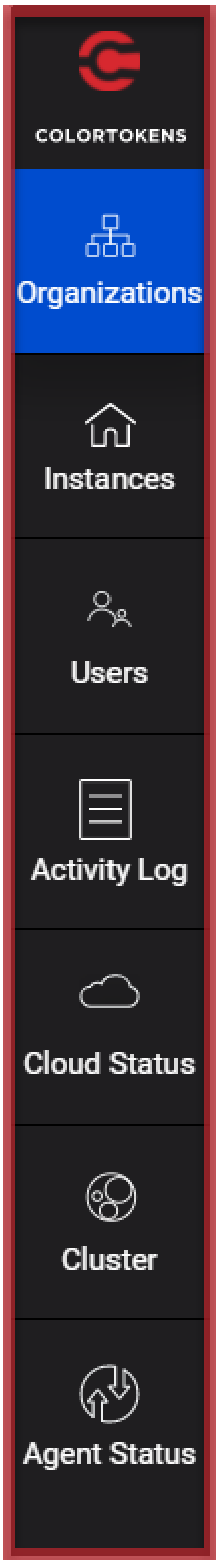

# Release Notes

# Xshield, Xaccess

2022 Release 01

# 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*:

- CentOS 7.9 and RHEL 6.4 OS Versions are supported in Microsegmentation Agent
- Unique registration of Xshield Agents provisioned as clones of a master host image is now possible with the newly added support for provisioning servers such as Citrix PVS or VMware Horizon View for large scale deployments.
- The platform supports white labelling the tenant portal UI pages with the tenant’s logo and name. Customer can upload their logos on to the platform and use them.

## Resolved Issues

The following issues are resolved:

| Bug ID | Description |
|---|---|
| CTSP-20269 | Unable to add domains with underscore symbol to domain group. The fix allows domains with underscore symbol. |
| CTSP-17757 | "OS All" option in the asset summary page takes the user to wrong page instead of OS summary page. The fix takes the user to OS summary page. |
| CTSP-19931 | The issue was with the policy version id being updated by agent to the platform. This is fixed now. |
| CTSP-18999 | The problem was observed in the policy version id tagging while switching from observe to enforce mode. During this time the active sessions showed up as blocked. The fix is to wait till the process of transition from observe to enforced is completed and then looking at the packet drops to send the alerts from the agent. |
| CTSP-18914 | Agent was not programming the policy on tunnel interfaces which was causing this issue. The fix was to program the policy on the tunnel interfaces which enabled proper working in the cluster. |
| CTSP-21273 | Quarantine is not working for an asset when configured through Public API. |
| CTSP-19576 | Audit logs generated when agent is upgraded does not include name of the host on which the upgrade is initiated. The fix hostname in audit log. |
| CTSP-18955 | While using Okta IdP, an error appears while importing the xml from okta. Resolution: The Issuer of the IdP is used as a unique identifier (displayed as Identity provider in my account section of Org Admin in spectrum UI), so that the Issuer is unique per application, even if the user is part of multiple applications. |

# Known Issues

The following known issues are present in this release:

| Bug ID | Description |
|---|---|
| **Xshield** | |
| CTSP-16900 | Policy update does not work when both the groups are in "Encrypt" state. |
| CTSP-16361 | Multiple firewall entries with duplicate IPs are added upon ping and *wget* actions in a Linux environment. |
| 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. |
| CTSP-13457 | Support for password protected decommission on Solaris OS does not exist. |

| Bug ID | Description |
|---|---|
| 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-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-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. |
| 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. |

| Bug ID | Description |
|---|---|
| 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 Connect automatically* 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. |