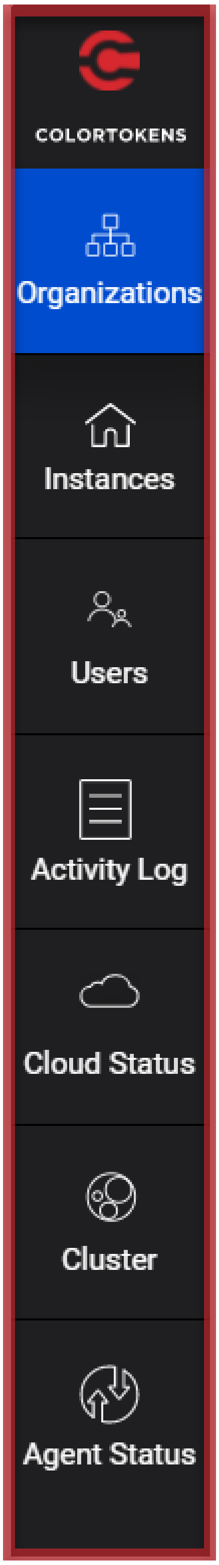

Release Notes

Xshield, Xaccess

2022 Release R4, Version 8.11.0.41

What’s Included

About the products

Xshield

Xshield Core is a cloud-delivered micro-segmentation solution based on a Zero Trust platform that secures corporates' critical assets, including applications and workloads. The infrastructure-agnostic platform simplifies and accelerates the enterprise journey to hybrid environments, driving full cloud adoption with a Zero Trust security model. It deploys seamlessly and enables enterprises to visualize and define secure micro-segment boundaries (micro-perimeters) for their application workloads.

Xaccess

Xaccess is a Zero Trust Network Access (ZTNA) platform that provides customers a secure Zero Trust remote access to employees, third parties and contractors while accessing cloud or datacenter-based applications. Xaccess allows customers to define intelligent and user identity-based access while handling more common and complex use cases such as enabling remote IT admins with deeper access specifications or session-based access needed for multi-user terminals. Its AI-based access engine dynamically autogenerates access policies based on risk, usage, and disruption metrics. Xaccess is easy to deploy, and it operates with no infrastructure or architecture constraints, no network or firewall configuration changes. It provides seamless On-Network and Off-Network user onboarding experience. It comes with built-in integrations for multiple identity providers for authentication and single sign-on.

What’s New in Xshield and Xaccess

New capabilities in Xshield:

- Users can configure the host firewall using Xshield, without deleting their locally defined firewall rules. This setting is applicable at a group level. Multiple stakeholders can control the host firewall when this feature is enabled.
- Xshield now allows users to select the appropriate firewall profile that should be applied to a workload. This is useful when a customer would like to select the application of micro-segmentation only for a subset of flows accessing the application. This feature is supported only on newer Windows platforms (Windows 2008 and above).
- The product will now enable multiple users to edit their policies simultaneously and apply them independently - allowing for a faster deployment especially when the number of workloads are large.

New capabilities in Xaccess:

- Customers can enable debug-level logging on user devices (where agents are deployed) through the Zero Trust Security Platform. These logs also are uploaded on to the platform without requiring any customer (or their user) intervention. This is very useful for troubleshooting user devices that are not able to access their desired applications.

Resolved Issues

The following issues are resolved:

Bug ID	Description
Xshield	
CTSP-25094	Colortokens agent does not update policy version properly when an agent moves from the enforced to the observed state.
CTSP-24875	Unable to download the log from the log download option only for Windows 2003 assets
CTSP-24825	Policy version is not properly updated when the state changes from the enforced to the observed mode.
CTSP-24762	Colortokens agent should add default rules to allow communication to proxy server. This will avoid manual configuration of such rules by the user.
CTSP-24756	Incorrect Policy was being pushed to resources while moving back from the enforced to the observed mode.
CTSP-24580	The agent version displayed in secure user access prompt does not match with the version displayed in the dashboard.
CTSP-24507	The workload page takes a long time to load data when the page level is set to 100.
CTSP-24487	Data does not refresh when a user navigates to a different tab under the traffic option of the workload group.
CTSP-25082	Public API to update groups is not working as expected. It fails with the 400 response code.
CTSP-24484	The accept and ignore policy options are always active even if the user did not select any of the recommended policies.
CTSP-24479	The horizontal scroll bar in the traffic tab of the workload group is not working properly.
CTSP-24413	The CPU and Memory usage information of a particular asset is not displayed on the assets page. This happened while the asset was upgraded from the 8.10.2.5 to the 8.10.2.6 agent version.
CTSP-24368	When a server is in the enforced state in the outbound direction, the inbound rules created manually get deleted when the server is restarted. This causes service disruptions.
CTSP-24253	The network discovery and file sharing options get disabled on the Windows 2008 server. This happens when the server is moved to the enforced state and the Windows firewall is enabled.
CTSP-24240	Flows are marked as unauthorized/blocked even when a policy is defined.
CTSP-24183	Colortokens agent attempts to communicate with some of the Xaccess domains even when Xaccess is not enabled.
CTSP-24179	Unable to turn off the Xaccess tunnel from the asset page of the Security platform. This issue is observed on Windows 11.
CTSP-23948	Unable to launch a tenant in a Colortokens cluster. It throws the “504 Gateway timeout” error.
CTSP-23812	Workloads running Citrix applications crash in the enforced mode. The issue does not occur in observed mode.
CTSP-22830	Groups created with a public API have incorrection policy action. The flow explorer logs show policy status as unauthorized even when the policy is applied.
Xaccess	

Bug ID	Description
CTSP-21202	The decommissioned asset’s hostname and workload details are still showing in flow explorer logs.
CTSP-20648	The Helpcenter link in the Spectrum portal is broken. The link for the Helpcenter icon displayed the HTTP 414 error when clicked for the first time and successfully loaded when clicked the second time.
CTSP-17357	When the user is trying to connect to Xaccess, “End user getting the connection down” message is displayed and the user is unable to access resources.

Known Issues

The following known issues are present in this release:

Bug ID	Description
Xshield	
CTSP-25287	The list of folders/paths and executables are not allowed for the Colortokens agent to work with the application control products like Airlock for the Windows 2003 server.
CTSP-25200	A manual guide for setting up AWS/Azure cloud Settings is required. This will help the user to add AWS/Azure subscription to Xshield.
CTSP-24866	The traffic status is shown as blocked /denied and authorized for same traffic at different time intervals. During troubleshooting we observed that it is expected because domain polices create a rule dynamically after resolving the domain group into IP address.
CTSP-24829	Visualizer displays “No group to display” message when the user loads the traffic for 7 days with the “Only show Groups with traffic” filter enabled.
CTSP-24642	Issue with FQL in flow explorer – the filtered results are not correct while using "OR" & "AND" conditions in the flow explorer page. For example: From the flow explorer page, when we apply the filter "src.groupname = Automation OR dest.groupname = Automation AND dest.ip != 224.0.0.0/8" the result shown still consists of traffic related to IPs of the destination subnet.
CTSP-24622	The traffic between workload and private network groups is not displayed. This happens when the "network groups" filter is used under the private networks wizard.
CTSP-24564	UDP outbound traffic is shown as inbound in flow explorer and visualizer. This happens whenever the response packet is delayed.
CTSP-24316	When a policy is defined on the workload, the number of rules it creates on the endpoint are not displayed to the user. The user should be given a warning message when firewall rules reach beyond the limit that can be configured on an endpoint
CTSP-23446	The Windows firewall services and the LGM services did not restart after a server reboot due to hypervisor crash. The user had to restart the server manually. In few servers, when the user tried to enable the firewall, “1068 service dependency error” was displayed.
CTSP-23378	The traffic from untagged assets is shown as blocked in Flow explorer.
CTSP-22955	CTSP drops Network flow messages from an agent when the maximum message limit (8 MB) is exceeded.
CTSP-22446	The Xprotect control data is marked as exfiltration data by Xshield. The Xprotect spectrum URL logs need to be exceptional in data exfiltration alerts.
Xaccess	
CTSP-24891	The Xshield User-agent (version - 8.10.4.3) utilizes high memory. This happens in few user agents.
CTSP-24751	Continuous login failure is observed in audit logs for multiple users. There were more than 1000 login failures in one minute.
CTSP-23949	Colortokens user agent does not re-authenticate when the password for the user has changed in AD.
CTSP-16983	Unauthorized access count shown on Xaccess dashboard does not match with the flow explorer count.