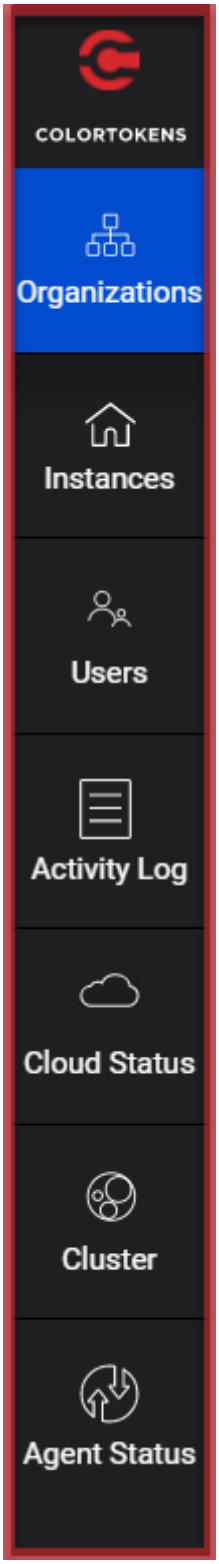


# Release Notes

# Xshield, Xaccess

2022 Release 02, 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*:

- The platform now supports archival of raw session data captured by the agents in a storage that can be retrieved for future use such as regulatory compliance audit. The supported archival is for a period of one year. The customer would be required to use standard tools to read the data post archival.
- The software has separated the storage of raw flow data into alternate storage. Due to this, the aggregation of network flow data (consolidation from 5-tuple to 4-tuple) is now performed inline which allows for the aggregated data to be available (for application consumption) at a much earlier time (within 30 minutes) than current time of up to two hours. Additionally, the data stored is much smaller in size, thereby providing more efficient and faster queries by the applications.
- A master backup file of original customer firewall rules will now be stored in the system. This master backup file can be used to restore the system back to the original state (before CT rules were applied) if needed.

## *New capabilities in Xacess*:

- Xaccess supports SAML based authentication to let customer choose among their preferred identity providers. With this change ADFS can be used as a SAML provider, which enables enterprises to use their local Identity provider, Active Directory, which sits within their firewall. ADFS integration enables them to allow their employees or partners to continue to use local AD for authentication. This feature not only enables enterprises to cater to their remote or mobile users to securely access their internal services but also for their in-office or local users to access other distributed data centres.

# Resolved Issues

The following issues are resolved:

| Bug ID | Description |
|---|---|
| CTSP-21792 | The traffic line colors in visualizer were displayed inconsistently when the number of connections were high. This fix will solve the inconsistency. |
| CTSP-20659 | The addition and deletion of Tags through public API was not functioning and not visible in user interface. This fix will solve both functionality and the display issue. |
| CTSP-20148 | The flow explorer data in the alerts page was retrieved inconsistently. This fix will solve the inconsistency with the data paltform1.1 changes |
| CTSP-18394 | The Policy violation alert data download into csv file in Flow explorer was not successful inconsistently. This fix will download of flow explorer data into csv file consistently |
| CTSP-19981 | In the flow explorer option to download 30days data is present. In the custom download we support upto maximum of 7 days only |
| CTSP-22570 | The flow explorer data was not showing while loading the traffic in visualizer, which was resolved. |
| CTSP-21055 | The flow explorer on the portal does not have the ability to download the latest 30 days. This fix will support the latest 30 days download and custom downlead supports only maximum of 7 days data download in Flow explorer |
| CTSP-22495 | Updating the policy commit ID was not consistent after the first 127 commits |
| CTSP-20737 | Domain Cache was not cleared when moving from enforced to observed mode, which is causing the issue and this was resolved. |
| CTSP-20422 | Earlier policy did not support parallelization of events in tenant. Causing even login and logout or some background resource related events to block Policy/group related task. We have made changes in policy architecture to support parallelization without having to block user due to background resource related events. |

# Known Issues

The following known issues are present in this release:

| Bug ID | Description |
|---|---|
| **Xshield** | |
| CTSP-22158 | The Connections count in the traffic panel and flow-explorer table is not matching with the flow explorer records count |
| CTSP-22876 | The keyword that is used in the FQL to show only the online users is showing the online users also. |
| CTSP-16978 | Asset page live user and Xaccess dashboard active users' options takes admin to all user details, it does not give information of all logged in users. |
| CTSP-22767 | Destination group name usually takes 5-10 min to show up in the flow records. |
| CTSP-16900 | Policy update does not work when both the groups are in "Encrypt" state. |
| CTSP-15858 | Outbound firewall rule added is not retained when system moves from Selective enforcement (Inbound) state to Observed state and vice versa. |
| CTSP-15774 | Block rules are added twice for domain-based policies.<br>CTSP |
| CTSP-15760 | Agent does the Aggregation of rules received from the backend and creates a single firewall rule. In this particular case user deleted one rule from workload machine and does some update from UI, because of aggregation check of matching rule is failing. |
| CTSP-15443 | When the Agent is decommissioned when it is in Block State, the Block CT rules are not removed |
| CTSP-15015 | When Agent restarts, probably it's receiving full policy update from backend which conveys agent to flush all existing rules and apply the rules received from the backend. For domain policy, since it will not have anything in cache for said domains, it has to the resolution first then create firewall rule. |
| CTSP-14765 | If user upgrade Agent for AIX from 8.6.x to latest the 443 rule to XShield is not removed. 8.6.x Agent we used to Add 443 rule to connect to Xshiled and subsequent agent versions we have removed it |
| CTSP-14722 | Firewall backup is not supported on macOS. |
| CTSP-14688 | Firewall rules are present after changing state from Enforced mode to Observed mode in macOS and AIX machines. |
| CTSP-14593 | When Enforced CT Rules are tampered, the same are not reverted in AIX. Policy Tamperering feature is not supported |
| CTSP-14592 | Domain Based Policies are not supported for AIX. |
| CTSP-14591 | Domains are not reported in AIX environment. |
| CTSP-14396 | Support for Domain-based policy on Solaris OS does not exist. |
| CTSP-14395 | Support for Selective enforcement on Solaris OS does not exist. |
| CTSP-14393 | Support for policy tampering on Solaris OS does not exist. |
| CTSP-13865 | Selective Enforcement does not work in Windows 2003. |

| Bug ID | Description |
|---|---|
| CTSP-13457 | Support for password protected decommission on Solaris OS does not exist. |
| CTSP-12798 | Pushing the policy to the AQ resource while manually updating the conditions on the resource is consuming more time. |
| CTSP-11368 | The installer will not read the product-key from the file name, and will not skip the product-key window for entering the product-key |
| CTSP-19630 | When Agent is downgraded from 8.4.2.2 version it fails |
| CTSP-19363 | When Agent add any firewall rule irrespective of allow/block, it add the rule and enable firewall. With Block policy support Agent need to make sure if firewall was disabled before, Agent should add allow all rule so that it behaves exactly same for allowed traffic. |
| CTSP-19865 | FW rule optimization implemented by eliminating rules with overlapping / duplicate IP addresses. This implementation has a limitation that it does not optimize the rules with overlapping ports. The port optimization will be taken up as separate enhancement in future releases. |
| CTSP-19844 | Generation of Security Sightings Report takes a very long time when volume of records in the system exceeds 1B. |
| CTSP-13335 | In the Zero Day scenario, users do not have an option to navigate to ***Pre-approved*** or ***Pending approval*** tabs for server resources. |
| CTSP-10929 | Tag rule is not saved in unstable state. |
| CTSP-21882 | Users are unable to dynamically select the check box for enabling and disabling PDF and console options |
| CTSP-20132 | Authorized traffic status with Rule mode No-Policy is confusing for the end user. |
| **Xaccess** | |
| CTSP-22941 | Connected to only two gateways after disable/enable the connector |
| CTSP-22882 | Configured Domain behind disabled connectors are still seen |
| CTSP-20086 | Connector re-establishing tunnel with Gateways whenever we deploy and tokenize new Gateway |
| CTSP-19725 | When Backend admin provisions a new Gateway (uknown to customer), the connectors will not form IPSEC tunnel with newly Provisioned gateway |
| CTSP-18888 | For certain time range, Xaccess dashboard widget for top connectors by data transfers shows the data value as NaN Undefined. |
| CTSP-13709 | When the department source changes to AD, the corresponding endpoint group is not updated. |
| CTSP-11651 | CPU usage is not distributed uniformly among the cores of CPU. |
| CTSP-10879 | When static IP pool is defined and the IPSec connection is switched to another gateway, the assigned ip changes to the pool defined for that gateway. It gets changed to the pool defined for that gateway. The static IP is maintained and is specific to the gateway. |
| CTSP-10463 | Two connectors cannot be deployed behind a single public IP via NAT. |
| CTSP-9923 | The users are allowed to add multiple SAML with the same file or metadata. |
| CTSP-8902 | The endpoint group is not updating group value when group name is updated in Azure AD. |

| Bug ID | Description |
|---|---|
| CTSP-8897 | The user session (who created the test connection) remains active on CM for long in the User's tab. |
| CTSP-4140 | The VPN connection information accessed via command line is not accurately displayed for non-admin users. |
| CTSP-21813 | When a new IP/Subnet is added apart from existing subnets behind the connectors it is resulting in FRR Config being reloaded resulting in existing TCP Connections being reset |
| CTSP-21314 | Connector Network config does not list all IP/Subnets if the list has more than 20 entries. So, use the search panel to search for a particular IP or Subnet |
| CTSP-12328 | If Multiple IDP , SAML, LDAP or Local is configured, SAML IDP takes Priority and subsequent IDPS's are not tried for user Authentication. But Not Available, Admin can have multiple IDP's however of same Type. |
| CTSP-18704 | CT-SRA gets connected in office network (DC Network). sometimes user is local in DC however ct-sra tunnel is up considering user as remote. |
| CTSP-18100 | To handle multiple IPs for a domain in DNS response |
| CTSP-17859 | When an end user turns off the CT-SRA automatically Connect option intentionally or otherwise, they cannot connect to the agent and hence won't be able to access the required resources. |
| CTSP-17802 | The Xaccess Tunnel disconnect option does not work after it is connected automatically to the gateway on Windows 11 resource. |
| CTSP-14456 | An error message is displayed indicating that the user is unauthorized to access a resource through the Tunnel when the user tries to access the resource for the first time. |
| CTSP-12721 | The Auto Quarantine rules do not work in gateway when the option "Enable default remote access to internal resources" is selected. *Workaround*: Do not enable this option if you plan to use Xaccess Auto-Quarantine policies for the user assets managed from the instance. |
| CTSP-18590 | Multiple icons of agent are noticed in the system tray when a system is restarted and rebooted. The stale entries will disappear when the cursor is placed on the stale icons. |
| CTSP-18211 | The feature to hide real IP is not functional only when the NAT pool is modified. |
| CTSP-17133 | The SUA session continues to appear even after SAML IdP is deleted. This issue also appears for LDAP IdPs. |
| CTSP-16983 | Unauthorized access count displayed on the Dashboard does not match with the count displayed in the Flow Explorer. |
| CTSP-16089 | When an endpoint is part of an enforced endpoint group, a blank CTI window is displayed after providing username or email ID on SAML IdP. |
| CTSP-15903 | Deep link unavailable to identify live users. |
| CTSP-14660 | Xaccess agent does not open from system tray upon left click. |