

HyBlue Secure Desktop/Laptop QuickStart

Welcome to HyBlue Secure. The Secure system is designed to be easy to implement, provide excellent protection, allow single point management of computers yet not intrude on user experience. Combined with HyBlue's Windows Monitor and Patch, you will have unprecedented control of the health and security of computers you manage.

Overview

HyBlue Secure consists of 2 basic elements, the client and the HyBlue Portal. The client, which consists of a number of sub-programs, communicates with HyBlue's Portal about the health, security and patch level of each computer. HyBlue automatically evaluates information from the client and sends back to the client updates regarding security policies. Additionally, the HyBlue Portal allows you to install patches and see the operational history of computers.

Installation

For detailed instructions on installation of Secure, please reference the HyBlue Installation QuickStart available at

https://www.hyblue.com/CustomerTools/docs/howto/hyblue_installation_quickstart.pdf

Please note that to successfully install Secure you MUST UNINSTALL any existing Virus or Spyware scanners. Disabling other virus or spyware software is not sufficient and the installation will fail.

Operation

HyBlue Secure is deceptively simple to use. In many cases you simply install the client and your customers are secure. HyBlue has created a set of best practices that protect computers without adding overhead or reducing functionality. These settings are put in place automatically when Secure is installed. Since all systems are a bit different, you have the ability to customize the installation either on the user's computer or centrally on the HyBlue Portal. Details on our basic settings are shown near the end of this document. You may want to review these basic settings before attempting to make changes.

Configuring Secure is easy. Simply login to the HyBlue Customer & Partner Login and click Secure under Configure Services. This shows the default settings that are in place. You can make changes as needed for each company. When you are done, click

the Confirm button and these settings will be implemented on your systems. Please note that it may take up to 3 hours for the changes to work through our system.

HyBlue is happy to provide you with in depth information regarding each of the policy settings available on request. This in depth information comes as a spreadsheet with all the variables laid out for review. Please let us know if you would like one of these.

The following pages provide an overview of what settings can be adjusted and what their basic range of settings are. Many of these settings require an email or conversation with support.

If you have any questions about the Secure settings, please call support at 206 838 7238 or email support@hyblue.com

Basic Settings for HyBlue Secure

Management Options for the Desktop/Laptop Client

- An administrative user is currently allowed to unload the anti virus products. This can be changed to never allowed or only allowed when not on a network.
- The firewall can not be unloaded, though there is a Basic Protection setting which removes the anti Malware filters. Use this for troubleshooting firewall issues.
- Administrative users are allowed to change certain settings, but not regular users. This can be changed so that no one can change settings
 - Troubleshooting note. It is sometimes handy to login as an administrator where you can disable certain sections of the security client in order to troubleshoot issues.
 -

Laptop/Desktop Secure

- **Virus Protection**
 - Definitions update automatically
 - No indicator is given to user when a virus is found
 - Real-time virus scanning is enabled
 - Manual file scanning is allowed
 - Boot sector and floppies are scanned at startup
 - Viruses found during scan are disinfected automatically and if they can't be disinfected they are renamed. Failure to rename generates an alert to the technical contact
 - Memory is scanned
 - Only the following file extensions are scanned:
 - COM EXE SYS OV? BIN SCR DLL SHS HTM HTML HTT VBS JS INF VXD DO? XL? RTF CPL WIZ HTA PP? PWZ POT MSO PIF . ACM ASP AX CNV CSC DRV INI MDB MPD MPP MPT OBD OBT OCX PCI TLB TSP WBK WBT WPC WSH VWP WML BOO HLP TD0 TT6 MSG ASD JSE VBE WSC CHM EML PRC SHB LNK WSF { * PDF ZL? XML
 - Exclusions can be added on user request
 - Scans can be scheduled centrally or individually
 - POP3/IMAP/SMTP scanning is automatically enabled or disabled depending on need. Outlook connecting to an Exchange Server is not protected by this part of the service.
 - Mail is scanned incoming and outgoing
 - Attachments are disinfected if they can be or removed.
 - Outgoing mail that is infected is stopped
 - Web Traffic Scanning
 - Scanning is enabled, malicious content is blocked
 - System Control
 - Registry protection is on and registry is protected against changes made when no user is present
 - The system will prompt for changes to
 - System Startup
 - Critical file association changes
 - Critical system changes

- The system will allow changes to application association
 - Dialup control is enabled, this keeps unauthorized programs from attempting to dial out.
- **Spyware Protection**
 - Realtime spyware scanning is enabled
 - The hosts file is protected from changes by applications (it can still be edited with a text editor)
 - The system scans for tracking cookies
 - The system quarantines automatically anything it considers Spyware
 - Tracking cookies are deleted automatically
 - Users do receive local alerts of spyware being found and removed.
 - Manual or scheduled scans can be run.
 - These scans look for
 - Active processes
 - Keyloggers
 - Dialers
 - Tracking Cookies
 - Deep scan the Registry
 - Scan system files
 - These scans automatically remove spyware found.
 - Browser popup windows are blocked. Note this can conflict with some applications and can be disabled
 - Users can add allowed or blocked sites to popup rules
 - The Browser Lock is automatically enabled on Internet Explorer
 - Browser lock protects against changes to registry settings, Active X installations and automatic file saving. Users can turn off Browser Lock under Options, IE Shield. They can configure them as well
- **Firewall**
 - There are a number of levels of security available in the system, we use **Office** by default.
 - Other levels are
 - Block all
 - Blocks all traffic
 - Mobile
 - More restricted than office for travelling
 - Home
 - A little more forgiving of games
 - Basic Protection
 - Very basic protection. Keeps general attacks at bay but does not block malware
 - Other levels can be setup for your use and the system does have the capability to "auto sense" which level of security to use. This function is based on parameters like the IP address of the DHCP server and DNS server. You can configure