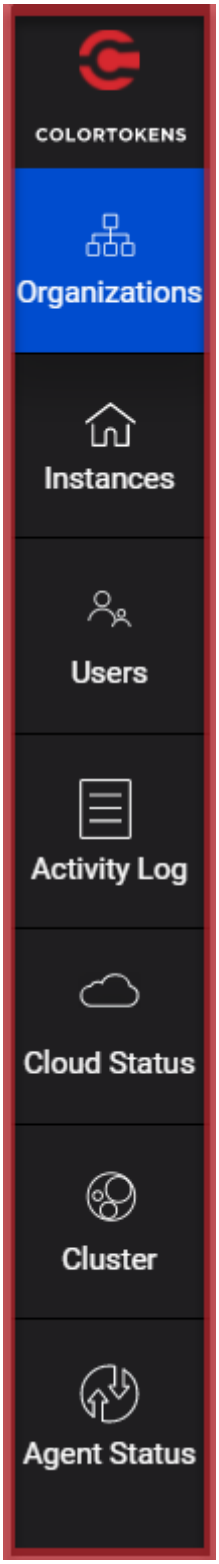

Release Notes

Xshield, Xaccess

2022 Release 03, Version 8.10.4.3

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:

- Installed agents renamed to distinguish between server and user agents ("ColorTokens Server Agent" and "ColorTokens User Agent"). Better visibility while using agent deployment tools.
- Private Networks in the visualizer now show the networks/subnets that are not grouped to improve visibility of traffic to these ungrouped networks.
- Administrators can easily author policies for entire internet or intranet without the need to create a group with many subnets.
- Corporate Policy Templates are now extended to allow Inbound rules. This helps in using them across multiple groups where similar Inbound communications are expected.
- Administrators can now configure a list of email addresses to be notified for alerts. Alert notifications were previously sent to all Instance Administrators.
- Higher resource Utilization creates a negative user experience or affects application performance which needs to be alerted so that immediate action can be taken by the administrators.
- Customers now get a consolidated list of all policies across Workload Groups in a CSV. Details of all the objects that make the policy are included. This is useful for sharing policies with multiple stakeholders involved in policy review and authoring.
- Increase our coverage by adding support for Oracle Linux 7.6
- Deprecated Security Sightings Report.
- Users can search the list of assets for which the Windows Firewall is turned off using FQL for troubleshooting.

Policy Workflow Enhancements

- New Group Workflow: a) Group-based navigation of assets, policies, traffic etc from a single screen. b) Dashboard for groups page to give a summarized view of state (observed/enforced) with an option to drill down into details.
- New Policy Workflow: Policy authoring is now a guided experience with a granular and flexible policy configuration wizard. Users can select/generate policies based on their preferences (Category, Depth and Granularity). For eg. Administrators can generate recommendations for specific categories like External networks, Internal Networks, Users and Groups and can apply these policies at an application or role level. At each step the wizard shows the strength of the policies to be applied. This can help administrators to approach policies in a phased and progressive manner.
- Policy recommendations are now loaded faster for a large number of groups which can help administrators use it effectively in larger deployments.

Resolved Issues

The following issues are resolved:

Bug ID	Description
CTSP-23750	This issue is seen only for Agents that are behind a proxy. The fix is to proceed with connection establishment from Agent to the Backend even if Domain resolution for colormaster fails.
CTSP-23066	When we have large number of Network groups Eg: 220 and more subnets under these groups like more than 1000 then Private network group bubble was not displayed in visualizer and due to this customer were not able to visualize the traffic
CTSP-22999	Modifications to Network group name via public API will not be supported
CTSP-22944	The Asset CSV download request was taking longer than expected to process when number of assets were few hundreds.
CTSP-22449	Policy synchronization status was not being calculated properly in few cases.
CTSP-22387	The filters are not working as expected, when we are selecting for inbound direction the traffic flow is shown in outbound direction.
CTSP-21116	A configuration option has been added to specify the folder where Agent should be installed. This folder can then be whitelisted in applications like Airlock.
CTSP-21097	Modifications to Corporate Policy Template name via public API will not be supported.
CTSP-20962	If domain name resolutions occurred prior to deployment of the policy, the mapping of the domain to its IP addresses will not be available to the agent and hence no policies will be enforced for those domain block rules. The issue is being addressed by having the agent make DNS queries for unresolved domains in configured policies.
CTSP-20860	Policy recommendations are not shown for workload groups that exceed the internal limitation of 40 workload groups
CTSP-20844	After selecting the policy from the recommendation page, the incorrect policy is applied in the assigned policies section.
CTSP-20714	Autosuggestions were not implemented for IP field when we moved to next gen UI.
CTSP-19364	From the audit logs during particular timestamps, we have observed that creation, updating policies and managed workloads activities were performed in less than 1 minute interval. Policy enforcement on servers can fail if other enforcement operations are currently in progress.
CTSP-17193	Policy and group creations/editing can take a long time (~22 seconds) as it can be blocked by the recommendation process running in the background

Known Issues

The following known issues are present in this release:

Bug ID	Description
Xshield	
CTSP-22955	The Connections count in the traffic panel and flow-explorer table is not matching with the flow explorer records count
CTSP-22446	Xshield is dropping Network flow messages from agent that are exceeding the maximum message limit (8 MB)
CTSP-15394	Session direction was marked incorrectly in some scenarios. Logic has been added to compute direction based on listening ports/Well know ports to mark the session direction correctly.
CTSP-22950	Audit logs page is taking time to load the data
CTSP-22767	Updating of the destination group name in the flow records will not happen in the first flow record. It is expected to be taken by maximum 1-5 minutes to reflect.
CTSP-22997	Tags are not getting removed after deleting it under scopes option
Xaccess	
CTSP-18454	Incorrect e-mail notification received for a user account that was not created
CTSP-17802	On windows 11 platform- there is no option for user to manually disconnect CT-SRA Tunnel
CTSP-17357	Users are getting the connection down message and unable to access resources intermittently
CTSP-21571	SRA Interface not getting created as Domain configuration is not populating in endpoints.
CTSP-16983	Unauthorized access count shown on Xaccess dashboard does not match with flow explorer count
CTSP-14660	End user must right click and click on open in order to open Xaccess end user app