SECURITY ENHANCED SYSTEM

SECURITY ENHANCED SYSTEM

USER GUIDE

DEF-LOGIX inc.

307 E RAMSEY
SAN ANTONIO, TX 78216

VERSION 1.1.0

TABLE OF CONTENTS

INTRODUCTION

With your purchase of this Security Enhanced System (SES) you have taken an important first step to a more secure computing experience. This SES is built on industry best practices from our years of cyber security research and development supporting the U.S. government. It has been specifically configured to provide you with a safer, more secure computing experience by addressing your Protection, Privacy, Auditing, and Backup needs. We recommend taking a few moments to read this guide before embarking on your new, more secure computing journey. Our hope is that the SES will strengthen your overall security posture to help avoid criminal exploits.

QUICK START

The SES is designed to quickly get you up and running. The most important thing to remember is to use the ‘User’ account for your day-to-day activities. The ‘Admin’ account should only be used for installing software or troubleshooting your PC. The User account privileges are limited, though should be sufficient to complete any normal task while blocking malware’s ability to cause damage.

An action that requires elevated (Admin) privileges will launch the User Access Control (UAC) dialog. This gives you a moment to reconsider your action prior to entering the Admin password and clicking ‘Yes.’

SECURITY ENHANCED SYSTEM MANAGER (SES MANAGER)

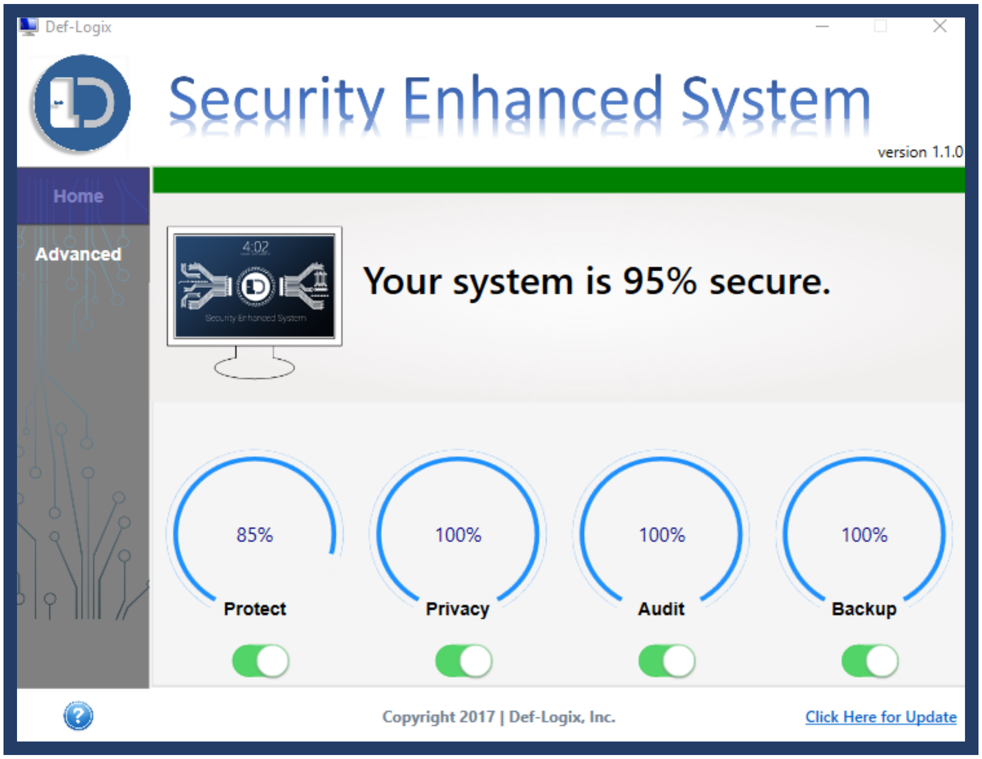
You can access your system’s Protection, Privacy, Auditing, and Backup settings from the SES Manager. The SES Manager allows you to make basic changes to the Protection, Privacy, Auditing, and Backup settings of your system. Your SES is pre-configured with maximum security and privacy in mind; reducing these settings will degrade the effectiveness of your system and put your security posture at risk.

LAUNCHING THE SES MANAGER

Left click the SES Manager icon on your Windows taskbar and enter your admin password to access the SES settings.

HOME

This is the home screen for the SES Manager. It gives you a quick view of your level of 'protection.' You can quickly edit security features by turning them on or off entirely. This will affect the percentage of the system's security.



Def-Logix

Security Enhanced System

version 1.1.0

Your system is 95% secure.

85% Protect

100% Privacy

100% Audit

100% Backup

Copyright 2017 | Def-Logix, Inc.

ADVANCED

The Advanced menu allows you to edit specific settings for each security feature: Protection, Privacy, Audit, Backup, and Other.

For example, under Protection, if you wanted to enable all Protection settings except for one, you can manually edit these specific settings to your liking.

PROTECTION

The default setting for each of these measures is **Enabled**.

Prohibited Execution Zones: Prevents programs from anywhere EXCEPT the following directories:

- Windows
- Program Files
- Program File (x86)

Launch SecureBrowser on Logon: Launches the SecureBrowser when the User logs in. This makes it more convenient to use this important tool. If this setting is disabled or you close the SecureBrowser, it can be launched on demand from the taskbar.

Use Microsoft Hyper-V: Only disable this setting if you want to use VirtualBox or VMWare. Disabling this setting causes the system to reboot and the SecureBrowser will no longer be available.

Restrict Peer to Peer Communications: This setting limits some Peer to Peer interaction.

Restrict Domain Management: Prevents access to known adware and malware websites. The list of prohibited sites is automatically updated each day.

User Hosts File: Provides access to the user defined portion of the hosts file. This is intended for advanced users who need to adjust internal network routing typically done through the hosts file.

Master Hosts File (Temporary): Provides access to hosts file to make temporary changes. Changes will be eliminated when the Restrict Domain Management update process happens. This is intended for advanced users who need to access a website which is listed as prohibited. A better alternative is to use the SecureBrowser when accessing any unsafe, unknown, or suspicious web sites.

PRIVACY

The default setting for each of these measures is **Enabled**.

Cortana Disabled: Cortana is known to collect and transmit user activity to Microsoft to provide a better customer user experience such as searching on the computer or the internet.

Location Services Disabled: Some applications rely on this setting to provide localized content.

Browser Privacy: Not implemented. Please access browser privacy settings through the browser.

Microphone Disabled: Prevents applications from using the microphone. The following applications retain access to the microphone when this setting is enabled: Microsoft Edge, OneNote, Skype, and Voice Recorder.

Camera Disabled: Prevents applications from using the camera. The following applications retain access to the camera when this setting is enabled: Microsoft Edge and Skype.

Other Telemetry Disabled: Disables miscellaneous telemetry.

App Access to Calendar, Contacts, 'Run in Background', etc. Disabled: Prevents specific apps from running in the background.

AUDIT

The default setting for each of these measures is **Enabled**.

Account Logon/Logoff: Logs events related to account logon/logoff in the Windows Event Viewer.

PowerShell: Logs events related to PowerShell in the Windows Event Viewer.

Detailed: Logs more detailed events such as when a process starts, stops, etc. in the Windows Event Viewer.

Registry: Logs events related to changes in specific Registry keys in the Windows Event Viewer.

BACKUP

The default setting for each of these measures is listed below.

Critical Data Backup: (Default: Enabled) Automatically backs up files found in the User profile directory (C:\Users\*) to the external USB (included) each day. This is backup capability is only intended for your most critical files. Does not backup very large files (≥100MB) and has a limited capacity. It is recommended to subscribe to a 3rd party, off-site backup service OR complete frequent, full backups to a removable storage device.

Critical Backup to Restore: (Default: A) Select which backup to restore and click ‘Restore’ to recover from lost files. Please note this replaces existing copies of all files within the User profile directory (C:\Users\*).

Enable System Snapshots: (Default: Enabled) Automatically saved a system restoration snapshot each week. This is useful when a program or driver causes the system to become unstable.

Restore to Snapshot: Select the restoration point and click ‘Restore’ to revert to the system configuration of the stored system restoration snapshot. The system will automatically reboot during this process.

OTHER

The default setting for each of these measures is **Enabled**.

Enhanced Desktop: Enables/disables the animated graphics on the desktop. Depending on your screen resolution, you may want to disable if it doesn’t fit correctly. Changes will be applied on next logon.

Security Enhanced System Log: Displays SES event logs. Entries include enabling/disabling SES settings and automated events such as Critical Data Backups, System Snapshots, and Restrict Domain Management updates. Click the refresh button to update the log.

FREQUENTLY ASKED QUESTIONS

PROTECTION

Your Security Enhanced System (SES) is built on Windows 10 Professional for a secure windows computing experience. Your system has two accounts, admin and user. DO NOT use the admin account for day-to-day activities. The lack of privileges on the user account will protect you from many malicious programs that require administrative privileges.

Q: How do I install new software?
The Security Enhanced System restricts installation of programs to avoid inadvertently introducing malware onto the system. Software installers with an “exe” extension require you to provide administrative credentials to run. Software installers with an “msi” extension must be moved to the Windows folder before it can be run.

Q: Why can’t I just log into and use the Admin account?
The Security Enhanced System was designed to provide maximum security to the normal user. Malware often requires administrative privileges to make the devastating changes to a user’s system. A user who chooses to either grant their normal account administrative privileges or simply uses the administrative account for normal use puts themselves at greater risk of a malware infection.

Q: Why can’t I save my login information or other data that I have previously entered into online forms?
The Security Enhanced System does not allow saving login information or other user entered data within the browser. Saved passwords and other data can be easily taken by hackers who may gain access to your system. We recommend using long, memorable passphrases that are unique between each of your accounts. You might also consider using a good password manager if you would like the convenience of not manually entering your password.

Q: Why do I have to type in the Administrator password when I try to run a program I have downloaded from the internet or my Downloads folder?
The SES was designed to protect normal users from accidentally introducing malware into their system. A good antivirus solution, such as Windows

Defender, can catch many known malware packages. However, the best protection against ALL malware is avoidance.

User accounts have limits on running programs due to software restriction policies. You will be prompted for the admin account password when performing privileged activities. Only enter the admin password if you trust the application you would like to run. You can turn off software restriction policies from the SES Manager, but we do not recommend it.

Q: Can I trust that Windows Defender provides enough protection against malware? Can I download 3rd party antivirus (AV) programs?
The SES relies on Windows Defender and specific Windows 10 operating system configurations to reduce your exposure to malware. Unfortunately, there is no single AV program that protects against all threats. However, if you would like to add to your protective posture, you may consider some of the free or commercial solutions. Please keep in mind that most 3rd party AV solutions will cause Windows Defender to turn off.

Q: Can I change the User/Admin account names?
The user/admin account names can be changed from the Admin account.

— PRIVACY —

Privacy is a high priority in an increasingly connected world. The SES helps protect your privacy while browsing using the pre-installed Chrome browser. We have configured it with maximum privacy settings. We also included Chrome extensions to increase your awareness of how a site handles your personal information (PrivacyCheck). The Chrome browser default search engine is DuckDuckGo. This alternative to Google and other popular search engines DOES NOT track your search activity or sell your information to 3rd party advertisers. We disabled location services and Cortana since these services transmit personal data to Microsoft.

Q: Why shouldn’t I use Cortana?
The Security Enhanced System was configured to provide the highest protection of your privacy. Cortana provides an enhanced user experience based on personalization and prediction. Unfortunately, this requires Microsoft to collect a significant amount of personal data such as key strokes, location, and other sensitive information. However, if you would like to use Cortana, you can disable the Cortana Disabled setting in the Privacy tab of the Advanced menu of the SES Manager.

Q: What is the recommended method for conducting secure online transactions?
The Security Enhanced System includes a SecureBrowser that runs in an isolated virtual machine. The virtual browser is 100% clean each time it is launched. We recommend you use this browser when conducting secure online transactions such as banking or shopping, or when you are unsure of a website's content. The virtual browser should be shut down and restarted before/after conducting any secure online transactions to avoid exposing this information to other websites.

Q: What is DuckDuckGo? Is it safe?
The Security Enhanced System default search engine in Chrome is configured to DuckDuckGo for maximum search engine privacy. DuckDuckGo does not store your personal information, does not follow you with ads, and does not track your activity. See their homepage for more information at https://duckduckgo.com.

AUDIT

Auditing, in cyber security, is when system activity is logged. The SES Audit feature records changes to files and system settings, accessed files, and account logon and logoff. If you use the SES as designed, your system is unlikely to be compromised. However, if you do experience a system compromise, we are standing by to assist you. The SES has been pre-configured with enhanced logging to help identify problems so that we can rapidly help you recover.

Q: What do I do if I get a virus or malware?
The Security Enhanced System has been configured to enhance your security and privacy however it is not infallible. We have enabled extra logging in the event you experience malware activity or other issues. These logs will help us assist you if you encounter an issue.

— BACKUP —

An important preventative measure against ransomware includes frequent backups of your most critical data. The SES comes with a USB memory storage device. The system automatically makes daily backups of the user folders (Documents, Desktop, Downloads, etc). The backup capability will only work with the provided USB and is limited to 12-15 GB. During the backup, you will see a file explorer window popup. We recommend you minimize the window and allow the system to automatically close the window upon completion.

Q: Are all of my files backed up?
The SES includes a basic backup capability to safeguard a limited number of your most critical files. Each day, all user folders (files less than 100MB in size) are backed up to the included USB storage device. If you are a victim of ransomware, these backups are likely to survive the attack. However, storage is limited. If you have the need to back up more than 12GB of personal data, consider an additional cloud backup solution.

Q: How often are my files backed up?
The SES is pre-configured to make daily backups of all user folders. The system maintains two backups, alternating each day.

Q: Are any other files automatically backed up?
The SES is pre-configured to create weekly restore points. In the event your system experiences issues, you can revert to a restore point through the SES Manager Backup section.

— OTHER —

Q: What is a good password?
A longer, memorable passphrase is more secure than a shorter complex password. We recommend passphrases of at least 12 characters with a mixture of upper case letters, lower case letters, numbers, and special characters. Avoid passwords that are so complex they must be written down, unless you are using a good password manager.

SUPPORT

Q: I am having an issue not mentioned in this FAQ; what do I do?
If you are having a problem we have not addressed in the FAQ or in this User Guide, you can always contact us through our website https://www.def-logix.com/contact/. On this page of our website, you can fill out a detailed Technical Support form and we will get back with you within 48 hours.

Please contact **info@def-logix.com** if you have any questions, concerns, or feedback with your Security Enhanced System experience.