**Zscaler Common Support Issues**

**Blocked Website(s)**

**Escalation:** **CSIRT and DOJ**

When a CFPB employee needs to access a website for official Bureau business, but the website is blocked or access is limited, an employee will contact the Service Desk. If an employee can access a website that should not be allowed on the CFPB network, a Blacklist request should be made.

* Whitelisted will allow access to the website(s).
* Blacklisted will not allow access to the website(s).

1. Service Desk Technician will direct the user(s) to submit a [Web Content Filtering Exception Request](https://cfpbprod.servicenowservices.com/servicecenter?id=sc_cat_item&sys_id=c1be7d621b897510db1da82fe54bcb63). (the request goes to the CSIRT team queue)
2. If approved, CSIRT will route the request to DOJ to implement. Create Outlook email from the [CFPB\_SOC@cfpb.gov](mailto:CFPB_SOC@cfpb.gov) mailbox and send to:

* [DOJ.Service.Desk@usdoj.gov](mailto:DOJ.Service.Desk@usdoj.gov)
* [DOJ.SharedServicesEngineering@usdoj.gov](mailto:DOJ.SharedServicesEngineering@usdoj.gov)
* Samantha Williams DOJ Customer Success Manager (CSM) Samantha.A.Williams@usdoj.gov
* Stephen J. Ramesh ([Stephen.J.Ramesh@usdoj.gov](mailto:Stephen.J.Ramesh@usdoj.gov))
* [servicedesk@cfpb.gov](mailto:servicedesk@cfpb.gov) (instructions in email to also inform DOJ to CC SD.)

1. DOJ will provide a Ticket number for reference to CSIRT. DOJ will CC CFPB mailboxes for updates ([CFPB\_SOC@cfpb.gov](mailto:CFPB_SOC@cfpb.gov) and [servicedesk@cfpb.gov](mailto:servicedesk@cfpb.gov)) as the process is completed.
   * The CFPB ServiceNow ticket should be manually updated with this information from the emails.
2. Once instructed that the request has been completed, SD updates their CFPB ticket and informs customer to test the website(s) are working as expected.
   * IF working, the ticket(s) can then be closed.
   * IF not working, the SD will contact CSIRT and CSIRT will continue the conversation with the DOJ. (SD should log issues to share)
3. CSIRT closes their ticket and SD closes the ticket in their queue.

**Slowness with Zscaler Service**

**Escalation:** SD, DOJ

Slow browsing or download issues can come from multiple source issues including DNS resolution delay, packet retransmission issues, or even third-party software components.

To find what is causing the slowness and get to the root cause as fast as possible, we want to collect a bit more information.

**Escalation**: **Escalate incident to SD, DOJ**

**Capturing end-user experience**

* When did the slowness start? (Estimation)
* Is this for all websites or a specific website/web application? Provide a list and describe behavior.
* Does this impact a single user, single site, or multiple sites?
* Which method(s) are you using to route traffic? (i.e., Explicit proxy, PAC, GRE, VPN)

**Information Gathering**

1. **Determine the Cloud Path**: Provide a screenshot of ip.zscaler.com from the affected machine.
2. Next, we will check the node health, datacenter throughput and provide an MTR back to your IP.
3. **Run MTR Trace** - with Zscaler Analyzer => z-traceroute found on the (ip.zscaler.com) page.
4. https://help.zscaler.com/zia/how-do-i-use-zscaler-analyzer
5. Collect at least 300 packets
6. If you are using IPsec or GRE tunnels this must show the route outside the tunnel.
7. This Zscaler Analyzer tool is present on (ip.zscaler.com) page, for download.
8. **Run Specific URL baseline** - Zscaler Analyzer => z-WebLoad tool with default settings.
9. Never test using google.com.
10. https://help.zscaler.com/zia/how-do-i-use-zscaler-analyzer

**Note 1:** Please be prepared to install Wireshark or Windows NetMon, for a WebEx with our engineers. We may need captures from your client and on our nodes, so we can analyze the traffic flow between yourselves and our nodes.

**Note 2:** We strongly recommend setting up Zscaler Analyzer on monitoring stations in various regions for long-term regional baselining and troubleshooting. Note, this may require correct firewall ruleset and routing considerations.

**Application(s) unable to connect to the internet**

Applications that are unable to connect to the internet are sometimes caused when SSL decryption using Zscaler breaks the application due to certificate pinning.

**Escalation**: **Network Management**

**Troubleshooting Data Collection:**

* When did the slowness start?
* Does this impact a single user, single site, or multiple sites?
* Is this for all websites or a specific website/web application? Provide a list
* Zscaler Application Logs in Debug Mode.
* Screenshot of the error seen.
* Also collect HTTP header capture and Wireshark capture, this will provide additional insights (optional).

**Issue**

Description

**Escalation:** Escalate incident to:

**Troubleshooting Data Collection:**

**Issue**

Description

**Escalation:** Escalate incident to:

**Troubleshooting Data Collection:**

**Issue**

Description

**Escalation:** Escalate incident to:

**Troubleshooting Data Collection:**

**Issue**

Description

**Escalation:** Escalate incident to:

**Troubleshooting Data Collection:**