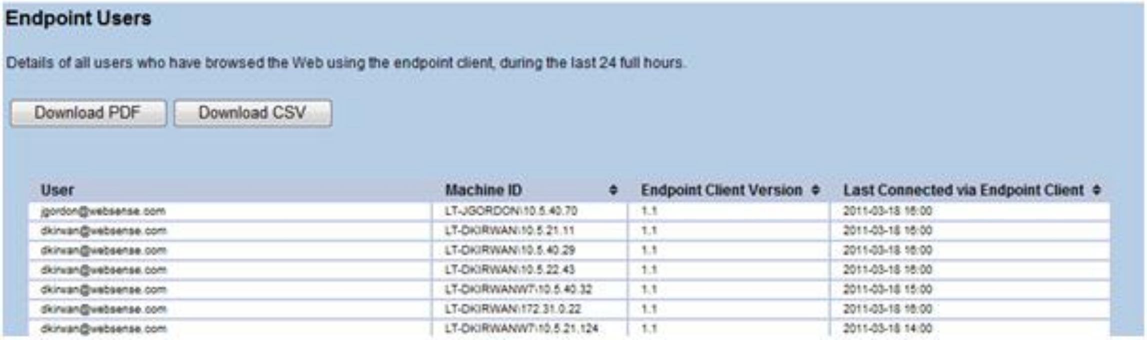


Endpoint Client Installations

Details of machines with the endpoint client installed, during the last 24 full hours.

Click on a time period to view a more specific version of this report

Machine ID	User	Endpoint Client Version	Last Connected via Endpoint Client
LT-DKIRWAN\10.5.40.29	nt authority.system@44-66-nosuchdomain.autoregistration.proxy	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\10.5.40.29	dkirwan@websense.com	1.1.7.6.1031	2011-03-18 16:00
LT-JGORDON\10.5.40.70	jgordon@websense.com	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\172.31.0.22	nt authority.network service@44-66-nosuchdomain.autoregistration.proxy	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\172.31.0.22	dkirwan@websense.com	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\10.5.22.43	dkirwan@websense.com	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\10.5.40.29	nt authority.network service@44-66-nosuchdomain.autoregistration.proxy	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\10.5.22.43	nt authority.network service@44-66-nosuchdomain.autoregistration.proxy	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\10.5.21.11	dkirwan@websense.com	1.1.7.6.1031	2011-03-18 16:00
QA-XP32\10.34.201.53	nt authority.system@44-66-nosuchdomain.autoregistration.proxy	1.1.7.6.1031	2011-03-18 16:00
LT-DKIRWAN\10.5.21.11	nt authority.network service@44-66-nosuchdomain.autoregistration.proxy	1.1.7.6.1031	2011-03-18 16:00



Endpoint Users

Details of all users who have browsed the Web using the endpoint client, during the last 24 full hours.

User	Machine ID	Endpoint Client Version	Last Connected via Endpoint Client
jgordon@websense.com	LT-JGORDON\10.5.40.70	1.1	2011-03-18 16:00
dkirwan@websense.com	LT-DKIRWAN\10.5.21.11	1.1	2011-03-18 16:00
dkirwan@websense.com	LT-DKIRWAN\10.5.40.29	1.1	2011-03-18 16:00
dkirwan@websense.com	LT-DKIRWAN\10.5.22.43	1.1	2011-03-18 16:00
dkirwan@websense.com	LT-DKIRWANW7\10.5.40.32	1.1	2011-03-18 15:00
dkirwan@websense.com	LT-DKIRWAN\172.31.0.22	1.1	2011-03-18 16:00
dkirwan@websense.com	LT-DKIRWANW7\10.5.21.124	1.1	2011-03-18 14:00

Policy Matching

The endpoint forwards an encrypted version of the logged-in user name to the Websense Cloud Security service. If this user name has already been provisioned for this account on the service then they will get the expected policy for that user. If the user name is not provisioned in the system, then we will automatically add the user to the Cloud Security directory for Cloud Web Security (Web Security Gateway Anywhere will have this added in a future release). Since we don't forward the group information in the header (in reality this would add potentially hundreds of bytes to every request if we did this which is not good), these users will be served the default policy. The only exception to this would be if the detected egress IP address had a policy associated with it, in which case the associated policy would be used instead of the default policy for the user.