SecureSchool Administrator Guide

Published by K12USA.com | support@k12usa.com | 877-225-0100

TABLE OF CONTENTS

NEWS & TIPS 📣

The **News & Tips** section is the first page that loads when logging into the SecureSchool web interface. It provides quick visibility into your system's status, available features, and useful updates from K12USA.

OVERVIEW

The panel is split into several informational tiles:

- **Welcome Message**
  A simple welcome header with a link to download the SecureSchool Manual (when available).
- **Subscription Services**
  Displays the status of your primary SecureSchool service and any additional services your school has subscribed to (e.g., SpamTrakker, MessageGuard, WirelessTrakker).
  - **Green** = Active
  - **Red** = Inactive
- **Optional Services**
  Lists any optional add-ons (e.g., VPN, Load Balancer, Transparent Filtering), along with their activation status and expiration date.
- **News and Tips Panel**
  Includes rotating announcements or helpful insights from the K12USA team, such as:
  - Remote learning guidance
  - Feature spotlights
  - Referral program announcements
- **Interface Traffic Charts**
  Small graphs display real-time bandwidth usage for **Outside Interfaces** and **Inside Interfaces**. Clicking "View More Graphs" opens more detailed traffic statistics.

GOOD TO KNOW 💡

- This page updates dynamically to reflect current service status and K12USA announcements.
- No configuration is required on this screen—it's for **informational use only**.
- If your SecureSchool appliance is offline or services are inactive, this is often the first place to check.

SETUP

BASIC SETUP

The **Basic Setup** page is the starting point for configuring your SecureSchool appliance. Here you define the essential network parameters, including proxy settings, outside (WAN) and inside (LAN) interfaces, and optional VLANs.

Important: Changing these settings incorrectly may cause SecureSchool to stop functioning and may disconnect your school from the Internet. Always confirm values with your network administrator or ISP before making changes.

📌 **Note:** Your SecureSchool appliance is pre-configured by **K12USA** before shipping, based on the network information you provide. You should only make changes here if your network settings have been updated or advised by K12USA Tech Support.

PROXY PORT SETTINGS

- **Proxy Port**: Default is **8080**.
  - This is the port used by SecureSchool's web proxy service.
  - If client devices are configured to use a manual proxy, this port number must match.

OUTSIDE INTERFACE (WAN) SETTINGS

Defines how SecureSchool connects to the Internet.

- **External DHCP Server**
  - If checked, SecureSchool will obtain its external IP address automatically from your ISP.
  - If unchecked, you must manually configure the WAN IP address, subnet mask, and default gateway.
- **External Media**: Typically autodetected; selects the interface type (e.g., Ethernet).
- **Outside IP Address**: The ISP-assigned public IP address for SecureSchool.
- **Outside Netmask**: Subnet mask provided by the ISP (e.g., 255.255.255.248).
- **Default Gateway IP Address**: The ISP's default gateway for routing external traffic.

INSIDE INTERFACE (LAN) SETTINGS

Defines the network SecureSchool uses to communicate with internal devices.

- **Internal Media**: Typically autodetected.
- **Inside IP Address**: The IP address of SecureSchool on the internal LAN (e.g., 10.81.0.1).
- **Inside Netmask**: Subnet mask for the internal LAN (e.g., 255.255.0.0).

Tip: The inside IP address is often set as the default gateway for staff and student devices.

OPTIONAL VLAN INTERFACES

SecureSchool supports additional VLANs to segment traffic (e.g., CCTV, BYOD, or guest networks). Each VLAN interface has its own:

- **Internal Media**: Autodetected.
- **Inside IP Address**: Gateway address for the VLAN (e.g., 192.168.50.1 for CCTV).
- **Inside Netmask**: Subnet mask for the VLAN (e.g., 255.255.255.0).

STATIC ROUTES

The **View** tab displays all active static routes.

Each route includes:

- **Name**: A descriptive label (e.g., *Router Serial*, *WiFi_Spare*).
- **Destination**: The network or host IP/subnet to which traffic should be directed (e.g., 192.168.254.2/30).
- **Gateway**: The next-hop IP address within your network for reaching the destination.
- **Actions**:
    - **Change**: Edit an existing route.
    - **Delete**: Remove a route.

ADDING A STATIC ROUTE

The **Add** tab allows you to define new static routes.

- **Name**: A descriptive identifier (up to 40 characters) to keep track of the route.
- **Destination**:
    - To route to a network: use CIDR notation (e.g., 192.168.0.0/24).
    - To route to a single host: use /32 (e.g., 192.168.0.1/32).
- **Gateway**: The next-hop IP address. This must exist within an already configured network.

Click **Add Static Route** to save.

BEST PRACTICES

- Use clear, descriptive names for routes to simplify management.
- Avoid overlapping subnets, which can cause routing conflicts.
- Only create static routes when absolutely necessary; otherwise, allow SecureSchool's default routing to manage traffic.

INTERFACES

The **Interfaces** page defines the physical and virtual network connections used by SecureSchool, including the outside (WAN) connection, inside (LAN) connection, and any VLANs.

Important: Changing interface settings incorrectly can disconnect your school from the Internet.

Customer Visibility
This section is **not accessible to customers**. Only K12USA technicians can view or modify interface settings. Interfaces are configured during initial setup and should not be changed by school administrators.

WHY THIS MATTERS

Interfaces determine how SecureSchool connects both **outward to the Internet** and **inward to your school's network**. Proper configuration ensures that traffic is routed correctly, devices receive the right gateway information, and VLANs (if in use) remain isolated and secure.

OVERVIEW OF FIELDS

Each interface entry includes the following details:

- **Interface Name**: Descriptive label for the interface (e.g., *Outside Interface*, *Inside Interface*, *CCTV*).
- **Facing**: Indicates whether the interface connects to the **Outside** (Internet) or **Inside** (LAN).
- **Parent Interface**: If applicable, identifies the parent connection for VLANs.
- **Media**: Connection type, typically autodetected (e.g., Ethernet).
- **Full Duplex**: Shows whether the interface is running in full-duplex mode.
- **Method**: Indicates how the IP is assigned (e.g., Static).
- **IP Address**: The assigned IP address of the interface.
- **Netmask**: The subnet mask associated with the IP address.
- **Default Router**: The gateway IP used for external traffic (only applies to WAN/Outside).
- **Driver**: The network driver in use (e.g., *bce*).
- **Tag / Metric**: Used for VLAN configuration and route prioritization.
- **Legacy**: Displays interface role (e.g., *oif* for outside, *iif* for inside).
- **Bandwidth In/Out**: Reserved for bandwidth monitoring (if enabled).
- **Actions**: Options to disable, edit, or delete an interface.

EXAMPLE INTERFACES

- **Outside Interface** – Connects SecureSchool to the Internet via WAN.
- **Inside Interface** – Connects SecureSchool to the internal LAN (staff/student devices).
- **CCTV VLAN** – Example of a VLAN configured for camera systems, linked to the inside interface.

BEST PRACTICES

- Do not attempt to adjust interfaces without K12USA Support guidance.
- Each interface must have a unique IP and subnet to avoid conflicts.
- VLANs can be configured by K12USA if your school requires segmented networks (e.g., CCTV, BYOD, or guest WiFi).
- Report any connectivity issues to K12USA Support rather than modifying interface settings directly.

VHID CONFIG

The **VHID Config** page is used to configure **Virtual Host Identifiers (VHIDs)**, which support advanced network redundancy and failover scenarios. This feature is typically used in high-availability setups where two SecureSchool appliances work together to provide continuous service if one fails.

Customer Visibility
This section is **not accessible to customers**. Only K12USA technicians configure VHID settings, usually during advanced deployments such as high-availability or clustering setups.

MANAGING VHIDS

- **View Existing VHIDs**: Displays a list of configured VHIDs (if any).
- **Add a New VHID**: Opens a form to create a new VHID and assign it to a specific interface.
- **Change/Delete**: Allows K12USA technicians to update or remove existing VHIDs.

WHY THIS MATTERS

VHIDs enable **seamless failover** and **network resilience**. If one appliance goes offline due to hardware failure or maintenance, a backup can immediately take over—ensuring uninterrupted Internet access, filtering, and firewall protection for your school.

EXAMPLE USES

- **High Availability (HA)**: Ensures network continuity by automatically failing over to a backup SecureSchool appliance.
- **Load Balancing**: Distributes traffic across multiple appliances for performance optimization (if configured).

BEST PRACTICES

- VHIDs should only be configured by K12USA Support as part of a planned HA deployment.
- Customers should not attempt to enable or modify this setting.
- Contact K12USA if you are interested in high-availability or redundancy options for your SecureSchool deployment.

SECONDARY IP ADDRESSES

The **Secondary IP Addresses** page allows additional IP addresses to be assigned to an existing interface. This is useful when multiple services or networks need to share the same physical connection but require separate IPs.

📌 **Customer Visibility**
While this page is visible to customers, changes should only be made under the guidance of **K12USA Support**. Misconfiguration may result in loss of connectivity or service disruption.

WHY THIS MATTERS

In some networks, a single interface may need to respond to multiple IP addresses. For example:

- Hosting multiple services on the same external connection.
- Supporting legacy systems or special devices (such as HVAC or security cameras).
- Providing flexibility when additional IPs are issued by your ISP.

By assigning secondary IPs, SecureSchool can handle these scenarios without requiring additional physical network interfaces.

VIEWING SECONDARY IP ADDRESSES

The **View** tab lists all active secondary IP addresses. Each entry displays:

- **Name**: A descriptive identifier (e.g., *ES-HVAC*).
- **For Interface**: The primary interface (e.g., Outside Interface, Inside Interface, VLAN).
- **Address**: The secondary IP assigned.
- **Netmask**: The subnet mask associated with the address.
- **VHID**: If linked to a Virtual Host Identifier (used for HA setups).
- **Actions**: Options to **Edit** or **Delete** the secondary IP.

ADDING A SECONDARY IP ADDRESS

The **Add** tab allows creation of new secondary IP addresses.

- **Secondary IP Address Name**: Descriptive label (e.g., CCTV, HVAC).
- **For Interface**: Choose the interface to which the IP will be assigned.
- **IP Address**: Enter the additional IP address (e.g., 192.168.0.10).
- **Netmask**: Enter the corresponding subnet mask (e.g., 255.255.255.0).
- **VHID**: If used in a high-availability setup, link this IP to a VHID. Otherwise, leave as **None**.

Click **Add Secondary IP Address** to save.

BEST PRACTICES

- Use descriptive names to clearly identify the purpose of each secondary IP.
- Only assign IPs that are provided by your ISP or reserved in your internal network plan.
- Avoid overlapping subnets between primary and secondary IPs.
- Contact K12USA Support before adding or changing secondary IP addresses to ensure proper routing and firewall behavior.

MULTI-NAT

The **Multi-NAT** page allows SecureSchool to support multiple Network Address Translation (NAT) configurations. This feature is typically used when a school is assigned more than one public IP address and wants to map specific services or internal devices to different external IPs.

Customer Visibility
This section is **not accessible to customers**. Only K12USA technicians configure Multi-NAT settings.

WHY THIS MATTERS

Multi-NAT allows SecureSchool to:

- Host multiple public-facing services (such as mail servers, web servers, or VPNs) using different external IPs.
- Assign specific public IP addresses to certain internal devices or networks.
- Increase flexibility for schools with multiple ISP-provided IPs.

Without Multi-NAT, all internal devices and services would share a single external IP address.

MANAGING MULTI-NAT ENTRIES

- **NAT Name**: Descriptive label for the mapping.
- **IP Address**: The external IP assigned by the ISP.
- **CIDRs**: Defines which internal subnets or devices are associated with the NAT entry.
- **Actions**: Options to edit or delete an existing NAT entry.

BEST PRACTICES

- Multi-NAT should only be configured by K12USA Support.
- Use clear naming conventions for NAT entries (e.g., *Mail Server NAT*, *VPN NAT*).
- Ensure firewall rules are updated to match new NAT configurations.
- Avoid overlapping NAT entries, which can create routing conflicts.

HOSTS

The **Hosts** page allows administrators to define, manage, and monitor specific host entries within the SecureSchool network. Hosts can represent individual servers, appliances, or other important devices that need to be tracked or managed.

WHY THIS MATTERS

Defining hosts ensures that SecureSchool recognizes and applies consistent policies to critical devices. This is especially useful for:

- Identifying internal servers (e.g., domain controllers, mail servers).
- Managing appliances or services that require special routing.
- Creating exceptions or blocks for specific hosts.

HOSTS TAB

The **Hosts** tab lists all defined hosts.

Each entry displays:

- **Host Name**: Descriptive name or DNS label (e.g., school-dc1.school.local).
- **Type**: Host type (typically IP).
- **IP Address**: The IP assigned to the host (e.g., 10.10.0.10).
- **Reason**: Notes for why the host entry exists.
- **List Group**: Used to group hosts for easier activation/deactivation.
- **Status**: Displays whether the host is **Active**.
- **Actions**:
    - **Activate/Deactivate** – Enable or disable the host entry.
    - **Change** – Edit the host entry.
    - **Delete** – Remove the host.

BLOCKED TAB

The **Blocked** tab lists hosts that have been specifically blocked from network communication.

Each entry displays the same details as regular hosts (name, type, IP, reason, list group, status, actions).

- **Activate/Deactivate** – Toggle the block.
- **Change** – Edit the block entry.
- **Delete** – Remove the block.

ADD TAB

The **Add** tab allows new hosts to be created.

- **Host Name**: Enter a descriptive label (e.g., library-printer.school.local).
- **IP Address**: Provide the IP address of the device (e.g., 192.168.0.50).
- **Block Host**: Option to immediately block the host instead of allowing it.
- **List Group**: Assign the host to a group for bulk management.
- **Reason**: Enter notes describing why the host is being added.

Click **Add** to save the new host.

BEST PRACTICES

- Use clear, descriptive names for each host entry.
- Group related hosts together (e.g., “Domain Controllers”) for easy management.
- Limit use of the **Blocked Hosts** feature to devices that should never access the network.
- Document reasons for host entries so future admins understand their purpose.

DHCP SERVICES

The **DHCP Services** page controls how SecureSchool manages IP address assignments for client devices on your network. DHCP (Dynamic Host Configuration Protocol) automatically provides devices with an IP address, subnet mask, gateway, and DNS settings—removing the need for manual configuration.

WHY THIS MATTERS

DHCP ensures that devices on your school's network can quickly and reliably connect without manual setup. Using SecureSchool as the DHCP server centralizes control, reduces configuration errors, and allows integration with filtering and firewall services.

SET DHCP SERVICES MODE

Choose how SecureSchool handles DHCP:

- **Don't Use K12USA SecureSchool's DHCP** – Disables DHCP services (another server, such as a Windows server, will provide DHCP).
- **Use K12USA SecureSchool's DHCP Server** – SecureSchool assigns IP addresses and related network information.
- **Use K12USA SecureSchool's DHCP Relay Agent** – SecureSchool passes DHCP requests to an external DHCP server.

Click **Save Changes** after selecting a mode.

MANAGE SCOPES

Scopes define the range of IP addresses that SecureSchool can assign. Each scope includes:

- **Scope Name**: A descriptive label (e.g., *Elementary LAN*).
- **Start IP Address / End IP Address**: The range of assignable IP addresses.
- **Netmask**: Defines the subnet size.
- **Lease Time**: How long a client keeps its assigned IP (e.g., 604800 seconds = 7 days).
- **Available / In Use / Remaining**: Shows scope capacity and usage.
- **Actions**: Options to **Edit** or **Delete** the scope.

RESERVATIONS

Reservations ensure a device always receives the same IP address. This requires:

- The device's **MAC address**.
- The specific IP address you want to assign.

Reservations are often used for servers, printers, or other fixed devices.

EXCLUSIONS

Exclusions are IP addresses or ranges within a scope that DHCP will not assign.

This is useful when certain addresses are reserved for devices with **static IPs** (e.g., servers, printers, or network appliances).

SCOPE DEFAULTS

Default options apply to all scopes unless overridden. Common settings include:

- **DNS Servers**: IP of the DNS server(s).
- **Domain Name**: Internal domain name (e.g., school.local).
- **Time Server / NTP Server**: IP of time synchronization servers.
- **WINS Servers / Node Type**: Used for legacy systems.
- **Web Proxy Auto Detect**: URL for automatic proxy detection (if used).
- **PXE / Boot Options**: For network booting (e.g., imaging labs).

LEASES

The **Leases** tab shows currently active DHCP assignments.

Each entry displays:

- **IP Address**: The assigned IP.
- **Starts / Ends**: The lease period.
- **MAC**: Device hardware address.
- **Hostname**: Device name.
- **Vendor**: Manufacturer of the network adapter.
- **Scope Name**: The scope the lease belongs to.
- **Action**: Convert a lease into a **Reservation** with one click.

BEST PRACTICES

- Use **Reservations** for critical devices (servers, printers, network gear).
- Exclude static IPs from DHCP ranges to prevent conflicts.
- Avoid overlapping scopes across VLANs or subnets.
- Review **Leases** periodically to monitor device usage and detect unknown devices.
- Contact K12USA Support before making large-scale changes to DHCP, especially if another server (like Windows) is also running DHCP in your environment.

AUTH METHOD

The **Auth Method** page controls how SecureSchool authenticates users before applying filtering and firewall policies. Multiple authentication options are available depending on the school's environment (Active Directory, Google Workspace, or local logins).

WHY THIS MATTERS

Authentication ensures that filtering policies are applied **per user** or **per group**, not just per device. This allows schools to customize Internet access by role (e.g., students, teachers, staff) and maintain accountability for network activity.

METHODS TAB

The **Methods** tab allows you to choose the type of authentication used. Options include:

NONE / IP GROUPS

- All users are filtered according to a default filter set, unless assigned to an **IP Group**.

SSB AUTHENTICATION

- Users log in with a username and password once per browser session.
- The appliance stores login and group membership information for filtering.

GOOGLE LDAP

- Integrates with **Google Workspace (G Suite)** accounts.
- Requires setup in the **GSuite Auth** tab.

NTLM

- Users are automatically logged in via Active Directory without entering credentials.
- SecureSchool checks login information against the domain controller.
- Example: Joined to Active Directory domain **SCHOOLAD**.

LDAP

- Generic LDAP authentication for schools using non-AD directory services.

After selecting a method, click **Save Changes**.

FEATURES TAB

The **Features** tab configures optional authentication features:

- **Portal Feature**
  - Displays a login portal for users.
  - **TTL (Time to Live)** determines how long a login remains valid.
    - **Fixed**: Same session length for all users.
    - **Variable**: Users can choose within a set range.
- **Transparent Portal Feature**
  - Integrates login prompts into network access without requiring a portal page.
  - Requires specifying a **Domain** if authentication is tied to Active Directory.
  - Example: Domain name could be schooldistrict.org.
  - TTL applies the same way as above.

GSUITE AUTH TAB

The **GSuite Auth** tab is used when integrating SecureSchool with Google Workspace (formerly G Suite).

- **Certificate Status**: Displays the validity of the Google LDAP certificate (start and end dates).
- **Zip File Upload**: Schools upload a Google-provided ZIP file containing their certificate and key.

For setup instructions, Google provides detailed guidance here: Google LDAP Documentation.

BEST PRACTICES

- Choose the simplest authentication method that meets your needs (NTLM for AD schools, Google LDAP for Google schools).
- Use IP Groups only for special cases (like labs or guest devices).
- Keep certificate files for Google LDAP safe and renew before expiration.
- Test authentication with a small group before rolling out school-wide.
- Contact K12USA Support if you're unsure which authentication method best fits your school.

EXTERNAL DNS SERVERS

The **External DNS Servers** page allows you to configure which DNS (Domain Name System) service SecureSchool will use for resolving Internet domain names.

WHY THIS MATTERS

DNS is essential for converting user-friendly names (like www.school.edu) into IP addresses computers can use. Choosing a reliable DNS service impacts:

- **Speed** – How quickly websites load.
- **Reliability** – Whether DNS lookups succeed consistently.
- **Security** – Some DNS providers filter malicious sites.

SETTINGS TAB

The following options are available:

USE BUILT-IN K12USA SECURESCHOOL DNS SERVICE

- Recommended default.
- Provides reliable, K12USA-managed DNS resolution tailored for SecureSchool.

USE OPENDNS

- Routes DNS through Cisco's OpenDNS service.
- Provides additional filtering and security features.

USE GOOGLE DNS

- Routes DNS requests through Google's public DNS servers (8.8.8.8, 8.8.4.4).
- Often chosen for speed and reliability.

USE EXTERNAL DNS SERVER(S)

- Allows manual entry of up to four external DNS server IPs.
- Useful if your ISP or district IT department requires specific DNS servers.

After making your selection, click **Save Changes**.

CAUTION

Incorrect DNS configuration can **break Internet access** for all users.

- Only change these settings if you fully understand the impact.
- Contact **K12USA Support** if you are unsure which option to select.

BEST PRACTICES

- Most schools should use the **Built-in K12USA SecureSchool DNS Service** for maximum compatibility.
- Only switch to OpenDNS, Google DNS, or custom DNS if required by your IT department or ISP.
- Avoid mixing SecureSchool DNS with third-party DNS without guidance, as this may affect filtering accuracy.
- If entering external DNS manually, double-check that the addresses are correct and reliable.

DOMAIN SPECIFIC NAME SERVERS

The **Domain Specific Name Servers** page allows you to define DNS servers for **internal domains** (such as school.local). This ensures that devices on your network can properly resolve names specific to your local environment (like domain controllers or printers), while still using your main DNS settings for external lookups.

WHY THIS MATTERS

Without proper internal DNS configuration:

- Staff and students may be unable to log in with Active Directory accounts.
- Printers, file shares, or internal applications may not resolve correctly.
- Filtering policies tied to internal directory groups may fail.

This feature ensures that **internal lookups** go to your local DNS servers, while **external lookups** continue using the configured external DNS service.

TABS OVERVIEW

Displays a list of defined internal domains and the DNS servers assigned to each.

- **Internal Domain Name**: Example: school.local
- **DNS Server(s)**: One to four internal DNS server IPs (e.g., 10.81.0.10, 172.16.0.10).
- **Actions**: Options to **Change** or **Delete** entries.

ADD

Allows you to add a new internal domain-specific DNS server entry.

- **Domain Name** – The internal domain requiring custom DNS resolution (e.g., district.local).
- **DNS Server(s)** – Up to four IP addresses for the DNS servers that handle this domain.

Click **Submit** to save.

CHANGE

Edit an existing domain/DNS entry if server IPs change or if additional DNS servers need to be added.

DELETE

Remove an entry if a domain or server is no longer required.

CAUTION

Deleting or misconfiguring internal DNS settings can **disrupt Active Directory logins and access to internal resources**.

- Only modify these settings if you are sure of your internal DNS configuration.
- Contact **K12USA Support** if you are uncertain about which entries to add or edit.

BEST PRACTICES

- Always include at least **two internal DNS servers** for redundancy.
- Use **internal domain names** (like school.local or district.lan), not public ones.
- Do not remove existing entries unless directed by your IT department or K12USA Support.

MULTICAST DNS (MDNS / BONJOUR / ZEROCONF)

The **Multicast DNS** feature enables Bonjour/ZeroConf traffic to function between selected interfaces or VLANs. This is often required for services such as AirPrint, AirPlay, and device discovery on a network with multiple VLANs.

📌 **Note:** This option is only available for customers who subscribe to the **Universal WirelessTrakker add-on**.

ACCESSING MULTICAST DNS

1. From the left-hand navigation menu, go to:
   Setup > Multicast DNS.
2. The configuration page displays the available network interfaces and VLANs.

ENABLING MULTICAST DNS

1. Select the checkbox **Enable Multicast DNS/Bonjour**.
2. Under **mDNS Listen/Send**, choose which interfaces or VLANs should be allowed to pass multicast DNS traffic.
   - **Inside Interface** – Typically your main internal network.
   - **Guest VLAN** – Allows guest devices to discover AirPrint printers or similar resources if enabled.
   - **Staff/Student/Public VLANs** – Allows separation of discovery traffic by role or group.
3. Save your changes.

BEST PRACTICES

- **Enable only where needed** – To reduce unnecessary broadcast traffic, limit mDNS to the VLANs or interfaces that require service discovery.
- **Restrict guest access** – Only enable mDNS on guest VLANs if guests truly need access to shared resources (e.g., a guest-accessible printer).
- **Monitor network performance** – mDNS generates broadcast traffic, so keep an eye on usage if enabling across multiple VLANs.
- **Use descriptive VLAN labels** – When configuring, ensure VLAN/interface names are meaningful (e.g., “Staff,” “Students”) for easier management.
- **Pair with security controls** – If enabled, ensure firewall rules still protect critical resources from unwanted access.

 Tip: Multicast DNS is most commonly used to support **Apple services** (AirPrint, AirPlay, file sharing) across VLANs. If your school does not rely on these services, you may not need to enable this feature.

PROXY EXCEPTIONS

The **Proxy Exceptions** section allows administrators to create a list of websites or hosts that should be accessed directly, bypassing SecureSchool's content filter and proxy service. This feature is typically used for services that do not work correctly when filtered, such as certain cloud services, device management tools, or specialized educational software.

TABS

- **List Exceptions**
  Displays all currently active proxy exceptions. Each entry includes:
  - **Description** (optional label for clarity).
  - **Type** (Subnet, Entire domain, Host, etc.).
  - **Host** (IP address, domain, or subnet).
  - **Action** (Deactivate or Delete the exception).
- **Add an Exception**
  Allows administrators to add a new exception. Required fields include:
  - **Description** – Optional label to identify the rule.
  - **Host** – The domain name (e.g., example.com), host, or subnet.
  - **Type** – Choose whether the exception applies to an entire domain, a specific host, or a subnet.

BEST PRACTICES

- Use proxy exceptions sparingly. Overuse can reduce the effectiveness of SecureSchool's filtering.
- Add exceptions only when required for functionality (e.g., cloud authentication services or trusted device management systems).
- Always test after adding an exception to confirm that the service works as expected.
- Document why each exception was created for easier management in the future.

TIME ZONE

The **Time Zone** section lets you configure the correct local time zone for your SecureSchool appliance. Having the proper time zone ensures that logs, reports, schedules, and other time-based services align accurately with your school's local time.

HOW TO CONFIGURE

1. Navigate to **Setup > Time Zone**.
2. Select the appropriate time zone from the list provided.
    - Time zones are broken down by U.S. regions and special county-level distinctions (e.g., Indiana, Kentucky).
3. Click **Save Changes**.
4. **Important**: You must **reboot the appliance** for the new time zone setting to take effect.

CUSTOMER VISIBILITY

- Time zone configuration impacts reporting accuracy, scheduling, and log timestamps.
- If the time zone is set incorrectly, administrators may see discrepancies in logs (e.g., blocked site attempts, DHCP leases, or authentication events may appear at the wrong times).

BEST PRACTICES

- Always set the time zone during initial installation of SecureSchool.
- Confirm the correct setting after daylight saving time changes to ensure accuracy.
- If your district spans multiple counties with different time rules (e.g., Indiana), make sure to select the **exact county-based time zone**.

LOAD BALANCING

The **Load Balancing** feature allows multiple public Internet connections to be used simultaneously for redundancy and bandwidth distribution.

📌 **Note:** The Load Balancing feature is only available if your school subscribes to the **Load Balancing add-on**.

STATUS

Displays the current health of all configured public connections. Each connection is marked **UP** (active) or **DOWN** (inactive).

- **Green highlight** = active and functioning.
- If a connection goes down, traffic will automatically be shifted to available connections.

SET BALANCE

Allows administrators to assign how traffic is distributed between public connections.

- Use the percentage grid to split traffic between the available WAN connections.
- Example: 70/30 split means 70% of traffic will go out the first connection and 30% out the second.
- Save changes to apply new balancing rules.

WEBSITE ROUTING

Provides the ability to direct specific websites or domains through a particular public connection.

- Click **Add a new Site/Domain…** to configure a rule.
- Useful for ensuring certain services always route through a specific provider (for example, VoIP traffic).

POLICY ROUTING

Enables creation of detailed traffic routing policies based on source and destination IP addresses.

- Each rule specifies:
  - **Source IP** (e.g., a VLAN or device subnet)
  - **Destination IP** (e.g., a service or external host)
  - **Public Connection** (which WAN connection to use)
- Administrators can **Change** or **Delete** policies as needed.

BEST PRACTICE

When configuring load balancing, monitor usage over time to ensure that the traffic split matches real-world needs. Critical services (such as VoIP or video conferencing) should be routed with specific website or policy routing rules for stability.

TASK CENTER

SEARCH CONTROL CENTER

The **Search Control Center** provides administrators with tools to enforce safe search policies and restrict search engine behavior. These settings ensure that inappropriate or undesired content does not appear in search results across commonly used search engines.

OVERVIEW OF OPTIONS

- GOOGLE SEARCH
  Enforces Google's **Strict SafeSearch** filter, which restricts web pages containing explicit sexual content (text and images).
- YOUTUBE RESTRICT MODE
  Provides the option to restrict YouTube content access.
  - **Strict Restricted YouTube** – Maximum restriction for YouTube content.
  - **Moderate Restricted YouTube** – Applies moderate restrictions.

    For more details, see the Knowledge Base article: *YouTube Restricted Mode*.

- DISABLE FIREFOX DNS OVER HTTPS
  Prevents Firefox browsers from bypassing SecureSchool's DNS filtering by forcing standard DNS resolution.
- DISABLE APPLE PRIVATE RELAY
  Stops Apple devices from masking browsing activity through iCloud's Private Relay feature, ensuring all traffic remains filterable.
- FORCE DUCKDUCKGO SAFESEARCH
  Enforces DuckDuckGo's built-in SafeSearch filter.
- BING SEARCH
  Enforces Bing's **Strict SafeSearch** filter, which restricts explicit sexual content (text and images).
- PORNOGRAPHY SEARCH FILTERING
  Blocks search queries for words contained in the **Pornography Search list**.
  - Note: This feature may block entire web pages if flagged keywords appear in the search query string.
  - Requires **Advanced SSL** to function properly.
- CUSTOM SEARCH FILTERING
  Allows administrators to create and enforce a custom list of blocked keywords for search queries.
  - Add words to the block list as needed.
  - Like Pornography Search Filtering, this requires **Advanced SSL**.

BEST PRACTICES

- Always enable **Google SafeSearch** and **Bing SafeSearch** for comprehensive search coverage.
- Use **YouTube Restricted Mode** (Strict) in schools to limit access to inappropriate video content.
- Enable **Disable Apple Private Relay** and **Disable Firefox DNS over HTTPS** to prevent students from bypassing SecureSchool filtering.
- Periodically review and update the **Custom Search Filtering** list to address new or emerging terms of concern.
- Remember that **Advanced SSL** must be configured for keyword-based filtering to work correctly.

ANTI-PROXY CENTER

The **Anti-Proxy Center** helps prevent users from bypassing filtering rules by using outside proxy servers. Proxy servers allow users to mask their browsing activity, which can undermine your SecureSchool filtering policies.

We recommend enabling **all available options** in this section to maximize security and compliance.

OVERVIEW OF OPTIONS

- APPLY TO ALL USERS
  Ensures that anti-proxy rules apply across all staff and student accounts.
- URL FILTERING
  Blocks URLs containing proxy-related keywords. This overrides settings from the **URL Filtering** page.
- WEBSITE ACCESS
  Blocks access to websites known for providing proxy services. This overrides rules on the **Website Access** page.
- BLOCK IP ADDRESSES
  Prevents access to proxy sites accessed by direct IP address (e.g., http://192.168.0.1). This overrides settings from the **Filter Setup** page.
- WEIGHTED WORDS AND PHRASES
  Applies weighted word and phrase rules to detect proxy-related activity. This overrides settings on the **Weighted Words and Phrases** page.
- DENY ALL BY DEFAULT
  Denies all internet traffic by default, except as allowed by Active Rules. This can also be configured on the **Protocol Rules**, **Chat Control**, and **Anti-File Sharing Center** pages.
- NORMAL/HTTP PORT ACCESS
  Blocks ports greater than 1024 for standard HTTP traffic. Exceptions may be managed on the **Port Access** or **Anti-File Sharing Center** pages.
- SSL/HTTPS PORT ACCESS
  Blocks port 443 (used for HTTPS traffic) to prevent encrypted proxy circumvention. Exceptions can be added per filter set (e.g., to allow sites like amazon.com).

BEST PRACTICES

- **Turn everything on:** For maximum protection, enable all available checkboxes.
- **Use exceptions sparingly:** Only add exceptions for trusted sites and services that require them.
- **Audit periodically:** Review the settings and exceptions regularly to ensure students and staff cannot bypass filtering.

ANTI-FILE SHARING CENTER

The **Anti-File Sharing Center** helps block programs and websites that use peer-to-peer (P2P) or other file-sharing services. These services often consume significant bandwidth, pose security risks, and are commonly used to distribute unauthorized or harmful content.

Using this section ensures your SecureSchool appliance enforces stronger controls against unauthorized file sharing across the network.

OVERVIEW OF OPTIONS

- ### WEBSITE ACCESS
  Blocks websites that provide file-sharing services for all filter sets. This setting overrides the File Sharing list found on the *Website Access* page.
- ### WEIGHTED WORDS AND PHRASES
  Applies the Weighted Words and Phrases rules to detect and block terms commonly associated with file-sharing. Overrides the File Sharing word list defined on the *Weighted Words and Phrases* page.
- ### BLOCK IP ADDRESSES
  Prevents web requests made directly to IP addresses (for example, http://192.168.0.1) rather than domain names. This setting helps stop file-sharing programs that attempt to connect directly to servers. Overrides the IP blocking rules configured on the *Filter Setup* page.
- ### DENY ALL BY DEFAULT
  Denies all internet traffic unless specifically allowed by Active Rules. This strict option can be used to lock down access when file-sharing programs are difficult to block by other means. Related settings are also found on the *Chat Control Center* and *Anti-Proxy Center* pages.
- ### NORMAL/HTTP PORT ACCESS
  Blocks ports greater than 1024 for all Normal/HTTP traffic. This prevents many file-sharing programs from running on alternate or non-standard ports. Exceptions can be managed on the *Port Access* page. Related settings are also available on the *Anti-Proxy Center* page.

BEST PRACTICES

- **Enable all blocking options:** Turn on all available protections to prevent circumvention of file-sharing restrictions.
- **Reduce bandwidth strain:** Blocking P2P traffic preserves bandwidth for legitimate educational and administrative use.
- **Audit exceptions carefully:** If exceptions are needed for specific instructional tools, review them regularly to ensure they remain appropriate.
- **Combine with other controls:** Use alongside URL Filtering, Weighted Words and Phrases, and Port Access rules for comprehensive coverage.

E-MAIL CONTROL CENTER

The **E-mail Control Center** helps administrators manage and restrict access to external and internal email services. By blocking unauthorized mail servers and protocols, schools can reduce the risk of spam, phishing attempts, and other email-based threats.

This section also supports configuration of **inside mail servers** by allowing specific IP addresses to bypass general restrictions.

OVERVIEW OF OPTIONS

- WEBSITE ACCESS
  Blocks websites that provide outside email services for all filter sets. This setting overrides the *Mail* list configured on the *Website Access* page.
- WEIGHTED WORDS AND PHRASES
  Applies the Weighted Words and Phrases rules for webmail-related terms across all filter sets. This setting overrides the *Webmail* word list defined on the *Weighted Words and Phrases* page.
- BLOCK MAIL PROTOCOLS
  Blocks direct access to mail servers using SMTP, POP3, and IMAP protocols, unless exceptions are defined.
- OUTSIDE MAIL SERVER IP ADDRESSES – Allows administrators to create exceptions for approved external mail servers by adding their IP addresses.
- INSIDE MAIL SERVER IP ADDRESSES – Allows exceptions for internal mail servers, ensuring that on-premises systems remain accessible while blocking all others.

BEST PRACTICES

- **Block unauthorized mail protocols:** Enable blocking for SMTP, POP3, and IMAP traffic to prevent users from bypassing filtering controls.
- **Allow only trusted servers:** Add only approved outside or inside mail server IPs to ensure email traffic flows through secure and sanctioned channels.
- **Use Weighted Words and Phrases:** Enable filtering for webmail-related terms to strengthen enforcement and prevent circumvention.
- **Combine with Web Access restrictions:** Pair with rules on the **Website Access** page to cover both traditional email clients and web-based services.

ANTI-STREAMING MEDIA CENTER

The **Anti-Streaming Media Center** allows administrators to control and block access to streaming media services such as internet radio, video sites, and web-based downloads. This helps conserve bandwidth, maintain network performance, and ensure students stay focused on educational resources.

OVERVIEW OF OPTIONS

- #### WEBSITE ACCESS
  Blocks websites that provide streaming media services for all filter sets. This setting overrides the *Streaming Media* list on the *Website Access* page.
- #### BLOCK STREAMING MEDIA EXTENSIONS
  Prevents downloading files that use extensions commonly associated with streaming media. This setting overrides file extension blocking rules defined on the *File Extension Blocking* page.
- #### BLOCK STREAMING MEDIA MIME TYPES
  Prevents downloading files identified by MIME types linked to streaming media. This setting overrides MIME type blocking configured on the *MIME Filtering* page.
- #### BLOCK EMBEDDED VIDEO
  Blocks web pages containing embedded videos from specified providers. The system maintains a provider list that is updated as new sources are identified.
  - Administrators can block **all providers** on the list, or choose to block only **selected providers**.
  - End users who attempt to access a blocked video will see a message explaining that the content was restricted due to embedded video detection.
  - For additional customization, filtering rules for embedded video can be managed on the *Embedded Video* page.

BEST PRACTICES

- **Enable broad blocking:** Check the boxes to block streaming-related websites, file extensions, and MIME types for maximum coverage.
- **Use embedded video controls:** Prevent access to embedded videos by blocking providers listed in the control center. This is updated periodically as new providers are identified.
- **Target specific groups:** Apply restrictions more strictly to student filter sets while giving staff more flexibility, if needed.
- **Monitor bandwidth usage:** Combine with SecureSchool's reporting tools to identify excessive streaming and adjust policies as appropriate.

CHAT CONTROL CENTER

The **Chat Control Center** provides tools to block common instant messaging and chat programs from being used on your network. These applications often bypass web filters, consume bandwidth, and can distract students from educational tasks.

Administrators can block popular services (such as AOL Instant Messenger/ICQ, MSN Messenger, and Yahoo Messenger), as well as apply broader restrictions to deny all traffic, block chat-related websites, or filter by weighted keywords and phrases.

OVERVIEW OF OPTIONS

- #### BLOCK AOL INSTANT MESSENGER (AND ICQ)
  Blocks access to servers and communication protocols used by AOL Instant Messenger and ICQ. This setting overrides MIME type blocking on the *MIME Filtering* page and file extension blocking on the *File Extension Blocking* page.
  > **Note:** This only blocks the default AOL communications port (5190). Since AOL and ICQ can also use alternate ports, it is recommended to enable **Deny All by Default** for comprehensive coverage.
- #### BLOCK MSN MESSENGER
  Blocks access to servers and communication protocols used by MSN Messenger. This setting overrides MIME type blocking on the *MIME Filtering* page.
  > **Note:** This only blocks the default MSN communications port (1863). MSN may attempt to use alternate ports, so enabling **Deny All by Default** is also recommended.
- #### BLOCK YAHOO MESSENGER
  Blocks access to servers and communication protocols used by Yahoo Messenger.
- #### DENY ALL BY DEFAULT
  Denies all internet traffic for all filter sets unless explicitly allowed by Active Rules. This provides the most restrictive enforcement and is also available under the *Protocol Rules* page, *Anti-Proxy Center*, and *Anti-File Sharing Center*.
- #### WEBSITE ACCESS
  Blocks websites that provide chat services for all filter sets. This setting overrides the *Chat* list on the *Website Access* page.
- #### WEIGHTED WORDS AND PHRASES
  Applies the Weighted Words and Phrases rules for chat-related terms across all filter sets. This setting overrides the *Chat* word list defined on the *Weighted Words and Phrases* page.

BEST PRACTICES

- **Enable legacy chat blocking:** Although many older chat services are no longer widely used, enabling blocks for AOL, MSN, and Yahoo Messenger adds an extra layer of protection.
- **Use "Deny All By Default" cautiously:** This option can lock down traffic completely, but should be used only in strict environments where all access must be explicitly allowed.
- **Block chat-related websites:** Prevent access to modern web-based chat platforms by enabling website restrictions.
- **Apply weighted word filters:** Add keyword-based filtering to catch emerging chat programs or messaging tools that are not specifically listed.
- **Apply student vs. staff policies:** Block all forms of chat for student filter sets while leaving flexibility for staff if messaging is needed for administrative purposes.

NETWORKTRAKKER

NetworkTrakker is an optional add-on that allows administrators to monitor hosts, services, and devices across the network. It provides visibility into uptime, outages, and performance metrics, while also supporting notification groups and schedules to ensure timely alerts.

📌 **Note:** This feature is only available if your school subscribes to the **NetworkTrakker add-on**.

SETUP

The **Setup** section allows you to define the hosts and organizational structures that NetworkTrakker will monitor. There are four tabs:

- **Hosts** – Add and manage individual hosts. Each host record includes a name, description, IP address, type, host group, notification group, SNMP community, and actions (edit, delete, manage services, and manage data recorders).
- **Host Groups** – Organize hosts into logical groups (e.g., switches, servers, UPS devices, vape detectors). Groups make it easier to manage and view related devices.
- **Notification Groups** – Create and manage groups of users who will receive alerts. For example, you might have a "Tech" group with multiple staff members listed.
- **Notification Scheduling** – Define schedules for when notification groups receive alerts (e.g., 24x7, work hours, weekends).

STATUS

The **Status** page shows the real-time state of all monitored hosts and services. Two tabs are available:

- **All** – Displays the status of every monitored device. Color-coded indicators (green = UP, red = DOWN, pink = CRITICAL) make it easy to spot issues.
- **By Group** – Displays status grouped by host group (e.g., Cameras, Switches, UPS).

Additional status details include:

- **Service** being monitored (e.g., ping).
- **Host** name.
- **Group** membership.
- **For** (duration of current state).
- **Since** (date/time state began).
- **Info** (e.g., packet loss or round-trip average).

GRAPHS

The **Graphs** section provides historical performance data by host and service. Two tabs are available:

- **Graph Sets** – Organize multiple graphs into sets for easier viewing and management.
- **Graphs** – Create and view graphs for specific hosts. You must first add data recorders to hosts before graphs can be generated. Graphs display metrics such as ping response times, packet loss, and service availability.

WEBSITE FILTERING

FILTER SETUP

The **Filter Setup** page allows administrators to configure baseline web filtering behavior for each **Filter Set**. A Filter Set defines the policies applied to specific groups of users (e.g., administrators, staff, or students). Schools may also create their own custom filter sets to tailor restrictions to local requirements.

OVERVIEW

From the dropdown menu at the top of the page, select the Filter Set you want to configure. Each set can have different filtering rules, providing flexibility for managing various user groups. The configuration options include:

YOUR CUSTOM SETTINGS

- **Block All Websites** – Prevents all web access.
- **Block All Except Whitelisted Sites** – Only sites explicitly marked as unfiltered in WEBSITE ACCESS will be available.
- **Allow All Except Blacklisted Sites** – Default setting; all sites are allowed unless blocked in WEBSITE ACCESS.

BLOCK IP ADDRESSES

When enabled, requests made with raw IP addresses (e.g., http://192.168.0.1) are blocked. This ensures that only valid domain names (e.g., http://example.com) are allowed, preventing circumvention of filtering rules.

BLOCK INTERNATIONALIZED DOMAIN NAMES (IDNS)

Blocks access to domains containing non-Latin characters or diacritics (e.g., Arabic, Hangul, Cyrillic). This option can help reduce exposure to phishing attempts using deceptive characters.

SIMPLE SSL INTERCEPTION

Intercepts SSL traffic without requiring certificate installation. Useful for basic inspection but limited in scope.

ADVANCED SSL INTERCEPTION

Provides full SSL inspection:

- **Off** – SSL traffic is not intercepted.
- **On for Select Sites** – Only applied to chosen sites.
- **On for All Sites** – Full interception, but may affect performance.

📌 **Note:** This feature requires the **Advanced SSL Intercept** add-on subscription. **Important:** These features only filter WEB SERVICES from sites. To block **all services** from a domain (such as FTP or Telnet), use the **Protocol Management** feature.

WEBSITE ACCESS

The **Website Access** section allows administrators to configure, review, and manage site filtering rules for each filter set. SecureSchool provides a series of predefined lists (e.g., Gambling, Social Networking, Chat) that are automatically updated to ensure new sites are blocked as they are discovered. Administrators can also create and maintain their own custom lists.

Access is configured by **Filter Set**, ensuring that students, staff, or custom groups can have different levels of access.

VIEW LISTS

Displays all available filtering categories (e.g., AI sites, File Sharing, Gambling, Social Networking).

- Each category shows whether it is currently active (checked = blocked).
- Clicking **View List** opens the specific domains contained in that list.
- Categories are updated automatically but may be customized by enabling or disabling them for the selected filter set.

VIEW SITES IN LISTS

Allows administrators to view the actual websites included in a selected list.

- Select a list from the dropdown (e.g., Gambling, Chat, Social Networking).
- A detailed list of domains within that category will be displayed.

SEARCH FOR SITES IN LISTS

Provides a search tool for quickly locating whether a specific website is contained in one or more filtering lists.

- Select the categories you want to search in.
- Choose a search method: **Begin With**, **End With**, **Contain**, or **Exactly Match**.
- Enter the keyword or domain and click **Search**.

ADD SITES

Administrators can add custom sites to be **Blocked**, **Content Filtered**, or **Unfiltered**.

- Enter the website address (without http:// or https://).
- Optionally include a **Reason for Change**.
- Choose the filtering rule (Blocked, Content Filtered, or Unfiltered).
- (Optional) Enable **Port Access Rules** for the site (opens required ports such as HTTPS/SSL).
- Apply changes to one or multiple filter sets, then click **Submit**.
- **Bulk Add:** Instead of entering sites one by one, administrators may paste a list of multiple sites into the form.

Common Mistake

- Incorrect: entering http://www.example.com/
- Correct: entering example.com

You can also add a reason for the change, which is helpful for tracking and documentation.

UNBLOCK REQUESTS

Displays requests submitted by users when they attempt to access blocked sites.

- Each request shows:
  - The user's email address
  - The IP address used
  - The requested website
  - The reason provided by the user
- Administrators may choose to **Allow Access**, keep the site blocked, or **Delete the Request**.

TIME RESTRICTIONS

The **Time Restrictions** feature allows administrators to limit Internet access for a specific filter set during designated times. Using a simple grid-based interface, you can permit or block access in customizable time intervals.

OVERVIEW

- Time restrictions are configured **per filter set** (e.g., Students, Staff, etc.).
- The grid displays days of the week across the top and time slots down the side.
- **Green blocks** = Allowed times.
- **Red blocks** = Blocked times.

HOW TO CONFIGURE

1. Select the filter set from the drop-down menu.
2. Check **Use Time Restrictions** to enable.
3. Choose the display range (e.g., starting at 12 AM, in 60-minute increments).
4. Click blocks on the grid to toggle access:
    - **Single-click selection**: Toggle individual time slots (green = allowed, red = blocked).
    - **Range selection**: Select a start and end block; all blocks in between will be set accordingly.
5. Click **Save Time Settings** to apply changes.

📌 NOTES

- Once you begin setting restrictions using a specific increment (e.g., 60 minutes), you cannot switch to a different increment (e.g., 30 minutes) unless you first **clear all existing settings** using the **Clear Existing Settings** button.
- Time restrictions apply only to **web access** filtering. Other services (such as email or VPN) are not affected.

PORT ACCESS

The **Port Access** section allows administrators to control which network ports are permitted for specific filter sets. By default, all ports are blocked. Administrators can add rules to allow access to specific ports, ensuring secure yet flexible connectivity for approved applications or sites.

LIST ALLOWED PORT RULES

Displays all currently permitted port rules. Each entry shows the port number, type (Normal/HTTP, SSL/HTTPS, etc.), associated IP or site, and available actions (Deactivate/Delete). Administrators can quickly review and manage existing rules from this list.

ADD AN ALLOWED PORT RULE

Provides a form to create new port rules:

- **Port**: Enter a number between 1–65535, or a range (e.g., 300–400).
- **Type**: Choose NORMAL/HTTP or SSL/HTTPS.
- **Site**: Enter a website address or IP address. Use any to apply the rule to all sites.
  - Do not include http:// in the entry. Only use the domain (e.g., example.com not www.example.com/index.html).
- Rules can be applied selectively to one or more filter sets.

📌 **Example – Correct vs. Incorrect Entry**

- ✅ Correct: example.com
- ❌ Incorrect: http://www.example.com/index.html

BEST PRACTICES

- Only enable ports necessary for educational or administrative functions.
- Use domain- or IP-specific rules when possible to limit exposure.
- Periodically review allowed port rules to ensure they are still required.

📌 **Note:** Port Access Rules apply **per Filter Set**. This means rules configured for staff may differ from those configured for students, allowing administrators to customize access policies based on user groups.

AUTHENTICATION EXCEPTIONS

The **Authentication Exceptions** page allows administrators to configure websites that bypass proxy authentication requirements. While this feature exists for compatibility reasons, it should be used with caution, as adding exceptions can sometimes create more problems than it solves.

⬘ Important Considerations

- Websites on this list **do not require Proxy Authentication**.
- Adding a website to this list **does not unfilter it**—the site will still follow the filtering rules applied to the selected filter set.
- Any site added here will apply to **all users** within the selected filter set.
- In most cases, problems accessing a website can be resolved by other methods, such as adding the site to **Website Access** instead.

List Websites

- Displays all websites currently exempt from proxy authentication.
- Shows details such as:
  - **IP or Website Address**
  - **Action** (Delete option)
  - **Added by**
  - **Date**
  - **Reason** (if provided)
- To remove an exception, click **Delete** next to the site.

Add a Website

- Use this form to add a new authentication exception.
- Enter the **IP or domain name** (without http:// or https://).
- Provide a **reason for the change** (required).
- Click **Submit** to save.

CACHING EXCEPTIONS

The **Caching Exceptions** page allows administrators to manage a list of websites that will not be cached by SecureSchool. Normally, web caching improves performance by temporarily storing frequently accessed content. However, some websites may not function properly when cached, requiring an exception.

📌 **Note:** Adding a website to the caching exceptions list may slow down access to that website since content will no longer be stored locally.

LIST WEBSITES

- Displays all websites currently added to the caching exceptions list.
- Sites on this list bypass caching but remain subject to filtering rules.
- Administrators can click **Delete** to remove a site from the list.

ADD A WEBSITE

- Allows administrators to add new sites to the caching exceptions list.
- To add a website:
    1. Enter the IP address or domain name.
        - Do not include http:// or https://.
        - Example: www.example.com or example.com
    2. Provide a **Reason for Change** (required).
    3. Click **Submit** to save.

BEST PRACTICE TIP

Use caching exceptions sparingly. Adding too many sites may decrease overall web performance for users across the network. Only add sites that fail to function properly when cached.

IP EXCEPTIONS

The **IP Exceptions** feature allows administrators to exempt specific workstations from web filtering until a defined expiration date. This can be useful for testing, troubleshooting, or granting temporary unfiltered access for a specific need. However, exceptions should be used sparingly to maintain compliance with CIPA requirements and E-Rate funding rules.

 Warning: CIPA compliance requires that ALL internet-connected devices have filtering enabled. Disabling filtering entirely may put funding eligibility at risk. Use this feature with caution.

LIST IP EXCEPTIONS

- Displays all current IP exceptions, including:
  - **Name** of the workstation.
  - **IP Address** with subnet notation.
  - **Exception Until** (expiration date).
  - **Action** (option to delete).
- Results are sorted by expiration date by default.
- Clicking on an IP address allows editing of its exception settings.

ADD AN IP EXCEPTION

- To create a new exception:
  - Enter a **Name** to identify the workstation.
  - Provide the **IP Address**.
  - Set an **Expiration Date** for when filtering should automatically resume.
  - Click **Submit** to apply the change.

BEST PRACTICES

- Use IP exceptions only for short-term, specific needs.
- Always assign an expiration date rather than leaving exceptions open-ended.
- Document the reason for each exception to maintain accountability.
- Regularly review and clean up expired exceptions.

SSL INTERCEPT SITES

The **SSL Intercept Sites** page allows administrators to specify which websites should be subject to SSL interception. Once added, traffic to these sites will be decrypted, inspected, and filtered according to your SecureSchool rules.

📌**Note:** This feature is only available with the **Advanced SSL Intercept add-on subscription**.

SETTINGS

- #### LIST SSL INTERCEPTION SITE
  Displays all sites currently configured for SSL interception. If no entries are listed, SSL interception is not being applied to any specific sites.
- #### ADD A NEW SSL INTERCEPTION SITE
  Allows administrators to add a new website or IP address to the interception list.
  - Enter only the domain portion (e.g., example.com) — do not include http:// or https://.
  - Provide a reason for adding the site.
  - Select one or more Filter Sets (e.g., Staff, Students, Administrators) to which the rule should apply.

Once added, traffic to the site(s) will be decrypted and filtered under the selected Filter Sets.

BEST PRACTICES

- **Limit SSL Interception to Essential Sites:**
  Only add sites where deep inspection is required (e.g., search engines, social media, or other content-rich platforms). Excessive use may cause performance issues.
- **Communicate with Users:**
  Some applications may break if SSL interception is applied. Inform staff and students ahead of time when enabling interception for widely used platforms.
- **Regularly Review Your List:**
  Periodically audit the SSL Intercept Sites list to remove obsolete or unnecessary entries.
- **Test Before Applying to All Filter Sets:**
  Consider applying new interception rules to a limited Filter Set (e.g., staff) before extending them to students to ensure compatibility.

TOP-LEVEL DOMAIN BLOCKING 🌐

The **Top-Level Domain (TLD) Blocking** feature lets administrators block or allow access to websites based on their top-level domain (for example, .com, .org, .net, .biz, .cn). This provides an additional layer of control over internet usage, especially when entire categories of domains are deemed unnecessary or risky.

Blocked TLDs appear in **red**, while TLDs saved for future blocking are shown in **green**.

LIST TLDS

The **List TLDs** tab displays all currently available and managed top-level domains.

- **Blocked TLDs (red):** Websites ending with these domains are actively blocked.
- **Saved TLDs (green):** These are stored for potential future blocking but are not currently restricted.
- Administrators can:
  - **Block Top Level Domain** → Immediately block all sites under that domain.
  - **Don't Block Top Level Domain** → Keep the TLD saved but not blocked.
  - **Delete** → Remove the TLD entirely from the list (only available for domains you've manually added).

ADD A NEW TLD

The **Add a New TLD** tab allows administrators to manually add a top-level domain for management.

- Enter the **domain name** (e.g., .xyz, .info).
- Add a short **description** (optional, for internal reference).
- Save the entry, after which the TLD will appear in the list for management.

BEST PRACTICES

- **Target high-risk domains first.** Many spam, phishing, or malware sites use obscure or inexpensive TLDs such as .xyz, .top, .club, .cn, or .ru.
- **Avoid blocking common domains** (like .com or .org) as this can unintentionally disrupt legitimate access.
- **Review new proposed TLDs periodically.** Newly introduced or low-cost TLDs often become havens for malicious activity.
- **Document changes.** When blocking or saving a TLD, note the reason so future administrators understand the rationale.

YOUTUBE FILTERING

The **YouTube Filtering** section allows administrators to control access to YouTube content by filter set.

📌 **Note:** This feature requires the **Advanced SSL Intercept add-on subscription**. SSL Interception must be enabled for the selected filter set. If SSL Interception is not active, a red warning banner will display at the top of the page, and any settings made here will have no effect.

SELECT METHOD

Administrators can choose how YouTube content is handled for the selected filter set:

NO SPECIAL HANDLING OF YOUTUBE CONTENT

All YouTube videos are subject to normal filtering rules without additional restrictions.

ALLOW INDIVIDUAL YOUTUBE VIDEOS BY UNIQUE ID

This option enables fine-grained control by allowing specific videos to be whitelisted using their unique YouTube ID. All other videos will be blocked.

📌 *Note: This method ensures that only videos explicitly approved by administrators are accessible, preventing circumvention through recommended or related video links.*

FILTER VIDEOS

When the individual-video filtering method is selected, the **Filter Videos** tab becomes active.

ADDING YOUTUBE VIDEOS

- Each video is identified by an 11-character YouTube ID (found in the URL after v=).
  - Example: https://www.youtube.com/watch?v=VLDeTOQg2hE → ID = **VLDeTOQg2hE**
- Admins can paste single IDs or a list of IDs with descriptions directly into the form.
- Descriptions help with identifying the video's content (e.g., "Ocean video" or "Lighthouse video").

MANAGING ENTRIES

- Use the **Add…** button to expand the form for multiple entries.
- Use **Submit All** to save new videos at once.
- Use **View** to preview a video in a new window.
- Use **Delete** to remove unwanted entries.

BEST PRACTICES

- Use descriptive labels for each video to simplify management later.

- Review video requests regularly to ensure only educational and appropriate content remains approved.
- Apply this method sparingly — approving only videos that serve instructional or district-approved purposes.

CONTENT FILTERING ✂

WEIGHTED WORDS AND PHRASES

 CONTENT FILTERING FEATURES, INCLUDING WEIGHTED WORDS AND PHRASES, ONLY FUNCTION IF YOUR SCHOOL IS SUBSCRIBED TO THE ADVANCED SSL INTERCEPT ADD-ON.

The **Weighted Words and Phrases** section allows administrators to control web access by assigning weights (positive or negative values) to specific words or phrases found on web pages. If a page's total weight exceeds the set threshold for the filter set, that page will be blocked.

OPTIONS AVAILABLE

CHOOSE RULE LISTS

- Select which predefined word/phrase lists to use (e.g., Gambling, Illegal Drugs, File Sharing, Social Networking).
- You can also create and use a custom list.
- Activated lists apply to the selected filter set (e.g., SSB_STUDENTS).

VIEW/CHANGE RULES

- Displays the individual rules for the selected list.
- Each rule shows the word/phrase, its weight, and whether it is active.
- Options include activating/deactivating rules or customizing weights.

SEARCH FOR RULES

- Search across selected lists for specific words or phrases.
- Match options include:
  - Exactly matches
  - Starts with
  - Ends with
  - Contains
  - All rules with

ADD RULES

- Create custom rules for a filter set.
- Define the word/phrase, assign a weight, and optionally block the web page outright.
- Multiple conditions can be combined with the **And…** button.

HOW IT WORKS

- Explains the logic behind weighted filtering:
  - "Good" words add positive values.

        - "Bad" words add negative values.
    - Matching types include Exact Match, Contains, Begins With, Ends With.
    - Example: BREAST alone could add a negative weight, but a phrase like CHICKEN BREAST might be weighted differently to avoid false positives.

KEY NOTES

- Predefined lists (e.g., Proxy, Pornography, Weapons) are updated by K12USA to reflect evolving filtering needs.
- Rules apply per **Filter Set** (e.g., students, staff, administrators).
- Administrators can fine-tune lists or add their own rules for greater precision.

WEIGHT THRESHOLD

 CONTENT FILTERING FEATURES, INCLUDING WEIGHT THRESHOLD, ONLY FUNCTION IF YOUR SCHOOL IS SUBSCRIBED TO THE ADVANCED SSL INTERCEPT ADD-ON.

The **Weight Threshold** setting determines the point at which a webpage is blocked based on the cumulative values assigned to words and phrases (see: WEIGHTED WORDS AND PHRASES).

When a page is scanned, all rules that match are added together to produce a total score. If the score exceeds the threshold set for the filter set, the page will be blocked.

SUGGESTED STARTING VALUES

- **70** for elementary school students
- **120** for middle school students
- **180** for high school students
- **300** for staff

📌 NOTE: THIS FEATURE IS DISABLED BY DEFAULT FOR ADMINISTRATORS BUT CAN BE ENABLED IF DESIRED.

KEY NOTES

- The **higher** the Weight Threshold, the less likely a page will be blocked.
- Setting the threshold too **high** will make Weighted Words and Phrases filtering ineffective.
- To **disable** Weighted Phrase Filtering entirely for a filter set, set the threshold to **0**.
- Settings apply per **Filter Set** (e.g., SSB_Students, SSB_Staff).

ADJUSTING THRESHOLDS

1. Select the desired **Filter Set**.
2. Enter the new threshold value in the form.
3. Click **Save Changes** to apply.

PICS FILTERING

 CONTENT FILTERING FEATURES, INCLUDING PICS FILTERING, ONLY FUNCTION IF YOUR SCHOOL IS SUBSCRIBED TO THE ADVANCED SSL INTERCEPT ADD-ON.

PICS Filtering is based on a system established by the Internet Content Rating Association. It relies on voluntary self-rating of web pages by publishers. When enabled, SecureSchool will block or allow pages based on the PICS ratings defined by their creators.

FILTER OPTIONS

For each filter set (e.g., SSB_STUDENTS), you may select one of the following:

- **Don't Use PICS Filtering** (DEFAULT)
- **PICS Filtering for Young Adults (14–16)**
- **PICS Filtering for Young Teens (13)**
- **PICS Filtering for Very Young Children**

IMPORTANT NOTES

- Since PICS filtering depends on websites voluntarily rating their own content, coverage is limited and not always reliable.
- K12USA recommends relying primarily on **Weighted Words and Phrases** and **Category Filtering** for more consistent results, using PICS only as a supplemental safeguard.
- Settings apply **per Filter Set**, so you can enforce stricter policies for students while leaving staff unaffected.

ADJUSTING PICS FILTERING

1. Select the desired **Filter Set** from the dropdown.
2. Choose the appropriate PICS filtering level.
3. Click **Save Changes** to apply.

FILE EXTENSION BLOCKING

The **File Extension Blocking** feature allows administrators to control whether certain types of files can be downloaded or accessed through the web. Blocking potentially harmful or unnecessary file types helps maintain network security and reduces bandwidth usage.

📌 **Note:** File Extension Blocking is only effective if the school is subscribed to the **Advanced SSL Intercept add-on.**

LIST EXTENSIONS

This tab displays all file extensions recognized by SecureSchool.

- **Red entries** are extensions currently blocked for the selected filter set.
- **Green entries** are extensions that have been saved for possible blocking in the future.
- **Gray entries** may be automatically managed by SecureSchool's **Task Center** options and cannot be changed here.

Administrators can:

- **Click to Block Extension** to prevent files of that type from being accessed.
- **Click to Unblock Extension** to allow access.
- **Delete** an extension from the list if it was manually added but is no longer needed.

Examples of commonly blocked file types include:

- **.exe** – Executable programs
- **.bat** – Batch files
- **.scr** – Screensaver executables
- **.vbs** – VBScript files
- **.mpg/.mp3** – Streaming media files (when restricted by policy)

This helps prevent users from downloading malicious software or accessing streaming services that consume excessive bandwidth.

ADD AN EXTENSION

Administrators may also manually add new file extensions to block.

Steps:

1. Navigate to the **Add An Extension** tab.
2. Enter the **file extension** (e.g., .xyz).
3. Provide a brief **description** (e.g., "Custom file type").
4. Select which **Filter Set(s)** the rule should apply to (e.g., Students, Staff).
5. Click **Submit** to save the rule.

The new extension will appear in the **List Extensions** tab and can be managed like other entries.

BEST PRACTICE:

Block executable and script file types (e.g., .exe, .bat, .cmd, .vbs) to reduce security risks. Consider also blocking high-bandwidth media formats if streaming is not permitted in your environment.

URL FILTERING

The **URL Filtering** feature allows administrators to control web access based on specific words, phrases, prefixes, or suffixes found in website addresses. Like all Content Filtering tools, this feature requires the **Advanced SSL Intercept Add-on** to be effective.

🔻 Overview
URL Filtering works by scanning the text of a web page's address (the URL). If the URL contains a word or pattern that matches a filtering rule, SecureSchool will block or allow the page accordingly.

A URL WORD is defined as any text between common URL delimiters such as . - \ ? + = / or a number. For example:

- https://example.com/ad/banner.jpg → the words include EXAMPLE, COM, AD, and BANNER.JPG.

TABS AND FUNCTIONS

CHOOSE RULE LISTS

- Administrators can enable pre-defined URL rule lists sorted by category (e.g., Advertising, Pornography, Proxy, Social Networking).
- These lists are automatically updated by K12USA to keep up with changes on the internet.
- To enable a rule list, check the box next to it and click **Save Changes**.
- Certain lists may also activate automatically when related features (e.g., Search Control, Anti-Proxy Center, Anti-Social Networking Center) are turned on.

VIEW RULE LISTS

- Displays the active URL filtering rules in the selected list.
- Rules are read-only but show how specific terms trigger filtering.

VIEW PREFIXES AND SUFFIXES

- Administrators can view lists of common prefixes (beginning portions of URLs) and suffixes (endings of URLs) that are used within each rule list.
- Example: The ADVERTISING list may include suffixes like .adserver.

HOW IT WORKS

- Explains the matching logic:
    1. **Exact Match** → matches only the standalone word.
    2. **Contains** → matches if the string appears anywhere in the URL.
    3. **Begins With** → matches if the URL starts with the string.
    4. **Ends With** → matches if the URL ends with the string.
- SecureSchool can also combine prefixes and suffixes with Exact Match conditions to reduce false positives.

EXAMPLE USE CASES

- Block all sites containing proxy in their URL to prevent circumvention.
- Allow only .edu domains while blocking general commercial sites.
- Prevent access to ad-tracking networks by enabling the Advertising rule list.

MIME FILTERING

MIME Filtering allows administrators to block or allow specific file types based on their **MIME type identifiers**. MIME types describe the nature and format of a file (for example, audio/mp3 for MP3 files or application/pdf for PDF documents). Blocking at this level gives administrators more control over what types of files can be accessed, downloaded, or streamed.

Important: Content Filtering features, including MIME Filtering, only function when the **Advanced SSL Intercept Add-On** is enabled.

ACCESSING MIME FILTERING

Navigate to:
Content Filtering → MIME Filtering

Two tabs are available:

- **List MIME Types** – View and manage existing MIME type rules.
- **Add a MIME Type** – Add a new MIME type to the block list.

LIST MIME TYPES

The **List MIME Types** page displays all MIME types currently available to SecureSchool for the selected Filter Set.

- **Entries in Red** → MIME types that are currently blocked.
- **Entries in Green** → MIME types available but not blocked.
- **Entries in Dark Red** → MIME types blocked by global Task Center settings (cannot be changed from this page).

ACTIONS AVAILABLE:

- **Click to Block MIME Type** → Blocks the MIME type for the selected Filter Set.
- **Click to Unblock MIME Type** → Removes the block, allowing access.
- **Block Already Enforced** → Indicates that the MIME type is blocked globally and cannot be modified locally.

Example uses:

- Block streaming media types (e.g., video/mp4, audio/mpeg) to conserve bandwidth.
- Block executables (e.g., application/x-msdownload) to reduce malware risks.

ADD A MIME TYPE

To create a new block rule:

1. Go to the **Add a MIME Type** tab.
2. Enter the **MIME Type** (e.g., application/zip).
3. Enter a **Description** (optional, for easier identification).
4. Select whether to **block this MIME type across all filter sets** or only for the current Filter Set.

5. Click **Submit** to apply.

📌 RECOMMENDED BEST PRACTICES FOR BLOCKING

To maximize security and conserve bandwidth, administrators often block the following categories of MIME types:

SECURITY RISK TYPES (EXECUTABLES & SCRIPTS)

- application/x-msdownload → Windows executables (.exe files)
- application/x-sh → Shell scripts
- application/x-bat → Batch files
- application/x-jar → Java archives

COMPRESSED/ARCHIVE FORMATS (CAN HIDE MALWARE)

- application/zip
- application/x-rar-compressed
- application/x-7z-compressed
- application/x-iso9660-image

STREAMING & MEDIA FORMATS (BANDWIDTH-HEAVY)

- video/mp4, video/x-ms-wmv, video/quicktime
- audio/mpeg, audio/x-wav, audio/x-ms-wma
- application/vnd.rn-realmedia

📌 NOTE: Blocking common document types such as application/pdf or application/msword is not recommended unless you have a specific policy reason, as these are widely used in education.

EMBEDDED VIDEO

The **Embedded Video** section allows administrators to control whether users can access web pages containing embedded videos from specific providers. This feature helps schools manage bandwidth and ensure that inappropriate or non-educational video sources are blocked.

When a page contains an embedded video from a blocked provider, SecureSchool will automatically prevent the page from loading and display a message to the end user explaining that the content was blocked due to an embedded video restriction.

HOW IT WORKS

- SecureSchool maintains a list of popular embedded video providers (e.g., YouTube, Vimeo, Dailymotion, MySpace).
- Administrators can **select or deselect providers** from the list to control which embedded videos are allowed.
- The system applies these settings at the filter-set level, allowing for flexibility between student, staff, and guest groups.

MAKING CHANGES

1. Navigate to **Content Filtering → Embedded Video**.
2. Choose the appropriate **Filter Set** from the drop-down menu.
3. Use the checkboxes to **block or allow specific video providers**.
4. Click **Save Changes** to apply your selections.

BEST PRACTICES

- **Block by Default**: Consider blocking all but a handful of educational or trusted providers to minimize distractions.
- **Pair with Streaming Media Controls**: For broader video control, use the **Anti-Streaming Media Center** and **Block Embedded Video** options together.
- **Review Periodically**: Providers can change over time; review your allowed list to ensure it continues to meet school policies.

TROUBLESHOOTING

- If users report that an educational page won't load, check whether the page contains an embedded video from a blocked provider.
- Encourage staff to whitelist educational platforms via the **Allowed Websites** list if needed.

FIREWALL

PROTOCOL RULES

🕮 OVERVIEW

Protocol Rules define which protocols are allowed or blocked for a given Filter Set. By default, SecureSchool includes rules to block outdated or insecure services such as instant messaging applications (e.g., AOL, MSN, Yahoo Messenger). Administrators may also add their own rules to manage protocols according to school policies.

📌 **Note:** Custom Protocol Rules can only be created or managed by the K12USA Tech Team.

⍰ MANAGING PROTOCOL RULES

VIEWING RULES

- Navigate to **Firewall > Protocol Rules > List Rules**.
- A table displays all active rules, including:
  - **Rule Name**
  - **Type** (Allow or Deny)
  - **Protocol** (TCP, UDP, etc.)
  - **Source/Destination Address and Port**
  - **Filter Set Applied**
  - **Actions** (Deactivate or Delete)

ADDING A RULE

- Click **Add a Rule**.
- Enter the following details:
  - **Rule Name**: A descriptive label (e.g., "Block POP3 Email").
  - **Reason**: Required field to document why the rule was created.
  - **Type**: Select *Allow* or *Deny*.
  - **Protocol**: Choose from available options (e.g., TCP, UDP).
  - **Arriving Through**: Specify *All Inside Interfaces* or another option.
  - **Source/Destination Address**: Enter IP addresses, CIDR ranges, hostnames, or use a Filter Set.
  - **Destination Port**: Define the service port(s) (e.g., 80 for HTTP, 443 for HTTPS).
- Click **Add Protocol Rule** to save.

Editing or Removing RuleS

- Rules may be **Deactivated** temporarily without deletion.
- To remove a rule permanently, click **Delete**.

⍰ BEST PRACTICES

- **Block legacy services**: Disable instant messengers and outdated protocols to prevent misuse.

- **Be specific**: Apply rules to particular Filter Sets (e.g., Staff vs. Students) rather than globally, unless absolutely necessary.
- **Document changes**: Always provide a clear *Reason* when adding or modifying rules for accountability.
- **Test before rollout**: Apply new rules during low-traffic hours to avoid disruptions.

FIREWALL: PORT FORWARDING

The **Port Forwarding** section allows administrators to map external ports on the SecureSchool firewall to internal IP addresses and services within the school's network. This is often used to provide secure access to internal services such as CCTV systems, HVAC controllers, or remote desktop services.

OVERVIEW

Port Forwarding ensures that specific types of incoming traffic from the Internet are directed to the appropriate internal server or device. Each rule includes:

- **Name** – Descriptive label for the service.
- **Inside IP Address** – The internal device receiving the traffic.
- **Outside IP Address** – The external-facing address of the SecureSchool firewall.
- **Ports** – The internal and external port numbers used.
- **Protocol** – TCP, UDP, or both.

MANAGING PORT FORWARDING

VIEWING RULES

- Navigate to **Firewall > Port Forwarding > List Forwarded Ports**.
- The table displays all configured rules, including service name, internal/external IP addresses, port numbers, and protocol type.

ADDING A RULE

- Click **Add Forwarded Ports**.
- Enter the following details:
  - **Name**: A descriptive identifier (e.g., "CCTV").
  - **Inside IP Address**: Internal address of the device/service.
  - **Outside IP Address**: Public-facing IP of the firewall.
  - **Port(s)**: Internal and external ports to be mapped (e.g., 80, 443, 3389).
  - **Protocol**: Select TCP, UDP, or both.
- Click **Add Forwarded Port** to save.

EDITING OR DELETING RULES

- Click on a rule to edit its details.
- To remove a rule, click **Delete** in the Actions column.

📌 IMPORTANT NOTES

- **Security Risk**: Opening unnecessary ports can expose internal services to outside threats. Only forward ports that are required.
- **Use VPN Instead**: Whenever possible, use VPN services such as SecureSchool's WireGuard instead of direct port forwarding.
- **Limit Access**: If forwarding is required, restrict the rule to specific external IP addresses instead of allowing all traffic.
- **Audit Regularly**: Review forwarding rules periodically to ensure they're still necessary and properly secured.

BEST PRACTICE

Use port forwarding sparingly.
Whenever possible, rely on SecureSchool's **WireGuard VPN** or other secure remote-access solutions instead of exposing internal services directly to the Internet. This greatly reduces the risk of unauthorized access and potential security breaches.

ADDRESS FORWARDING

The **Address Forwarding** feature allows administrators to forward traffic from an external (outside) IP address directly to an internal (inside) IP address. This is useful when you need a specific device inside your network (such as a server) to appear on the Internet with its own public IP.

ACCESSING ADDRESS FORWARDING

1. From the left-hand navigation menu, go to:
   Firewall > Address Forwarding.
2. Two tabs are available:
   - **List Addresses** – Displays all existing forwarded IP addresses.
   - **Add Forwarded IP Address** – Allows you to create a new forwarding rule.

ADDING A FORWARDED IP ADDRESS

1. Select the **Add Forwarded IP Address** tab.
2. Fill out the form:
   - **Name** – A label to identify why this forwarding rule is set up (e.g., *Mail Server*).
   - **Inside IP Address** – The internal IP address of the device you are forwarding to (e.g., 192.168.0.10).
   - **Outside IP Address** – Select the public IP address from the drop-down list that will be mapped to the inside device.
   - **Notes** – (Optional) Add descriptive notes for future reference.
3. Click **Submit** to save the forwarding rule.

VIEWING AND MANAGING FORWARDED IP ADDRESSES

1. Go to the **List Addresses** tab.
2. A table displays all configured forwarding rules, including:
   - **Name**
   - **Inside IP Address**
   - **Outside IP Address**
3. To modify a rule:
   - Click on the IP address entry to edit.
   - Use the **Delete** link next to an entry to remove it.

BEST PRACTICES FOR ADDRESS FORWARDING

- **Use only when necessary** – Forwarding exposes an internal device directly to the Internet, so limit its use to services that absolutely require it (e.g., mail server, VPN gateway).
- **Restrict access with firewall rules** – Combine address forwarding with **Protocol Rules** to allow only the specific traffic and ports required.
- **Assign static internal IPs** – Ensure the inside device always has the same IP address (via static assignment or DHCP reservation) to avoid broken forwarding rules.
- **Document your rules** – Use the **Name** and **Notes** fields to record the purpose of each forwarding entry for future administrators.
- **Review regularly** – Periodically check the **List Addresses** tab and remove unused or outdated forwarding entries.
- **Combine with security layers** – Always pair forwarding with proper device hardening (e.g., strong passwords, up-to-date patches, intrusion detection where possible).

DMZ RULES

The **DMZ Rules** page controls traffic entering and leaving the Demilitarized Zone (DMZ). A DMZ is typically used for servers that must be accessible from the Internet (such as mail, web, or FTP servers) while remaining logically separated from your internal network.

DMZ Rules allow you to permit or deny specific traffic between the DMZ and other networks based on customizable criteria.

ACCESSING DMZ RULES

1. From the left-hand navigation menu, go to:
   Firewall > DMZ Rules.
2. Two tabs are available:
   - **List Rules** – Displays all current active and inactive DMZ rules.
   - **Add A Rule** – Create a new DMZ rule.

VIEWING DMZ RULES

On the **List Rules** tab, rules are displayed in two sections:

- **Active Rules** – Rules currently in effect.
- **Inactive Rules** – Rules that are defined but not active.

Each rule includes:

- **Sequence Number (Seq)** – Determines rule order (lower numbers have higher priority).
- **Protocol Rule Name** – The name of the rule.
- **Type** – Allow or Deny.
- **Protocol** – Such as TCP, UDP, or both.
- **Source Address / Source Port** – Defines the origin of the traffic.
- **Destination Address / Destination Port** – Defines the target of the traffic.
- **Arriving Through** – Specifies the direction of traffic (Two Way or From DMZ).
- **Actions** – Options to **Activate** or **Delete** the rule.

ADDING A DMZ RULE

1. Open the **Add A Rule** tab.
2. Fill out the form:
   - **Rule Name** – A descriptive label for the rule.
   - **Reason** – A short explanation of why the rule is being added (required).
   - **Type** – Select **Allow** or **Deny**.
   - **Protocol** – Choose TCP, UDP, or both.
   - **Arriving Through** – Select whether the traffic is Two Way, From DMZ, or To DMZ.
   - **Remote Address** – The external address or network (can be a single IP, range in CIDR, hostname, filter set, or firewall table).
   - **Remote Port** – The source port(s) if applicable.
   - **Local Address** – The internal address of the DMZ device.

- **Local Port** – The destination port(s) for the traffic.
- **Sequence Number** – Normally set automatically, but may be adjusted to control rule order (1–999). Lower numbers take precedence.

3. Click **Add DMZ Rule** to save.

BEST PRACTICES FOR DMZ RULES

- **Use the principle of least privilege** – Only allow the traffic that is absolutely necessary for the DMZ service.
- **Start with Deny by Default** – The final rules in the list should block all traffic except what you've explicitly allowed.
- **Be specific with ports and addresses** – Avoid using "Any" unless absolutely required. This reduces potential exposure.
- **Document your rules** – Use the **Rule Name** and **Reason** fields to clearly describe why the rule exists.
- **Review regularly** – Periodically audit DMZ rules to remove outdated or unused entries.
- **Combine with monitoring** – Enable packet logging for troubleshooting or when testing a new DMZ service.
- **Sequence carefully** – Remember that rules with lower sequence numbers override higher ones. Place critical Allow/Deny rules at the correct priority.

ADVANCED FIREWALL MANAGEMENT (K12USA TECH TEAM ONLY)

The following sections in the SecureSchool firewall interface are reserved for use by the **K12USA technical team only**. While you may be able to view existing entries, changes to these settings should never be made by school administrators.

These rules are highly advanced and affect core system operations. Incorrect adjustments could cause Internet outages, security issues, or service disruptions.

PRE-NATD MANAGEMENT (K12USA TECH TEAM ONLY)

The **Pre-Natd Management** section handles firewall rules before Network Address Translation (NAT) takes place. These rules can influence how traffic is filtered or redirected at the most fundamental level of the firewall.

- **Purpose:** Advanced troubleshooting, traffic shaping, or special routing scenarios.
- **Managed By:** K12USA tech team only.

NATD MANAGEMENT (K12USA TECH TEAM ONLY)

The **Natd Management** section defines how certain types of traffic are diverted or rewritten through NAT processing.

- **Purpose:** Specialized traffic handling for NAT-dependent services.
- **Managed By:** K12USA tech team only.

PRE-USER MANAGEMENT (K12USA TECH TEAM ONLY)

The **Pre-User Management** section applies firewall rules before user authentication or filtering policies are enforced. These are critical baseline rules that ensure stable and secure Internet access.

- **Purpose:** Establish system-wide traffic rules prior to user-level controls.
- **Managed By:** K12USA tech team only.

TRAFFIC WEIGHTING (K12USA TECH TEAM ONLY)

The **Traffic Weighting** section allows prioritization of specific protocols or traffic types, ensuring that critical services are not disrupted by heavy network usage.

- **Purpose:** Assign priority (weight) to traffic, such as VoIP or critical services.
- **Managed By:** K12USA tech team only.

 Reminder: These advanced firewall tools are fully supported and maintained by K12USA. No administrator action is required.

FIREWALL TABLES

The **Firewall Tables** feature provides a way to group related IP addresses, domains, or services together. Instead of entering the same addresses repeatedly across multiple firewall rules, administrators can reference a **table**. This makes rules easier to manage and reduces errors.

For example, instead of listing every mail server IP address in multiple rules, you can create a **MailServers** table and then reference that table wherever it's needed.

ACCESSING FIREWALL TABLES

1. From the left-hand navigation menu, go to:
   Firewall > Firewall Tables.
2. Two tabs are available:
   - **Manage Tables** – Create and manage the overall firewall tables.
   - **Manage Table Entries** – View and manage the entries within a specific table.

MANAGING TABLES

On the **Manage Tables** tab, you'll see a list of available firewall tables. Each table has:

- **Name** – The identifier used in firewall rules.
- **Description** – A brief explanation of what the table contains.
- **Actions** – Options to **View Table Entries** or **Manage Table Entries**.

Examples of common tables include:

- **AllowOutsideProxy** – Defines which proxies are allowed outside connections.
- **BlockedWorkstations** – Groups machines that should be denied access.
- **InternalServers** – Contains local IP exceptions.
- **MailServers** – Lists outside mail servers.
- **NTServers** – Contains public NTP servers.
- **ProxyExceptions** – Defines exceptions to proxy rules.

MANAGING TABLE ENTRIES

On the **Manage Table Entries** tab, you can drill down into any specific firewall table.

Each entry includes:

- **Name** – A label for the entry (e.g., Gmail, AOL, Office365).
- **Type** – Indicates how the entry is defined (e.g., DNS or IP).
- **Value** – The domain or IP address associated with the entry (e.g., imap.gmail.com, smtp.office365.com).
- **Actions** – Options to **Activate** or **Deactivate** an entry (note that many entries cannot be edited or deleted).

Example:
In the **MailServers** table, entries might include Gmail, AOL, Outlook, and Office365 mail server addresses. These can be activated or deactivated depending on the school's requirements.

COMMON USE CASES

- **Mail Servers** – Control which external mail services (e.g., Gmail, AOL, Office365) can be accessed.
- **NTP Servers** – Ensure devices use only approved time servers for synchronization.
- **Proxy Exceptions** – Allow traffic to bypass proxy filtering for specific services.
- **Internal Servers** – Define exceptions for school-hosted servers that need direct communication.
- **Blocked Workstations** – Centralize a list of machines denied Internet access.

BEST PRACTICES FOR FIREWALL TABLES

- **Use tables for consistency** – Tables ensure the same list of addresses is applied across multiple firewall rules.
- **Review regularly** – Periodically check for outdated entries (e.g., old mail server domains).
- **Do not modify reserved entries** – Many core tables (e.g., Private, ProxyExceptions) are system-critical and should not be changed.
- **Use activation/deactivation** – Instead of deleting entries, deactivate them. This preserves history and makes it easy to re-enable later.
- **Contact support if unsure** – If you are uncertain about adding or modifying entries, reach out to the K12USA Support Team for guidance.

Tip: Firewall Tables are especially useful when working with services that may change IP addresses frequently (such as cloud mail providers). Using domain-based DNS entries within a table ensures your rules stay up-to-date.

USER AUTH

USER GROUPS

The **User Groups** section allows administrators to organize users into permission-based groups. Each group can be assigned a **filter set** and customized access permissions, making it easier to manage how different roles interact with the SecureSchool system.

VIEWING GROUPS

When you open **User Groups**, you'll see a list of existing groups. Each group entry includes:

- **Group Name** – The label for the group (e.g., Administrators, Moderators, Users).
- **Filter Set** – The content filtering rules applied to that group.
- **Users** – Number of assigned users.
- **Actions** – Options to:
  - **Edit Permissions** – Adjust what system sections and functions the group can access.
  - **Delete** – Remove the group entirely.

📌 **Note:** Clicking a group name opens its permission settings.

EDITING GROUP PERMISSIONS

Permissions define what features users in that group may access.
From the **Edit Permissions** screen, you can assign access to:

- **SecureSchool Interface Sections** (e.g., Setup, Task Center, Network Trakker, Website Filtering, Content Filtering, Firewall, Logs & Reports, VPN Services).
- **System Functions** such as restarting services (DHCP, DNS, Firewall, SSL Proxy, Wireguard, etc.).
- **Commit/Restart** – Required if you want the group's changes to take effect.
- **Reboot Options** – Full system reboot or service restarts.

 Important:
Granting a group access to configuration pages without also enabling **Commit/Restart** prevents their changes from being applied. Always pair interface access with the ability to commit when appropriate.

ADDING A NEW GROUP

1. Go to **User Groups > Add a Group**.
2. Enter a **Group Name** (e.g., Teachers, Students, IT Staff).
3. Select a **Filter Set** from the dropdown (e.g., Administrators, Staff, Students).
4. Click **Submit**.

Once created, you can assign users to the group and edit its permissions.

COMMON USE CASES

- **Administrators** – Full access to all SecureSchool sections and restart privileges.
- **Moderators/IT Staff** – Limited system access, often restricted to monitoring and troubleshooting functions.
- **Users/Students** – Assigned basic filter sets, typically without system permissions.
- **Custom Groups** – Create specialized groups (e.g., Teachers with fewer restrictions, Testing Accounts with temporary access).

IP GROUPS

The **IP Groups** section allows administrators to manage workstation IP addresses and ranges. These groups determine how devices on the network are filtered and whether they require authentication. IP Groups are especially useful for shared devices or labs where individual login credentials aren't practical.

LISTING WORKSTATION IPS

The **List Workstation IP(s)** tab displays all configured IPs and their group assignments. Each entry shows:

- **Name** – Descriptive label for the device or range (e.g., LAN, Staff, Student Lab).
- **IP or IP Range** – The assigned IP address or block.
- **IP Group Name** – The group this IP belongs to.
- **Transparent** – Indicates whether the group bypasses login/authentication.
- **Filter Set Name** – The filter set applied to that group.
- **Actions** – Options to:
    - View access status.
    - Delete the IP/range from the list.

Green Rows: Active IPs with access enabled.
Red Rows: Reserved IPs saved for future inclusion.

ADDING A WORKSTATION IP

To add an IP or range that bypasses authentication:

1. Go to **Add a Workstation IP**.
2. Enter the **IP Address or Range**. Examples:
    - Single: 192.168.0.1
    - Subnet: 192.168.0.1/24
    - Range: 192.168.0.1-192.168.0.12
3. Enter a **Name** for the entry (e.g., "Library PCs").
4. Select an **IP Group** from the dropdown.
5. Click **Submit**.

LISTING IP GROUPS

The **List IP Groups** tab shows all available groups with:

- **IP Group Name** – The label (e.g., Staff, Students).
- **Filter Set** – Defines the content filtering rules.
- **Transparent** – Yes/No indicating whether login is required.
- **Action** – Option to delete the group.

ADDING AN IP GROUP

To create a new IP Group:

1. Go to **Add an IP Group**.
2. Select a **Filter Set** (Administrators, Staff, Students).
3. Enter a **Group Name**.
4. Set **Transparent** to Yes/No.
    - **Yes** = Devices bypass login and are automatically placed in the assigned filter set.
    - **No** = Devices require user login.
5. Click **Submit**.

Tip: Transparent IP Groups are commonly used for shared wireless devices such as iPads or Chromebooks.

COMMON USE CASES

- **Administrators** – Direct IP assignment for IT staff machines, with full permissions and no login prompts.
- **Staff** – Staff workstations grouped by subnet, applying a staff filter set.
- **Students** – Student lab computers or classroom devices requiring login.
- **Transparent Groups** – Used for mobile devices or shared labs to bypass login while still applying proper filters.

USERS

The **Users** section is most commonly used to create and manage accounts that provide **access to SecureSchool's web-based controls**. Each account is tied to a **User Group** and inherits its assigned **Filter Set**.

This section is also used in environments where **SSB Authentication** is enabled. In that setup, each user logs in once per browser session with their username and password, and SecureSchool applies filtering based on their group membership.

LIST USERS

The **List Users** tab shows all existing accounts. Each row includes:

- **User** – First and last name.
- **Username** – Login name for SecureSchool.
- **Group** – The user's assigned group (e.g., Students, Staff).
- **Filter Set** – The filter rules applied to that group.
- **Proxy Access** – Indicates if proxy authentication is enabled for that user.
- **Graduation Year** – Useful for managing student accounts (e.g., bulk cleanup by graduating class).
- **Email Address** – Optional contact field.
- **Actions** – Delete option (except for the default **admin** account, which cannot be removed).

A search and filtering bar lets you quickly narrow results by user type or graduation year.

ADD A USER

To create a new user:

1. Go to **Add A User**.
2. Enter the following fields:
    - **First Name / Last Name**
    - **Username** (used for login)
    - **Password** (automatically generated; shown briefly after creation)
    - **Graduation Year** (for student accounts)
    - **Uses Proxy Authentication** (check if this user logs in through the proxy)
    - **Let User Set Their Own Password** (optional; applies on first login)
    - **Group** (assign to an existing user group)
    - **Email Address** (optional)
3. Click **Add User**.

📌 **Note:** After adding a user, changes in group membership or filtering may take up to **15 minutes** to take effect. To apply them immediately, restart Auth on the **Commit Changes** page.

EDITING A USER

Click a user's name to open the **Edit User** screen. From here, you can:

- Update name, username, and password.
- Change graduation year.
- Toggle proxy authentication.
- Reassign the user to a different group.
- Add a **Yubikey** for two-factor authentication.

BULK IMPORT OF USERS

For schools with large numbers of accounts, **K12USA can bulk import users** directly into SecureSchool.

- Admins should email the file to **support@k12usa.com**.
- The file must include **username, password, and group membership** details.
- Credentials are securely stored in the SecureSchool appliance.

This method is recommended for initial setup or yearly student rollovers.

UNFILTERED PROXY USERS

The **Unfiltered Proxy Users** section allows administrators to temporarily bypass web filtering for specific accounts. This can be useful for devices or services that require unrestricted Internet access (e.g., servers, postage machines, or certain administrative tasks).

⚠ **Important CIPA & E-Rate Compliance Notice:**
Disabling filtering may put your school out of compliance with the Children's Internet Protection Act (CIPA). Schools participating in the **E-Rate program** must ensure that all Internet-connected computers have filtering enabled. Bypassing filtering should be done sparingly and only when necessary. Failure to comply may result in repayment of E-Rate funds.

LIST UNFILTERED USERS

The **List Unfiltered Users** tab displays all accounts currently exempted from filtering. Each entry includes:

- **Username** – The account name.
- **Exception Until** – The expiration date when filtering will be restored automatically.
- **Action** – Delete option (removes the exemption immediately).
- **Reason** – Notes for why the exemption was created (e.g., "Postage Machine," "HP Server Access").

ADD AN UNFILTERED USER

To add a new exception:

1. Go to **Add An Unfiltered User**.
2. Enter the **Username** (must already exist in the Users list).
3. Select an **Expiration Date** when the exemption will end.
4. Provide a **Reason** for documentation (recommended for accountability).
5. Click **Submit**.

Tip: Always use a reasonable expiration date. Long-term unfiltered accounts increase compliance risks.

EDITING AN UNFILTERED USER

Click on a username to change the details of an existing exemption:

- Update the **expiration date**.
- Modify the **reason** for the exemption.
- Click **Save Changes** to apply updates.

COMMON USE CASES

- **Postage machines** – Some require full Internet access for updates.
- **Network devices** – For example, printers or servers that cannot operate correctly under filtering.
- **Temporary administrative testing** – When staff need short-term access to unrestricted Internet for troubleshooting.

BEST PRACTICES

- **Always set an expiration date** — Never leave accounts permanently unfiltered.
- **Document the reason** — Helps track why exceptions were made and by whom.
- **Review exemptions regularly** — Remove outdated entries to reduce risk.
- **Use only when necessary** — Keep filtering enabled for nearly all accounts to maintain CIPA compliance.

FILTER SETS

Filter Sets define the Internet filtering rules applied to users and devices in SecureSchool. Each set can be linked to one or more **User Groups** or **IP Groups**, and may include moderators who review unblock requests.

VIEW FILTER SETS

The **View Filter Sets** tab shows all existing filter sets. Each entry includes:

- **Filter Set Name** – The label for the set (e.g., Administrators, Staff, Students).
- **People in this filter set are** – Indicates which group of users the filter applies to.
- **Applies to** – Lists the User Groups or IP Groups using this filter set.
- **Special Filtering** – Identifies if the set applies to exceptions (e.g., Proxy Authentication sites).
- **Moderators** – Displays moderators assigned to handle unblock requests.
- **Actions** – Options to edit or remove moderators.

📌 **Note:** You cannot delete a filter set if it is associated with a User Group, IP Group, or set as a system default.

ADD A FILTER SET

To create a new filter set:

1. Go to **Add a Filter Set**.
2. Enter a **Filter Set Name**. (Letters, numbers, and underscores only.)
3. Choose whether to copy settings from an existing set or start with defaults.
4. Select the type of people the filter applies to (e.g., Staff, Students).
5. Click **Submit**.

ADD A MODERATOR TO A FILTER SET

Moderators are users who can review and approve or deny unblock requests. To add one:

1. Go to **Add a Moderator to a Filter Set**.
2. Enter the moderator's **username**.
3. Select the filter set the moderator will oversee.
4. Click **Submit**.

CUSTOMIZE BLOCK MESSAGE

When users attempt to access blocked sites, they see a customizable block page. To edit:

1. Go to **Customize Block Message**.
2. Select the filter set you want to modify.
3. Customize options such as:
    - School logo and organization name.
    - Link to the school's **Acceptable Use Policy (AUP)**.
    - Display of moderator email addresses.
    - Request access form fields (email, reason).
    - Custom message text.
4. Preview changes and click **Save Changes**.

The block page can be tailored to include school branding and instructions for requesting site access.

COMMON USE CASES

- **SSB_Administrators** – Assigned to IT staff or administrators who require full or nearly unrestricted access.
- **SSB_Staff** – Applies to teachers and staff, with moderate filtering.
- **SSB_Students** – Applies to students, usually the most restrictive filter set.
- **Custom Sets** – Schools may create additional sets for groups like Testing Devices, Guests, or Special Programs.

PORTAL

The **Portal** feature manages authenticated web sessions for SecureSchool users. It provides a centralized way to view and control active logins and allows administrators to configure portal behavior.

LIST PORTALS

The **List Portals** tab displays all currently active portal sessions. Each entry includes:

- **Username** – The authenticated user's login name.
- **IP Address** – The IP associated with the session.
- **Filter Set** – The filtering rules applied to the user.
- **Started** – The time the session began.
- **Expiration** – When the session will automatically expire.
- **Action** – Options to:
    - **Put User in Group** – Assign the user to a specific group during their session.
    - **Disconnect** – End the user's session immediately.

A search box allows you to quickly find a specific user or IP. You can also export the session list to **CSV** for recordkeeping.

CONFIGURE PORTAL

The **Configure Portal** tab defines how the portal behaves after login:

- **Show the logout button after a successful login** – Displays a logout option for users.
- **Redirect the user to a URL after successful login** – Optionally send users to a specific website (e.g., the school homepage) after logging in.

Enter the desired **Redirect URL** and click **Save Changes** to apply.

SESSION EXPIRATION

Portal sessions automatically expire after a set amount of time. Once expired, the user must reauthenticate to continue browsing. This ensures secure session management and prevents indefinite access.

COMMON USE CASES

- Monitoring active authenticated sessions in real time.
- Disconnecting unauthorized users quickly.
- Redirecting staff or students to a school resources page after login.
- Temporarily reassigning a user to a different group during testing or troubleshooting.

RADIUS AUTH

The **Radius Auth** section is used to configure and manage RADIUS authentication servers within SecureSchool. This allows for centralized authentication of users, particularly useful in wireless environments.

📌 **Note:** Radius Auth is only available to customers who subscribe to the **Universal Wireless Support add-on**.

VIEW RADIUS SERVERS

The main screen lists all configured RADIUS servers. Each entry shows:

- **Name** – The descriptive label of the server.
- **Authentication Type** – The method used for authentication.
- **Server Info** – The IP address or details of the configured server.
- **Actions** – Options to manage or remove the server.

If no servers are defined, the list will be empty.

ADD A RADIUS SERVER

To add a new RADIUS server:

1. Click **Add a new Radius Server**.
2. Enter a **Name** (used for identification within SecureSchool).
3. Choose an **Authentication Type**:
    - **Active Directory** – Authenticate against your AD domain. (NOTE: SECURESCHOOL MUST FIRST BE JOINED TO YOUR ACTIVE DIRECTORY DOMAIN.)
    - **WirelessTrakker Auth** – Uses the WirelessTrakker controller for authentication.
    - **Remote SecureSchool Database** – Authenticate against a different SecureSchool appliance.
    - **Google LDAP** – Integrates with Google directory services.
4. Enter the **IP address of the remote SecureSchool box** or authentication server. (Example: 192.168.0.1)
5. Click **Add Radius Server** to save.

COMMON USE CASES

- **Wireless Network Authentication** – Provide secure login for wireless users.
- **Active Directory Integration** – Reuse existing staff and student credentials.
- **Multi-Site Authentication** – Centralize authentication across district appliances.
- **Google Directory Environments** – Authenticate using Google Workspace LDAP.

BEST PRACTICES

- **Document configuration details** – Keep a record of server names, IPs, and authentication types for quick reference.
- **Test after setup** – Always verify authentication by connecting a test user before rolling out to the entire network.
- **Use redundancy wisely** – Configure backup servers only as needed to avoid unnecessary complexity.

- **Secure communication** – Ensure firewall rules and encryption settings protect communication between SecureSchool and the RADIUS server.
- **Monitor logs** – Regularly review authentication logs for failures or anomalies.

🛠TROUBLESHOOTING TIPS

- **Authentication failing for all users?** Check that the SecureSchool appliance is properly joined to the Active Directory domain.
- **Only some users can't log in?** Verify group membership and ensure the correct filter set is mapped.
- **Server unreachable?** Confirm the RADIUS server's IP is correct and firewall rules allow communication.
- **Timeouts or intermittent failures?** Review network stability and ensure there's no duplicate IP conflict.
- **Google LDAP issues?** Double-check credentials and directory synchronization settings.

LOGS & REPORTS

GRAPHS

The **Graphs** section provides real-time and historical visualizations of your SecureSchool appliance's network performance. These charts help administrators quickly spot usage patterns, detect issues, and confirm overall health.

OPTIONS AVAILABLE

- **Full Net** – Displays bandwidth usage for outside and inside network interfaces.
- **Latency & Loss** – Monitors connection stability and packet loss to key destinations.

You can adjust the timeframe displayed using quick-select buttons at the top (e.g., **1 hour**, **3 hours**, **24 hours**, **7 days**, **month**, **quarter**, **year**).

FULL NET GRAPHS

These graphs show **bandwidth usage** across interfaces:

- **Outside Interfaces** – Internet-facing traffic (upload/download to your ISP).
- **Inside Interfaces** – Internal traffic between SecureSchool and your local network.

Each set includes:

- **Average Bandwidth (left graph)** – Smooths usage over time to show overall traffic trends.
- **Max Bandwidth (right graph)** – Highlights peak usage at each interval, useful for spotting spikes.

How to Read:

- **Green** = Outbound traffic (upload).
- **Blue** = Inbound traffic (download).
- **Y-axis** = Bandwidth in kilobits/megabits per second (Kbps/Mbps).
- **X-axis** = Timeline for the selected period.

☞ Example: If the blue (download) spikes near the top of the graph during school hours, it may indicate streaming or high student usage.

LATENCY & LOSS GRAPHS

These graphs measure **connection stability and responsiveness**:

- **Latency to Gateways** – Shows response times (in milliseconds) to your default internet gateways.
- **Latency to External Sites** – Tracks stability to external sites such as K12USA.com (and optionally, customer-chosen test sites).

How to Read:

- **Green line** = Median latency (normal response time).
- **Black/Grey shading** = Variability or spikes in latency.
- **Red marks** = Packet loss (missed responses).

☞ Example: A steady green line at ~30ms with no red marks means your connection is healthy. If latency spikes above 100ms or red loss indicators appear, you may have ISP or routing issues.

PRACTICAL USES

- Detect high bandwidth usage during specific hours.
- Identify when network slowdowns occur (e.g., large spikes in download traffic).
- Monitor ISP stability by checking for packet loss or latency spikes.
- Validate if reported outages match historical data.

BEST PRACTICES FOR GRAPH ANALYSIS

- **Check both Average and Max graphs together** – Average shows trends; Max exposes short-lived spikes.
- **Correlate with the time of day** – If spikes align with student arrival or lunch, it's likely normal usage. If they appear overnight, investigate further.
- **Look for consistent patterns** – Repeated daily peaks are normal. Random, sharp spikes may indicate misconfigured devices or abuse.
- **Use Latency & Loss to confirm ISP issues** – If packet loss shows across multiple sites, the issue may be with your ISP. If it only affects one site, it may be that site's server.
- **Compare Inside vs. Outside interfaces** – If Inside usage is high but Outside is low, traffic may be staying internal (e.g., file sharing, local servers).

REPORTS & STATISTICS

The **Reports & Statistics** section provides detailed logs and summaries of web activity, bandwidth use, and workstation traffic. These tools help administrators analyze usage trends, identify heavy consumers of bandwidth, and generate reports for compliance or troubleshooting.

FILTER REPORTS

The **Filter** tab allows you to generate detailed reports for a specific date. You can select from a wide variety of report types, such as:

- IP Addresses by Size or Hits
- Top-Level Domains (TLD) by Hits
- Most Blocked or Most Denied IPs
- Users by Size or Hits
- MIME Types (file types) by Size or Hits

☞ Example: Running "Most Blocked IP Addresses" can help you identify misbehaving devices or compromised systems attempting repeated access.

EMAIL NIGHTLY REPORTS

This feature lets you configure **automatic nightly emails** with summary reports.

- Choose from Top 10 IPs, TLDs, or Users.
- Enter one or more administrator email addresses.
- Reports are delivered automatically, saving time and providing daily insight without manual checks.

SUMMARY REPORTS

The **Summary** tab shows monthly breakdowns with both **daily averages** and **monthly totals**.

- Columns include Hits, Files, Pages, Visits, and Sites.
- Graphs at the top provide quick visualization.

☞ Use this to spot overall long-term usage trends and seasonal patterns (e.g., higher activity during the school year vs. breaks).

DAILY REPORTS

The **Daily** tab provides charts by day, broken down by month and year.

- Useful for identifying peak traffic days.
- Can help correlate events (e.g., testing days, assemblies) with spikes or drops in usage.

HOURLY REPORTS

The **Hourly** tab drills down into usage per hour for a given month.

- Ideal for spotting bandwidth spikes during class changes, lunch, or other predictable times.
- Helps distinguish normal usage patterns from abnormal after-hours traffic.

WORKSTATIONS

This tab reports activity per **workstation (IP address)**.

- Includes files requested, MB of traffic, and individual sessions.
- Can help track a specific device if it is suspected of unusual usage.

WEBSITES

The **Websites** tab provides a list of visited websites, including:

- Website address (domain or URL).
- Number of Hits.
- MB of Traffic consumed.

☞ Example: If a workstation shows unusually high usage, check this tab to see which websites are responsible.

BEST PRACTICES FOR REPORTS & STATISTICS

- **Schedule nightly reports** for quick daily insight without manual checks.
- **Use Filter reports** to drill into suspicious traffic, such as repeated blocks or high-bandwidth users.
- **Compare Daily and Hourly views** to spot both long-term patterns and short-term spikes.
- **Check Workstations before Users** – often an IP-level view is more reliable if usernames are shared or cached.
- **Review Websites tab regularly** to detect inappropriate or unexpected browsing trends.

FILTER LOG

The **Filter Log** provides detailed records of all web activity filtered through SecureSchool. Administrators can use it to review blocked or successful requests, troubleshoot user complaints, and ensure that filtering policies are being applied correctly.

VIEWING LOGS

From the Filter Log screen, you can select how much data to review:

- **For a whole day** – Shows all entries for the selected day.
- **For a particular time** – Narrow down to a specific time window.
- **Across several days** – Useful for spotting recurring issues.

Click **Generate View** to display results.

SEARCH & FILTER OPTIONS

You can refine log views using one or more criteria:

- **Username** – View traffic by user (if user authentication is enabled).
- **IP Address** – View traffic tied to a specific workstation.
- **Website Address** – Search by full or partial URL.
- **Filter Set** – Narrow results by the policy set applied.

Additional options let you exclude certain file types (images, JavaScript, CSS) or unfiltered websites from your search.

LOG CATEGORIES

BLOCKED LOG MESSAGES

These entries indicate that SecureSchool blocked access. Common reasons include:

- Blocked due to **IP or blanket restrictions**.
- Access to **non-allowed websites** only.
- **Banned phrases, file extensions, or MIME types** detected.
- **Banned Websites** (explicitly blacklisted).
- **Weighted Words and Phrases** threshold exceeded.
- **Port or PICS filter** violations.

Blocked entries appear highlighted, often with the reason shown (e.g., “Banned Website: youtube.com”).

SUCCESSFUL LOG MESSAGES

These entries show traffic that was allowed:

- Access granted because the site was on the **Allowed Websites list**.

- Access allowed for an **exception user** or **exception IP**.
- Access allowed because no filter rules were triggered.

READING FILTER LOG ENTRIES

Each log line typically includes:

- **Time** – When the request occurred.
- **Proxy User** – Username (if available).
- **Filter Set** – Which policy applied.
- **Workstation IP** – Device making the request.
- **Status** – Blocked or allowed (with the reason).
- **Mime Type** – Content type (e.g., text/html, image/jpeg).
- **Website Address** – The full URL requested.

BEST PRACTICES FOR FILTER LOGS

- **Check the Status column first** to quickly determine if a request was blocked or allowed.
- **Search by IP address** if usernames are unclear or unavailable.
- **Filter by time window** to investigate complaints ("I couldn't access Google Docs at 10:30 AM").
- **Download logs as a tab-delimited file** for offline review or long-term record keeping.
- **Use exclusions** (images, scripts, etc.) to reduce noise in searches and focus on relevant web traffic.

COMMON SCENARIOS & HOW TO INVESTIGATE

1. Student reports that YouTube is blocked, but it should be allowed.

- Search by **username** or **IP address**.
- Look for entries with Status = **Banned Website: youtube.com**.
- If blocked, confirm whether YouTube is on the **Allowed Websites list** for their Filter Set.

2. Teacher says a site won't load, but it's not in the banned list.

- Search by **website address**.
- Check if it was blocked for another reason (e.g., MIME type, phrase filter, or port block).
- If it's safe, add the domain to the **Allowed Websites list**.

3. Bandwidth seems slow during class.

- Use Filter Log with **summary of websites visited**.
- Look for heavy traffic sites (e.g., streaming services, downloads).
- Combine with Reports & Statistics for top users or sites.

4. Student bypassing filters using proxies or VPNs.

- Search logs for **uncommon domains** or high volume of random IPs.
- Check if Status shows **Blocked Port** or unfamiliar SSL tunnels.
- Add these sites or IPs to the **Banned Websites or IP groups**.

5. Parent or administrator requests proof of filtering.

- Generate a **tab-delimited export** for the requested date.
- Provide blocked/allowed entries showing how SecureSchool applied rules.

ACTIVITY LOG

The **Activity Log** records all user and system actions within SecureSchool. It is an essential tool for tracking administrative activity, troubleshooting changes, and maintaining accountability.

When an administrator accesses reports, modifies filter settings, or views system logs, those actions are automatically recorded in the Activity Log with a **timestamp, page accessed, and user account**.

VIEWING OPTIONS

The Activity Log can be filtered to display specific information:

- **Show Session** – Groups activity entries into user login sessions.
- **Show Remote Address** – Displays the IP address from which the user accessed SecureSchool.
- **Show Referrer** – Shows the previous page before the action was taken.
- **Show Get/Post Values** – Displays additional technical details about requests.
- **Show Oldest Activity First** – Reverses order so that the earliest entries appear first.
- **Show Activity Log Accesses** – Includes entries where administrators view the Activity Log itself.
- **Show Traffic Graph Accesses** – Includes entries for viewing Graphs.
- **Show Summary** – Provides a condensed view of activity instead of detailed line items.

You can also:

- **Filter by User** – Useful when multiple administrators manage SecureSchool.
- **Jump to Time** – Quickly navigate to a specific date and time to review activity.

USE CASES

- **Accountability** – Verify who made configuration changes (e.g., updated Filter Sets).
- **Troubleshooting** – Track recent admin actions before an issue began.
- **Audit Trail** – Maintain a history of administrative access for compliance.

📌 **Note:** The Activity Log is very detailed and can grow quickly. Use filters and time ranges to narrow down to relevant entries when troubleshooting.

TOOLS & TESTS 🛠

The **Tools & Tests** menu provides administrators with diagnostic and monitoring utilities for troubleshooting network performance, firewall behavior, and connectivity. These tools help confirm whether network issues are local, external, or related to SecureSchool configurations.

TOOLS

The **Tools** subsection includes a suite of network utilities accessible directly within the SecureSchool interface. These are helpful for administrators who want to quickly test connectivity without needing command-line access to another machine.

Available options include:

- PING – Sends ICMP echo requests to test connectivity and response times to a host.
- FROMA – Performs an outbound ping test from the appliance's perspective to verify external connectivity.
- TRACEROUTE / MTRACEROUTE – Traces the path packets take to a destination, identifying potential bottlenecks or dropped hops.
- PACKET CAPTURE – Captures live network traffic for detailed troubleshooting.
- TRAFFIC SAMPL**e** – Provides a snapshot of network traffic activity.
- ARP-SCAN – Lists devices on the local subnet by scanning for active ARP entries.
- WHOIS – Queries domain registration information.
- DNS / DNSTRACE – Resolves hostnames or traces DNS resolution paths.
- CIDR CALCULATOR – Assists in subnet calculations for IP addressing.
- PHONE HOME – Reports status information back to K12USA support.
- SUBNETS – Displays subnetting information for your network.

FIREWALL

The **Firewall** section provides access to live firewall rule activity and logs. It includes:

- **Stats** – Displays hit counts for firewall rules, showing which rules are most active.
- **Zero** – Resets firewall counters.
- **Full Log** – Shows detailed firewall logging activity.
- **Accept Log / Deny Log** – Displays entries for allowed or blocked traffic.
- **Count Log** – Summarizes firewall traffic by rule.

This view is especially useful for verifying whether traffic is being blocked due to firewall policy or external network issues.

STATUS

The **Status** section provides detailed information about SecureSchool's interfaces and routing. Tabs include:

- **Interface Setup** – Displays IP addresses, netmasks, and link status for each network interface.
- **Interface Stats** – Monitors traffic statistics on each interface.
- **Routes** – Lists active routing table entries.
- **Date/Time** – Displays and manages system time.
- **ARP / Flush ARP** – Displays ARP table entries and allows cache resets.
- **Network Accounting** – Provides per-interface traffic statistics.

This section is commonly used when diagnosing physical or configuration-related connectivity issues.

NETWORK SPEED TESTS

SecureSchool includes built-in **LAN** and **WAN** speed tests:

- **LAN Test** – Measures speed between your browser and the SecureSchool appliance.
- **WAN Test** – Measures internet speed between the SecureSchool appliance and the wider internet.

These tests help determine whether slowness originates inside the local network or from the internet connection.

CONNECTION MONITORING

The **Connection Monitoring** tool allows administrators to continuously monitor the availability of internal and external resources.

- Sites (IP addresses or hostnames) can be added to the monitoring list.
- Each entry can be toggled **On** or **Off** for monitoring.
- Results are color-coded:
    - **Green** = Online and responding.
    - **Red** = Offline or unreachable.

Typical uses include:

- Monitoring the school's internet gateway.
- Verifying uptime for critical internal servers.
- Watching external services (e.g., VoIP providers, web portals).

ACTIVE DIRECTORY

SecureSchool can integrate directly with your school's Active Directory (AD) domain, allowing seamless authentication and filter assignment based on existing user accounts and groups.

JOIN ACTIVE DIRECTORY

To connect SecureSchool to your AD domain:

1. Navigate to **Tools & Tests > Active Directory**.
2. Under the **Join Active Directory** tab, complete the following fields:
    - **Domain Specific Name Server**: Choose the DNS server associated with your domain.
    - **NetBIOS Domain Name**: Enter the short domain name (e.g., HSD).
    - **NetBIOS Name for this Appliance**: Assign a unique identifier for SecureSchool (e.g., SECURESCHOOL).
    - **Domain Admin Username**: The username of a domain administrator.
    - **Domain Admin Password**: The corresponding password.
3. Click **Join Active Directory**.

Once successful, you'll see confirmation that the appliance is joined to your AD domain.

 Important: To disconnect, click **Disconnect from Active Directory**. Doing so will remove the appliance from the domain.

GROUP MEMBERSHIP

This tab allows you to assign AD groups to SecureSchool filter sets.

- Enter the **username** of the account.
- Changes may take up to 15 minutes to apply.
- To apply changes immediately, restart authentication under **Commit/Restart > Auth**.

GROUP LIST

The **Group List** tab displays all groups retrieved from Active Directory.

- Groups without spaces in their names can be directly mapped to filter sets.
- Examples:
    - staff
    - students
    - tech-support

STATUS

The **Status** tab shows diagnostic information about the AD connection, including:

- Domain join confirmation
- LDAP server details

- SecureSchool's registered service principal names (SPNs)
- Trust verification results

This page is useful for troubleshooting when authentication issues occur.

BEST PRACTICE:

Always verify the SecureSchool appliance time is synchronized with your domain controller. A time mismatch can cause authentication failures.

VPN SERVICES

WIREGUARD SERVER

The **WireGuard Server** feature in SecureSchool allows administrators to configure secure, high-performance VPN connections for both individual clients (e.g., staff working from home) and site-to-site links between school networks.

WireGuard is included with the VPN Services module and provides a simple, modern alternative to traditional VPN solutions.

POOL SETTINGS

The **Pool Settings** tab is where administrators configure the base WireGuard server settings.

- **Use WireGuard** – Enables the WireGuard service.
- **IP Pool** – Defines the subnet range available for VPN clients. The recommended format is a /24 network (e.g., 192.168.230.0/24) to support up to 253 client addresses.
- **Listen Port** – Specifies the port WireGuard listens on. A common value is 51820.
- **Allowed IP Cache** – Lists permitted network ranges. This helps ensure VPN clients only access the intended school resources. Example values include:
    - 192.168.10.0/24
    - 192.168.12.0/24
- **Public/Private Keys** – Generated automatically by the system. These keys are used for secure cryptographic exchange.

Click **Save Configuration** after making changes.

CLIENT MANAGEMENT

The **Client Management** tab provides tools for creating and managing individual VPN clients.

- **Add a New Client** – Create a new WireGuard client profile. Each device (laptop, phone, tablet) requires its own unique client entry.
- **Client List** – Displays all configured clients, along with connection statistics. Columns include:
    - **Client Name** – Friendly label for the client (e.g., “John’s Laptop”).
    - **Client #** – Unique identifier.
    - **Endpoint** – The client’s current IP if connected.
    - **Latest Handshake** – Shows the last time the client communicated with the server.
    - **Received / Sent** – Traffic counters.
    - **Status** – Indicates whether the client is enabled.
    - **Actions** – Options to download the client configuration, display a QR code (for easy mobile setup), or delete the client.

SITE MANAGEMENT

The **Site Management** tab allows administrators to configure site-to-site VPN tunnels.

- **Add a New Site** – Adds a remote site to connect securely to the main network.
- **Site List** – Displays configured sites with details including:
  - **Site Name** – Label for the remote site.
  - **Remote IPs** – IP ranges accessible over the VPN.
  - **Endpoint** – IP of the remote site's WireGuard gateway.
  - **Latest Handshake** – Last successful communication.
  - **Received / Sent** – Data usage.
  - **Actions** – Download the site configuration or delete the entry.

This feature is useful for connecting multiple school buildings securely over the internet.

ACTIVITY

The **Activity** tab provides a real-time view of WireGuard tunnel usage and peer status.

- Displays the server's interface, public key, and listening port.
- Lists all connected peers (clients or sites), along with:
  - **Endpoint** – The peer's external IP.
  - **Allowed IPs** – Subnets accessible by that peer.
  - **Latest Handshake** – Confirms the peer is active and communicating.
  - **Transfer Statistics** – Tracks the amount of data sent/received.

This section helps administrators verify VPN health and troubleshoot connectivity.

⍰ COMMON USE CASES

- **Remote Work** – Allow staff or IT administrators to securely access school resources from home.
- **Site-to-Site VPN** – Connect multiple campuses or administrative offices to share resources seamlessly.
- **Secure Management** – Provide encrypted access for remote system monitoring and updates.

WIREGUARD CLIENT

The **WireGuard Client** feature allows your SecureSchool appliance to connect *outbound* to another WireGuard server. This is typically used when your school network needs to connect securely to a remote site, data center, or hosted resource that is already running a WireGuard VPN server.

Unlike the **WireGuard Server**, which allows remote devices to connect *into* your school's network, the Client mode makes SecureSchool act as a VPN endpoint that initiates connections outward.

CLIENT SETTINGS

- **Use WireGuard Client** – Enables the WireGuard Client feature on your appliance.
- **Save Configuration** – Always click this button after enabling or disabling the feature to apply your changes.

📌 *Note: Simply enabling the client does not establish a VPN. You must configure at least one connection under* ***Connection Management*** *before it can be used.*

CONNECTION MANAGEMENT

Here you can add and manage VPN connections to remote WireGuard servers.

- **Create a New Connection** – Starts the process of entering connection details (e.g., server endpoint, public key, allowed IPs).
- **Connection List** – Displays all defined VPN connections. At this stage, no connections are shown until configured.

Each connection typically requires:

- **Remote Server Address** – The IP or hostname of the WireGuard server you are connecting to.
- **Remote Public Key** – The public key of the server for authentication.
- **Allowed IPs** – Defines what traffic should pass through the VPN tunnel.
- **Local Keys** – Automatically generated by SecureSchool when you create the connection.

BEST PRACTICES

- Use **WireGuard Server** for staff/student remote access into the school, and **WireGuard Client** only for site-to-site or outbound tunnels.
- Document each connection's purpose clearly to avoid confusion between multiple tunnels.
- Test connectivity after saving a new connection by verifying traffic routes properly through the VPN.
- Avoid overlapping IP ranges between your local network and the remote site's subnets.

SCHOOL-TO-SCHOOL VPN

The **School-to-School VPN** feature allows two or more SecureSchool appliances to connect securely over the internet, creating an encrypted tunnel between locations. This is often used by districts with multiple campuses, allowing internal resources to be shared as if they were on the same local network.

SETTINGS OVERVIEW

SITES

- Displays all configured remote sites.
- Each entry includes:
  - **Site Name** – Friendly identifier for the remote location.
  - **User Name** – The authentication user for the VPN connection.
  - **Remote Networks** – Lists IP addresses and subnet masks that define which traffic should pass through the VPN tunnel.
  - **Actions** – Options to EDIT or DELETE the site configuration.
- You can add new sites with the **Add a new Site…** link.

ACTIVE CONNECTIONS

- Shows currently active VPN tunnels between configured school sites.
- VPN connections will automatically attempt to reconnect if disconnected.
- To permanently disable a connection:
  1. Disable VPN privileges for the user.
  2. Disconnect the tunnel.

CONFIGURE

- Defines core tunnel parameters:
  - **Tunnel Address** – A private, non-routable address used for the VPN tunnel itself (e.g., 172.29.230.0).
  - **Netmask** – Typically set to 255.255.255.0.
  - **Port** – The port used for VPN traffic (commonly 1195).
  - **Management** – Localhost management address/port for the service.
- Once set, these values generally remain unchanged.

CERTIFICATE

- Displays the **VPN certificate** required for secure communication between sites.
- This certificate must be installed on participating sites to authenticate and encrypt traffic.

BEST PRACTICES

- **Plan Subnets Carefully**
  Avoid overlapping subnets between sites. Assign distinct IP ranges to each campus before configuring tunnels.
- **Document Connections**
  Keep a record of all configured sites, including IP ranges, site names, and assigned tunnel addresses.
- **Monitor Active Tunnels**
  Regularly check the **Active Connections** tab to confirm tunnels are up and stable.
- **Use Strong Certificates**
  Ensure certificates are unique per site and periodically review expiration dates.

TROUBLESHOOTING TIPS

- **Tunnel Not Establishing**
  - Verify both ends are using the correct tunnel address and subnet mask.
  - Ensure the configured port is not blocked by upstream firewalls.
- **Frequent Disconnects**
  - Check for unstable internet connections at either site.
  - Review **Active Connections** for auto-reconnect behavior.
- **Routing Issues**
  - Confirm that traffic destined for remote networks is correctly included in the **Remote Networks** configuration.
  - Avoid IP conflicts between local and remote subnets.
- **Certificate Errors**
  - Ensure the correct certificate is installed at each site.
  - If the certificate is corrupted or expired, regenerate and reinstall.

IPSEC/STRONGSWAN CONFIG

The **IPSEC/Strongswan Config** page allows administrators to enable and configure an IPSEC VPN service using Strongswan. This feature is considered **experimental/alpha** and should only be used with the guidance of K12USA Support. While SecureSchool primarily supports WireGuard and legacy OpenVPN options, Strongswan is available for advanced users who may require IPSEC compatibility.

CONFIGURATION OPTIONS

- **Use Strongswan/IPSEC**
  - Check this box to enable the Strongswan/IPSEC feature.
- **Config File**
  - Enter the full contents of your Strongswan configuration file.
  - This defines how the IPSEC tunnel should be established, including authentication methods, endpoints, and encryption settings.
- **Secrets File**
  - Enter the full contents of the secrets file.
  - Typically includes pre-shared keys (PSKs), certificates, or other credentials required to establish the tunnel.

IMPORTANT NOTES

- **Experimental Feature** – This option is not widely used among K12USA clients. If you are interested in using it, please contact K12USA Support for assistance.
- **Preferred Alternatives** – In most cases, **WireGuard Server** (for site-to-site and remote access) is the recommended solution due to its simplicity and performance.
- **Advanced Use Case** – Strongswan may be useful when connecting to third-party networks or legacy systems that require IPSEC for compliance or interoperability.

BEST PRACTICES

- **Test in a Lab First** – Before deploying Strongswan in production, test your configuration in a controlled environment.
- **Secure Secrets** – Never share or store the secrets file insecurely, as it contains sensitive credentials.
- **Monitor Stability** – Because this feature is experimental, monitor logs and connection stability closely after enabling it

COMMIT/RESTART

The **Commit/Restart** section manages the application of changes made throughout the SecureSchool system. Many configuration adjustments—such as updates to firewall rules, filter sets, or authentication settings—require a service restart before they take effect.

SecureSchool automatically selects the services that need restarting based on the changes you make, but administrators can also manually restart services as needed.

HOW IT WORKS

- **Pending Commits**:
  When changes are saved but not yet applied, SecureSchool lists the affected services in the **Commit/Restart** section.
  - You'll see a yellow notification banner stating: *"There are changes that need to be committed!"*
  - Services requiring a restart will be highlighted.
- **Automatic Selection**:
  SecureSchool determines which services need restarting based on the specific configuration changes (e.g., Firewall, Filter Sets, Cache Server).
- **Manual Restarts**:
  Administrators can choose to restart individual services directly from this section without making additional changes.

COMMON SCENARIOS

- **Website Whitelisting/Blacklisting**:
  Adding or changing site permissions in Website Filtering requires a commit/restart of the Firewall, Filter Set(s), and sometimes the Authentication and Cache services.
- **Firewall Updates**:
  Modifying firewall tables, rules, or NAT policies requires a firewall service restart.
- **Authentication Changes**:
  Updating user groups, Active Directory links, or related policies requires the **Authentication Server** to restart.

BEST PRACTICES

- **Plan Ahead**: Restarting certain services may briefly interrupt internet usage for end-users (e.g., Firewall: ~15 seconds, SSL Proxy: ~1 minute). Schedule changes during low-traffic periods when possible.
- **Review Carefully**: Always verify which services are listed for restart before committing changes.
- **Batch Changes**: If making multiple updates (e.g., adding firewall rules and modifying filter sets), apply them together to reduce restart frequency.
- **Manual Restarts**: Use manual restarts to troubleshoot or refresh a service without needing to make configuration changes.

EXAMPLE WORKFLOW

Add a website to the **Whitelist** in Website Filtering.
SecureSchool automatically marks the **Firewall**, **Filter Set**, and **Cache Server** for restart.
Navigate to **Commit/Restart** → review the services listed.
Click **Restart Selected Services**.
Services restart, and your changes take effect.

Tip: You don't need to restart SecureSchool itself—only the individual services affected by the changes.

SHUTDOWN/REBOOT

The **Shutdown/Reboot** section provides administrators with the ability to power down or restart the SecureSchool appliance. While these options are available, **reboots should be approached with caution**.

WHY CAUTION IS IMPORTANT

- **Log Data Loss**:
  Certain logs are cleared upon reboot. This can erase valuable information that our support team needs to diagnose issues such as DNS attacks, misconfigurations, or abnormal traffic patterns.
- **Misdiagnosis Risk**:
  Problems like slow internet speeds are often symptoms of underlying issues (e.g., DNS attacks, overloaded filter sets, or network misconfigurations). Rebooting may temporarily mask the issue but prevent proper troubleshooting.
- **Support First**:
  Our tech team can remotely view logs in real time. This allows them to pinpoint the cause of the problem without losing critical diagnostic information.

OPTIONS AVAILABLE

- REBOOT APPLIANCE
  Restarts the SecureSchool appliance while keeping power on.
  - Use only if directed by K12USA Support.
  - Brief downtime will occur while services restart.
- SHUTDOWN APPLIANCE
  Powers down the SecureSchool appliance.
  - Use this option only when physically moving, servicing, or retiring the device.

BEST PRACTICES

- **Call Support First**: Always contact K12USA Support (877-225-0100) before rebooting. In many cases, problems can be fixed remotely without needing a restart.
- **Avoid "Quick Fix" Reboots**: Do not reboot SecureSchool as the first step in troubleshooting slow internet or connection issues.
- **Use Reboots Strategically**: Only reboot when advised by support staff or when applying hardware-related maintenance.

BEFORE YOU REBOOT…

- ☐ Confirm that the issue cannot be resolved another way.
- ☐ Call K12USA Support (877-225-0100) so logs can be reviewed in real time.
- ☐ Only proceed with a reboot or shutdown if directed by support staff.
- ☐ Do **not** reboot as a first step for slowness or connectivity problems.

LOGOUT 👋

The **Logout** option allows administrators to securely exit the SecureSchool interface. This helps prevent unauthorized access to the appliance if a session is left unattended.

When you click **Logout** from the navigation menu, you are immediately redirected to the **Login screen**. From here, you must re-enter your administrator credentials (username and password) to access the system again.

🔻 Example Login Screens
The login page typically displays:

- The **school name** and SecureSchool branding.
- Fields for **Username** and **Password**.
- A **Login to SecureSchool** button.
- Links to the WirelessTrakker login (if applicable).
- A quick overview of optional services (e.g., PowerTrakker, SSL Intercept, School-to-School VPN).
- Date and time, along with K12USA contact information.

BEST PRACTICE
Always use the **Logout** button when finishing your session, rather than just closing the browser window. This ensures your session is terminated properly and helps protect system security.