**Overview**

Initial troubleshooting and triage support for Zscaler issues will be performed by the CFPB Service Desk (SD) Tier I and Tier II Technicians and involves categorizing, prioritizing, and managing support tickets based on complexity and urgency. This process includes deciding the order of treatment, tagging, assigning, and routing of Incident Tickets and SCTASKS in ServiceNow to ensure that the right specialist(s) or group(s) provides effective support or escalation to the DOJ.

Incident Ticket escalation occurs when Technician completes their troubleshooting process and finds an issue to require a higher level of access and expertise. The Technician will pass an issue through the assignment method in ServiceNow to the Zscaler Support group to provide a resolution or further escalation to the DOJ, often times with an increased priority level.

Zscaler issues will be first received by **Tier I** and **Tier II Technicians**, with a real time resolution expected, if possible. If needed, there will be an escalation workflow provided:

e.g., **Escalation:** **End-user > Service Desk > Zscaler Support Group > DOJ**

Common Support Topics

The components of this service are:

* **Zscaler Client Connector (ZCC)** - Provides seamless user experience by automatically recognizing when you connect to a CFPB-trusted network or to Wi-Fi hotspots (e.g., airports, hotels) where you must accept a use policy before connecting.
* **Zscaler Internet Access (ZIA)** - Ensures your internet traffic to external sites is forwarded and protected.
* **Zscaler Private Access (ZPA)** - Securely access your organization's internal resources from any location.
* **Zscaler Digital Experience (ZDX)** – Performs synthetic probing to a desired Software-as-a-Service (SaaS) application or internet-based service (e.g., OneDrive, Teams, etc.) to triage and pinpoint the source of performance issues.

Initial Troubleshooting (Tier I & II)

**Initial Troubleshooting** practices aid in reduced resolution times and proper triaging.

**Resources and Tools**:

* Zscaler Client Connector (ZCC)
* Zscaler Digital Experience (ZDX) Monitoring
* BeyondTrust (Bomgar)
* ServiceNow Service Desk Ticketing System
* ServiceNow Service Desk Documentation Knowledge base

**Tier I** and **Tier II** **Technicians** will:

* Clarify the problem through information gathering with end-user.
* Attempt to isolate the cause by referencing the SD Knowledge base and peers to seek known solutions.
* Remote into end-user’s device using BeyondTrust to reproduce/resolve the issue, capture screen grabs, and other information as needed.
* Document actions performed in the ServiceNow Incident Ticket.
* Resolve or Escalate to Zscaler Support Group. If escalated,
  + Attach all relevant screen grabs and documentation.
  + Keep communication open with other groups until issue is closed.
* Post-Resolution Review for critical takeaways.

Blocked Website(s) (Tier I & II)

When an end-user needs to access a website for official Bureau business, but the website is blocked or access is limited, it may be because:

* Website is **Blacklisted** and needs to be **Whitelisted**.
* URL incorrectly categorization in Zscaler **URL** or **Security** Databases

If users can access a website that should **not** be allowed on the CFPB network, a **Blacklist** request should be made to block or limit access. See [5.1.6 Blacklist Requests (Tier I & II)](#_Blacklist_Requests_(Tier)

**Escalation:** **End-user > Service Desk (I or II?) > Zscaler Support Group > DOJ**

**Tier I** and **Tier II** **Technicians** will:

* Submit a [Web Content Filtering Exception Request](https://cfpbprod.servicenowservices.com/servicecenter?id=sc_cat_item&sys_id=c1be7d621b897510db1da82fe54bcb63) on behalf of the end-user.

This request goes to the CSIRT team queue.

**If not approved**

**CSIRT** will:

* + Update the request the notes.

**Tier I** and **Tier II** **Technicians** will:

* + Update and close the Incident.

**If approved**

**CSIRT** will:

* Route the request to DOJ to implement by creating an 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 ([samantha.a.williams@usdoj.gov](mailto: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)

**CSIRT** will:

* Route the request to DOJ to implement

**DOJ** will:

* + Provide a Ticket Number for reference to CSIRT.
  + Include all 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.

**Tier I** and **Tier II** **Technicians** will:

* Manually update CFPB ServiceNow ticket should be with information from DOJ emails communications.
* Once the request is completed by the DOJ, work with the end-user to test the website(s) are working as expected.
  + IF resolved, the ticket(s) can then be closed.
    - * **CSIRT** will close their ticket.
  + IF not working, the SD will update ticket and contact CSIRT.
* **CSIRT** will continue the conversation with the DOJ.

Slowness with Zscaler Service (Tier I & II)

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. (The updated site is https://ip.zscalergov.com/, ZIA is still active and is part of the ZCC, add that from the previous version. The ZDX can be accessed in myapps.microsoft.com)

**Required**: **Zscaler Digital Experience (ZDX) Monitoring**

**Escalation:** **End-user > Service Desk > Zscaler Support Group > DOJ**

**Capture end-user experience**

* Can you provide an estimation on how long you have been experiencing slowness?
* Currently, how many users and devices are actively using your Wi-Fi and bandwidth?
* Is your firewall configured to block or limit access to any websites that are being used for work purposes? (Windows Firewall)
* Is your router configured to block or limit VPN access on any device?
* Are there any bandwidth limitations per device being used? (Quality of Service)
* 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?

**Note:** If the issue is on a CFPB device, Technicians can log into those devices to check configurations. If the issue is not on a CFPB device, such as the user’s router, Technicians may not continue troubleshooting and defer users to ISP or manufacturer for continued support.

Technicians will collect the above data, including screenshots if possible, and include in Incident Ticket to Networking Engineering or the Zscaler group. (Cardell or Network engineering?)

**Capture end-user data through ~~Bomgar~~ ZDX**

* **Determine Cloud Path** by providing a screenshot from the affected machine.
  + Check Node Health and Datacenter Throughput in ZDX Admin. Console.
* **Run speed test using fast.com** – Using Bomgar
* **Run a Diagnostic Session** using ZDX to collect at least 300 packets.

**Note:** If using IPsec or GRE tunnels, this must show the route outside the tunnel.

**Resource:** https://help.zscaler.com/zdx/about-diagnostics

Application(s) unable to connect to the internet (Tier I & II)

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:**

* Can you provide an estimation on how long you have been experiencing outage?
* Currently, can any user (including yourself) access any website using any device on your Wi-Fi and bandwidth?
* Is this for all websites or a specific website/web application? Provide a list and describe behavior.
* Is your firewall configured to block or limit access to any websites that are being used for work purposes? (Windows Firewall)
* Is your router connectivity light blinking or solid? If solid, what color? Contact ISP.
* Are there any bandwidth limitations per device being used? (Quality of Service)
* Screenshot of the error seen.

Note: If the issue is on a CFPB device, Technicians can log into those devices to check configurations. If the issue is not on a CFPB device, such as the user’s router, Technicians may not continue troubleshooting and defer users to ISP or manufacturer for continued support.

Technicians will collect the above data, including screenshots if possible, and include in Incident Ticket to Zscaler Support group. (Is this going to Cardell or Network engineering?)

Network Engineering will also collect HTTP header capture and Wireshark capture will provide additional insights.

Unable to connect to the CFPB Intranet (Tier I & II)

**Escalation**: **Network Management or Zscaler Support**

**Troubleshooting Data Collection:**

* Can you provide an estimation on how long you have been experiencing outage?
* Currently, can any user (including yourself) access any website using any device on your Wi-Fi and bandwidth?
* Is this for all websites or a specific website/web application? Provide a list and describe behavior.
* Is your firewall configured to block or limit access to any websites that are being used for work purposes? (Windows Firewall)
* Is your router connectivity light blinking or solid? If solid, what color? Contact ISP.
* Are there any bandwidth limitations per device being used? (Quality of Service)
* Screenshot of the error seen.

**Note:** If the issue is on a CFPB device, Technicians can log into those devices to check configurations. If the issue is not on a CFPB device, such as the user’s router, Technicians may not continue troubleshooting and defer users to ISP or manufacturer for continued support.

Forward to Network Engineering.

New Issues go to Zscaler Support (Network Engineering and System Engineering groups)

Unable to connect while at HQ (Tier II)

**Escalation**: **Tier I** > **Tier II** > **Zscaler Support Group**

When an end-user needs to access the internet for official Bureau business, on a CFPB-device **ONLY**, but the user’s connection is blocked or access is limited, it may be because:

* The network port may not be active.
* The network cable could be shorted, or a cable is missing.
* The docking station may not have a connection or is damaged.
* The firmware for the docking station may need to be updated.
* The USB-C port may be damaged.

Deskside Support Technician will go to the user to inspect all the above and any configurations on the device to rule out hardware issues. If any of the hardware is the issue, Technician will follow equipment replacement protocol.

If hardware has been ruled out, Technicians will follow these steps

**Troubleshooting Data Collection:**

* Can you provide an estimation on how long you have been experiencing outage?
* Can user’s device access any website using this device on the CFPB Wi-Fi?
* Is this for all websites or a specific website/web application? Provide a list and describe behavior.
* Screenshot of the error seen.

Technicians will collect the above data, including screenshots if possible, and include in Incident Ticket to the Zscaler Support group. (Is this going to Cardell or Network engineering?)

Note: New Issues go to Zscaler Support (Network Engineering and System Engineering groups)

Blacklist Requests (Tier I & II)

If an employee can access a website that should **not** be allowed on the CFPB network, a **Blacklist** request should be made to block or limit access. This is a high priority item.

**Escalation:** **End-user > Service Desk > Network Management > DOJ**

1. SD Technician will create an **Incident** in the ServiceNow portal.
2. SD Technician will create a **Request** from the **Incident**. The **Incident** creates a **RITM**, which creates a **Task** for the Technician to follow the progress updates.

Note: This **Request** goes to the Network Management team queue.

1. If approved, Network Management will route the request to DOJ to implement by creating an 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 ([samantha.a.williams@usdoj.gov](mailto: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)

**Note:** If not approved, the Network Management team will update the ticket and SD will receive the update, then close the Incident, including the notes.

1. DOJ will:
   * Provide a Ticket Number for reference to CSIRT.
   * Include all 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.
2. The CFPB ServiceNow ticket should be manually updated with information from the emails by Service Desk Technicians.
3. Once the DOJ completes the request, SD will update the related CFPB ticket and inform end-user 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)
4. Once SD closes the ticket in their queue, CSIRT will close their ticket.

Other Issues (Tier I & II)

**Escalation:** **End-user > Service Desk > Network Management > DOJ**