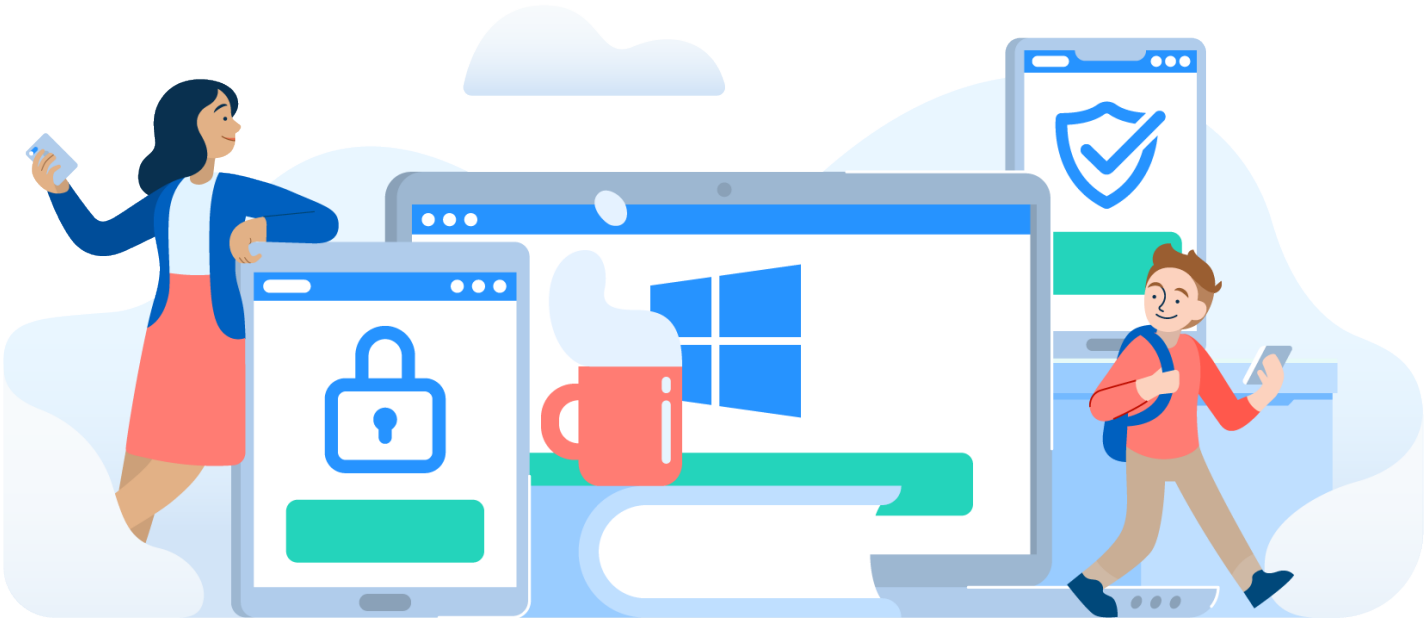
securly://

Windows best practices

A guide to keep your students safe and productive on Windows devices



January 2020

Table of contents

Overview

The one factor that makes any Windows deployment successful is security, AKA ensuring students are using the device safely and productively. This document addresses several aspects of Windows Server and Group Policy Management that are important to configure correctly for a successful deployment. The good news is that most of the Device and User settings described below can be deployed en masse through a Windows Domain Controller, better ensuring that all domain-joined workstations and users receive the appropriate settings.

Note: *If you do not have a Windows Domain Controller, it is still possible to perform most if not all of the below best practices, but it will need to be performed by a Local Administrator individually on each Windows Workstation. So it's highly recommended that one leverage a centralized management solution such as a Windows Domain Controller or MDM.*

Understanding the jargon

Active Directory (AD): A Microsoft service that allows network administrators to create and manage domains, users, and workstations within a network. AD provides a way to organize large numbers of users and workstations into logical groups or subgroups while providing management at each level. (Learn more here.)

Group Policy Object (GPO): A component of Group Policy Management that lets you control both user accounts and workstation settings. The GPO is implemented within an Active Directory Domain according to various Group Policy settings and scope. (Learn more here.)

Man-in -the-Middle Decryption (MITM): Information/data on websites may be encrypted during transmission. The process of translating encrypted data into an understandable or original format is decryption. Securly does selective decryption of sites for filtering, activity logging, and sentiment analysis. Sites that need to be decrypted are routed through our MITM server before connecting the user. (Note: Securly does not decrypt sensitive information, or personally identifiable information(PII) such as credit card numbers, etc.)

Firewall: A protective layer between sensitive information and unauthorized users or illicit software. A firewall acts as the first line of defense and can be implemented using hardware, software, or a combination of both.

Basic Input Output System (BIOS): A low-level program designed to initialize hardware and make resources available for the operating system to run. It manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, etc.

Domain Name System (DNS): Servers that contain a directory of domain names and converts them into IP addresses whenever requests are sent by users. Securly maintains its own DNS servers for its DNS filtering solution.

Secure Sockets Layer (SSL): A security protocol that uses TCP for communication between web server and browser, or mail server and mail client, any server and client for that matter. It is a secure network and creates an encrypted link making it ideal to be used to transmit private and integral data.

Bring Your Own Device (BYOD): This refers to personal devices that users bring to schools instead of using school-owned devices. From a filtering perspective it is important to keep the BYOD architecture segmented from the rest of the school network so that the school network stays protected from malware, harmful software etc. that BYODs might bring in.

Internet Protocol version 6 (IPv6): An updated network layer protocol that gives you more address space, 128-bit length to be precise. IPv6 peacefully coexists with IPv4. It is intended to allow a near-infinite number of devices to connect to the internet. It also comes with the IPSec security embedded into it to help manage encryption and authentication between hosts.

Proxy server: This works as an intermediary between the user's computer and the endpoint machine to fetch information from the endpoint website on behalf of the user. A proxy server helps control which websites students/users can and cannot access.

Transmission Control Protocol (TCP): A network communication protocol that sends data packets over the internet. It breaks large data into small chunks and helps maintain data integrity when the pieces of data are reassembled at the destination node. TCP transports and ensures that the data is delivered to the correct destination.

User Datagram Protocol (UDP): This is an open systems interconnection (OSI) transport layer protocol for client-server network applications and is used to send short messages called datagrams. It's suitable for real-time applications as it sends and receives packets in varying orders and allows for better performance.

Dynamic Host Configuration Protocol (DHCP): A network management protocol used on UDP/IP networks. DHCP servers reduce the need for a network administrator or user to manually assign IP addresses to network devices. Instead, it enables computers to request IP addresses and networking parameters automatically from the internet service provider (ISP).

Best practices

Restrict local administrator permissions

It's critical that average users, including students and most staff, do not have local administrator permissions to their device. Any user with access to such permissions is able to make any setting change they wish, including bypassing any of the best practices outlined in this document. This best practice is most important for schools who function within a workgroup, but it should be noted that even domain workstations have local accounts.

Install the Securly SSL certificate

Securly uses the Man-in-the-Middle (MITM) SSL decryption method on a large number of websites to provide user differentiation, student safety, and reporting for categorized https sites. Unless your Windows workstations are on Securly's Guest Network Policy, it is highly recommended that you deploy the Securly SSL certificate from your domain controller to ensure your end-users have the best experience on the internet. Any devices filtered by Securly that does not have our SSL certificate, run the risk of receiving SSL errors on sites we decrypt. If you do not have a domain controller or other form of centralized management, you can still install the Securly SSL Certificate manually using our one-click installer for both Windows and MacOS. You can also tell BYOD and Guest users to navigate to securly.com/ssl where they'll be prompted with the proper installation steps, video instructions, and direct download link.

- Manual installation guide
- Install via Group Policy Management
- BYOD and Guest SSL Portal

Restrict access to network settings

It's important that users are unable to manipulate the DNS settings received via DHCP from your DHCP server. By changing the DNS IP's, you run the risk of not only breaking internal network name resolution (such as accessing file servers or printers) but potentially being able to bypass Securly's DNS Filter if your Internal DNS Servers are pointing to our Forwarders. For this, ensure that users are unable to edit network settings. This can be achieved by enabling or disabling URIs of specific app pages. To learn more, check out the latest guidelines from Microsoft here.

Enable and configure Windows firewall settings

Enabling your Windows firewall settings will ensure that your users are protected from hackers and malicious software. Enterprising users can also manipulate or block traffic locally if left open, which can potentially be used as a way to inhibit Securly's ability to properly filter a device. To do this, navigate to your Control Panel > Windows Defender Firewall and verify that your firewall settings are turned on. You can enable these settings by GPO as well by following the detailed instructions available here.

Disable IPv6

Securly is working on adding full IPv6 support for all devices in the near future. IPv6 is difficult and expensive to implement for anyone, be it schools or enterprises. Even if your school is already using a dual-stack network solution that supports both IPv4 and IPv6, Securly will filter and scan traffic over IPv4. Filtering will not be impacted even as IPv6 adoption increases. However, it is recommended that you disable it on your DNS Server and/or locally on the workstation itself. To learn what this means as a Securly user, click here.

To disable IPv6 on a Windows DNS Server follow these steps:

1. Right-click “Start” and select “Run” and type in “control.”
2. Open the control panel item "Network and Sharing Center."
3. Click “Change adapter settings.”
4. Double click on the network connections and go to “Properties.”
5. Uncheck the “Internet Protocol Version 6 (TCP/IPv6)” field.
6. Click “Ok” to complete the process.

Set up regular security patches and updates on all devices

Windows security patches and feature updates are a great way to ensure that your users’ devices remain protected from hackers and malware. They also allow users to be compatible with the latest features or applications, making for good user experience in general.

Ensure that Windows Updates are set to automatically download and install on all of your devices. You can also use the Windows Server Update Service (WSUS) to choose which updates you want to push to users’ devices and when. WSUS is important for large Windows deployments as it mitigates the chance of bogging down your network when large updates are released. For details check out this guide from Microsoft. You can also manage Windows updates from the System Center Configuration Manager as explained here.

Restrict users from installing unapproved browser apps and extensions

Within many modern browsers, anyone can install a variety of applications or extensions to enhance their browsing experience. In many cases, these are benign and add value, such as Grammarly and LastPass. However, many applications and extensions can be used for nefarious reasons such as avoiding a school's internet filter.

Restrict app installations on Chrome devices with these steps:

1. Log in to your G Suite account at admin.google.com
2. Navigate to Device Management > Chrome Management > User Settings
3. Scroll down to Apps and Extensions
4. Select the 'Block all apps and extension except the ones I allow' option from the dropdown for the Allow or Block Apps and Extensions field.

For more information refer to our Chromebooks Best Practices guide.

Lockdown browser proxy settings

Allowing users to edit proxy settings can help them bypass filtering. To prevent users from changing the proxy configuration, it's recommended that you enforce a group policy to disable the option for Internet Explorer.

Note: *This affects the End of Life IE only and ensures that the older browser works better while filtered. We cannot guarantee performance on legacy/End of Life browsers.*

For Chrome users, it is recommended that the use of a proxy is set to auto-detection by the system at all times. To disable proxy settings for Chrome:

1. Log in to your G Suite account at admin.google.com
2. Navigate to Device Management > Chrome Management > User Settings
3. Scroll down to Network
4. Select the 'Always auto-detect the proxy' option from the dropdown for the Proxy Settings field.

To disable the proxy settings on a Mozilla Firefox:

1. Double-click Mozilla Firefox icon.
2. On the Mozilla Firefox window, click on Tools then click Options.
3. Click Advanced.
4. Click the Network tab then click on the Settings button.
5. On the Connection Settings window, ensure that the No Proxy option is selected. Then, click on the OK button to apply the changes.

Note: *The latest versions of Firefox trust the internal certificate store by default. This is for legacy versions of Mozilla only*

Implement a strong password policy

Another recommendation is to implement a strict password policy within your Active Directory environment. One that incorporates complexity requirements, password history, and age. This ensures that you're better prepared for users being compromised by hackers and brute force password attacks. To do this, navigate to Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy and set your policy as per guidelines. For more best practices about password rules, click here.

In conjunction with a strong password policy for your Windows domain, it's highly recommended to have that coincide with a thoughtful account lockout policy. If a malicious actor has one of your users' account names and is attempting a brute force attack, you can ensure this account is locked out after a set amount of incorrect attempts. To learn more, click here.

Customize browser homepage

It is possible to predefine a web page that should be automatically displayed when users begin browsing. It's also recommended that you display such pages as your school's Acceptable Use Policy (AUP) here so that students are reminded of following proper online conduct, as well as other school policies they are bound by. This is also great when presenting users to other school resources or SSO methods like ClassLink or Clever.

This can be implemented at scale with GPO's for the following browsers: Internet Explorer/ Microsoft Edge, Firefox, and Chrome.

Conclusion

By following the best practices recommended in this whitepaper, you'll be able to manage all Windows devices in your school while ensuring proper security and a smooth user experience.