



Start-of-Year Maintenance Checklist

School / District

Name

Date

*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 and check the expiry date of your: • Default Certificate Authority. • Dynamic Certificates. If either expires at the start of the school year, renew them before students return.		
2	Update your On-Premise Appliance.	Go to System > Maintenance > Updates & releases. Update to the latest version for the latest security updates, fixes, performance improvements, and features. See the steps for updating to Maiden and Newport.		



Start-of-Year Maintenance Checklist

#	Action	Description	Done*	Notes
3	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 check marks.		
4	Update IDex directory.	Clear IDex data and perform a full sync to ensure group memberships are up to date. - Go to Services > Authentication > Settings - Select Clear IDex Directory. - Run 'sendaddatanow.exe' on your Active Directory server at C:\ProgramFiles\Smoothwall\IDexAgent\SendAdDataNow.exe.		
5	Schedule regular backups.	Go to System > Maintenance > Archives to schedule backups or create them manually . Set Prune archives to a value other than Don't prune .		
6	Optimise log settings.	Reduce over-logging to clear up disk space.		
7	Check that services are working.	Sign in to the Smoothwall Appliance to view the Dashboard: Green checkmark: The service is working as expected. Grey: You don't use this feature. Red cross: Contact Smoothwall Support.		



Start-of-Year Maintenance Checklist

#	Action	Description	Done*	Notes
8	Add new IP addresses to your interfaces.	If your internal network has changed: 1. Update internal interfaces with the new IP addresses from Network > Configuration > Interfaces . 2. Add or edit your Web Proxy authentication policy to use the new interfaces from Web Proxy > Authentication > Manage policies .		
9	Add any new IP address ranges to Tenants.	Go to System > Administration > Tenants and update tenants with any new Subnet information .		
10	Check your third-party Firewall.	If you use a third-party Firewall, ensure you allow access to these domains and block QUIC access . Allow outbound DNS, HTTP and HTTPS (UDP/TCP 53, TCP 80 and TCP 443).		
11	Check your System Alerts .	Go to Reports > Settings > Output Settings and ensure alerts are sent to the correct Distribution Groups .		



Start-of-Year Maintenance Checklist

#	Action	Description	Done*	Notes
12	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.		
13	Update Domains in DNS forwarders.	Go to Network > Configuration > DNS and update the conditional DNS forwarders with the new IP addresses or domains if you previously made any network or infrastructure changes.		
14	Confirm network and appliance connectivity.	Ensure all network and infrastructure appliances are on and connected to your systems and the internet.		
15	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.		
16	Check access for all administrators and users.	If staffing has changed or additional access is required, add users in the Cloud Portal and the On-Premise Appliance .		



Start-of-Year Maintenance Checklist

#	Action	Description	Done*	Notes
17	Install Smoothwall software on new devices.	Deploy Cloud Filter Extension, Android Filter App or Smoothwall Browser to all new devices.		
18	Check your Safeguarding Alerts.	Ensure Safeguarding Alerts are sent to the correct people: • On-Premise Appliance: Check the users in your Distribution group from Reports > Safeguarding > Notifications. • Cloud Filter: Update email addresses in the Contacts field from Filter > Safeguarding.		
19	Prevent Double Filtering.	If you use a Hybrid setup , go to Guardian > Client interfaces > Cloud Filter and either segregate devices or turn on the 'Secret Knock'.		
20	Ensure only required services are connected.	Only connect the Smoothwall Appliance or Cloud Filter to networks that need 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.		



Start-of-Year Maintenance Checklist

#	Action	Description	Done*	Notes
21	Verify web filtering and policies	Check access to blocked or allowed content and Filter Mode. • Test staff and students' devices through testfiltering.com to confirm basic blocks and HTTPS inspections are working. • Check your Web Filter policies and use the Real Time Log Viewer for websites to block or allow in your policies. • For On-Premise Appliance, block or allow ports using Firewall rules. • Check that user identification and group-specific policies are working as expected by ensuring sites restricted to students remain accessible to staff.		