



School/Organisation

Name

Date

This checklist contains two sections:

- Appliance: Specific steps to check in your On-Premise Appliance
- Appliance and Cloud Portal: Steps to check in Cloud Portal, On-Premise Appliance or both, depending on your setup

If you require additional help completing the checklist, [contact Smoothwall Support](#).

Appliance

*Mark the action as "Not Applicable" (N/A) if a checklist item doesn't apply.

#	Action	Description	Done*	Notes
1	Check your Certificates .	Go to System > Certificates > Certificates for Services . Check the expiry date on your: • Default Certificate Authority. • Dynamic Certificates. If one or both will expire in September, renew them before students return.		
2	Update your On-Premise Appliance .	Go to System > Maintenance > Updates & releases . Update to the latest version and release available to you.		
3	Schedule regular backups.	Go to System > Maintenance > Archives . • Schedule backups or create them manually. • Set Prune archives to a value other than Don't prune.		

Smoothwall Appliance and Cloud Portal Start of Year Maintenance Checklist



4	Optimise log settings.	Reduce over-logging to clear up disk space.		
5	Check that services are working.	Sign in to the Smoothwall Appliance to view the Dashboard : - Green tick: The service is working as expected. - Grey: You don't use this feature. - Red cross: Contact Smoothwall Support.		
6	Add new IP addresses to your interfaces.	If your internal network has changed: Update internal interfaces with the new IP addresses from Network > Configuration > Interfaces. Add or edit a Web Proxy authentication policy to use the new interfaces from Web Proxy > Authentication > Manage policies.		
7	Add any new IP address ranges to Tenants.	Go to System > Administration > Tenants and update tenants with any new Subnet information .		
8	Check your third-party Firewall.	If you use a third-party Firewall, ensure you: Allow these domains. Prevent QUIC access. - Allow outbound DNS, HTTP and HTTPS (UDP/TCP 53, TCP 80 and TCP 443).		
9	Check your System Alerts .	Go to Reports > Settings > Output Settings . Ensure alerts are sent to the correct Distribution Groups .		
10	Check the System time .	Go to System > Preferences > Time . To prevent issues with Authentication and directories: - Ensure your Appliance's time is correct. - Update the details for new Servers or Network Interfaces on the Time page.		
11	Update Domains in DNS forwarders .	Go to Network > Configuration > DNS . If you made network or infrastructure changes, update conditional DNS forwarders with new IP addresses or domains.		



Appliance and Cloud Portal

*Mark the action as "Not Applicable" (N/A) if a checklist item doesn't apply.

#	Action	Description	Done*	Notes
1	Confirm network and appliance connectivity.	Ensure all network and infrastructure appliances are on and connected to your systems and the internet.		
2	Update email addresses.	If your email domains have changed, update email addresses across all your systems before the old ones expire to prevent users from losing access.		
3	Check access for all administrators and users.	If staffing has changed or more access is required, add users in: • Cloud Portal. • On-Premise Appliance.		
4	Install Smoothwall software on new devices .	Deploy Cloud Filter Extension, Android Filter App or Smoothwall Browser to all new devices.		
5	Check your Safeguarding Alerts .	Ensure Safeguarding Alerts are sent to the correct people: • On-Premise Appliance: Check and update the users in your Distribution group from Reports > Safeguarding > Notifications. • Cloud Filter: Add or update email addresses in the Contacts field from Filter > Safeguarding.		
6	Prevent 'Double Filtering' .	Go to Guardian > Client interfaces > Cloud Filter . If you use a Hybrid setup, segregate devices or turn on the 'Secret Knock'.		

Smoothwall Appliance and Cloud Portal Start of Year Maintenance Checklist



7	Update your Directories.	If you made changes to your Directory groups, remap your User Groups. • Update any group-based Web Filter policies. • In Appliance > Services > Authentication > Directories, check that your directories show green ticks. If red crosses show, fix the issues or contact Smoothwall Support.		
8	Ensure only required services are connected.	Only connect the Smoothwall Appliance or Cloud Filter to networks that require filtering or firewall protection. For example, don't connect networks used by cashless catering, door access, boiler control, building management, CCTV, or sign-in systems.		
9	Test your Web Filter policies.	Use a staff or student device to test access to blocked or allowed content and to check the Filter Mode. If content is allowed or blocked incorrectly: • Check your Web Filter policies. • Check HTTPS inspection settings. • Use the Real Time Log Viewer to identify the website so you know what to block or allow in your Web Filter policies. • For On-Premise Appliance, check the application's documentation to block or allow ports using Firewall rules.		