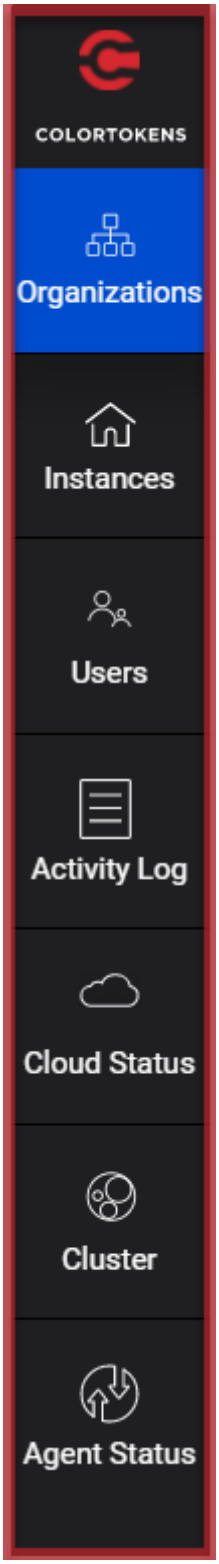

Release Notes

Zero Trust Security Platform

2022 Release R6, Version 8.22.6.2

What's Included

About the products....2
Xshield....2
Xaccess....2
What's New in Xshield and Xaccess....3
Changes to Public APIs:....4
Resolved Issues....5
Known Issues....6

About the products

The ColorTokens Zero Trust Security Platform is a multi-tenant Software As A Service (SaaS) security platform built to manage key security functions for an enterprise.

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 datacentre-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

- The Zero Trust Security Platform now supports network firewall integration with Palo Alto Panorama. This allows securing server workloads on which ColorTokens agents cannot be installed. This is accomplished by configuring a firewall protecting those servers.
- Policy recommendation can now recognize flows between two endpoints over a range of ports and summarize them into a single policy rule. This provides optimization in the number of policy rules to be programmed.
- The Zero Trust Security Platform now allows a tenant to set a banner (custom) for their users. The tenant users must read the banner and accept the terms and conditions provided in the banner to be able to login to the system.
- The Zero Trust Security Platform provides the firewall fusion status and enables profile on both the group pages as well as the summary page.
- The software will now send e-mail on alerts when server agent status changes.
- The agents will now notify whether the policy was deployed successfully. This will give better debuggability when agent enforcement is not working as expected.
- The new version of the server agent can now be supported on RHEL 8.5 and RHEL 8.6 operating systems.

Changes to Public APIs

Currently the public APIs expose some of the internal fields that force users to fill the fields with specific default values. In this release, the API documentation has been updated to mark all internal fields as “deprecated with default values set”. Eventually in subsequent releases, the internal fields will be removed completely - making the APIs user friendly and compatible with the interface used by the frond-end tool. **The support for the below fields will end in December 2022.**

Group	API	Fileds marked as "deprecated"
Domain Group	POST	• filters: attribute_name, exclude, hasDuplicate, invalid • group_type • state
	PUT	group_type
Endpoint Group	POST	• filters : attribute_name, exclude, hasDuplicate, invalid, selected • allowRemoteAccess • block • enable_dnat • group_type • state
	PUT	group_type
Network Group	POST	• filters : attribute_name, exclude, hasDuplicate, invalid, selected • allowRemoteAccess • block • enable_dnat • group_type • state
	PUT	group_type
Workload Group	POST	• filters : attribute_name, exclude, hasDuplicate, invalid, selected • allowRemoteAccess • block • enable_dnat • group_type • state
	PUT	group_type

Resolved Issues

The following issues have been resolved:

Bug ID	Description
Xshield	
CTSP-28455	Archival of flow records in S3 bucket was not working as expected.
CTSP-28072	During software upgrade, the traffic was getting mapped to the incorrect policy.
CTSP-27989	CPU utilization on the server was becoming high when the host firewall was programmed with a large number of rules.
CTSP-27271	It was not possible to add the private subnets to network groups.
CTSP-27024	It was not possible to access discovered private subnets when the number of discovered subnets exceed 2000.
CTSP-26437	Platform reported Firewall status as disabled for Windows 2003 even when Firewall was enabled. Firewall status will now be displayed as “N/A” for Windows 2003.
CTSP-25838	Traffic matching policies defined with CPT was shown as blocked.
CTSP-24829	Visualizer showed the “No groups to display” message when traffic was loaded for 7 days with the filter “Only show Groups with traffic”.
Xaccess	
CTSP-27641	A user logged out from the Xaccess UI was still able to access their applications for a period of time (10 minutes).
CTSP-24751	Continuous login failure was observed in audit logs for multiple users.

Known Issues

The following known issues are present in this release:

Bug ID	Description
Xshield	
CTSP- 28652	Deletion of a role-specific policy fails if the role was deleted prior to the policy.
CTSP-28551	While checking the vulnerability data using FQL filter, the device count changes continuously.
CTSP-27774	Domains which are already part of a domain group are displayed under the ungrouped bubble in the visualizer.
CTSP-27714	In the visualizer page, the traffic lines for private and public networks are not visible when “network groups” filter is selected. Additionally, when the option “only show groups with traffic" is selected, the public and private network bubbles do not get displayed.
CTSP-26961	It is not possible to download agent logs from the server.
CTSP-26881	The firewall state shows as Disabled in the dashboard for windows 2008 R2 enforced workload assets.
CTSP-26057	In tag rules tab, the asset hyperlink only displays server assets; user assets are ignored. Ideally, it should display both server and user assets, mapped by tag rules.
CTSP-26052	Newly created CPT is not visible in the CPT list even though the pop-up confirms the creation of the CPT with increased count.
CTSP-25794	FQL should have the ability to stick the whole query instead of individual blocks within the query. Also, the query should be executed when the enter key is pressed.
CTSP-25287	The list of folders/paths and executables are not allowed when a Colortokens agent works with application control products like Airlock for the Windows 2003 server.
CTSP-24866	The traffic status is shown as blocked/denied or authorized for the 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-24316	Warning should be given on dashboard once firewall rules reach beyond the limit that can be configured on an endpoint.
CTSP-23378	The traffic from untagged assets is shown as blocked in the flow explorer.
CTSP-22446	When Xprotect agents are installed along with Xshield agents, the control data generated by Xprotect is marked as unauthorized. As a workaround, an exception policy could be added to allow traffic from an Xprotect agent to its orchestration service.
Xaccess	
CTSP-26796	The ColorTokens-SRA tunnel does not get established in few scenarios when the user is remote.
CTSP-26228	User group information is not fetched from AD for some users after they have logged into the application.
CTSP-24126	User Access Group does not get updated consistently for the same user logging into different systems.
CTSP-23949	The user agent does not re-authenticate when the password for a user has changed in active directory.
CTSP-21311	Ipsec profile does not get pushed at the connector.

Bug ID	Description
CTSP-16983	Unauthorized access count shown on the Xaccess dashboard does not match with the flow explorer count.