Service Desk

Zscaler Standard Operating Procedure

Consumer Financial Protection Bureau (CFPB)

<< Document Number>>

August 2024

1. 

Table of Contents

[Table of Contents i](#_Toc174434052)

[Table of Figures iii](#_Toc174434053)

[Table of Tables iii](#_Toc174434054)

[Revision History iv](#_Toc174434055)

[1 Introduction 1](#_Toc174434056)

[1.1 Purpose 1](#_Toc174434057)

[1.2 Intended Audience 2](#_Toc174434058)

[1.3 Roles and Responsibilities 2](#_Toc174434059)

[1.4 Primary Points of Contact 3](#_Toc174434060)

[1.5 Related Support Documents 3](#_Toc174434061)

[1.6 Related Website Links 4](#_Toc174434062)

[2 Diagrams 5](#_Toc174434063)

[3 Service CI 7](#_Toc174434064)

[4 Zscaler Client Connector (ZCC) 8](#_Toc174434065)

[4.1 Service Components 8](#_Toc174434066)

[4.2 Installation Packages 8](#_Toc174434067)

[5 Triage (End User Support) 9](#_Toc174434068)

[5.1 Common Support Issues 9](#_Toc174434069)

[5.1.1 Blocked Website(s) (Tier I & II) 9](#_Toc174434070)

[5.1.2 Slowness with Zscaler Service (Tier I & II) 10](#_Toc174434071)

[5.1.3 Application(s) unable to connect to the internet (Tier I & II) 13](#_Toc174434072)

[5.1.4 Unable to connect to the CFPB Intranet (Tier I & II) 14](#_Toc174434073)

[5.1.5 Unable to connect while at HQ (Tier II) 14](#_Toc174434074)

[5.1.6 Blacklist Requests (Tier I & II) 15](#_Toc174434075)

[5.1.7 Other issues 16](#_Toc174434076)

[5.1.8 Tools 16](#_Toc174434077)

[5.2 Zscaler Troubleshooting Menu 17](#_Toc174434078)

[5.2.1 Troubleshooting Zscaler in Windows 17](#_Toc174434079)

[5.2.2 Troubleshooting Zscaler services in macOS 19](#_Toc174434080)

[5.2.3 Troubleshooting Zscaler services in iOS 21](#_Toc174434081)

[5.2.4 Zscaler Common Error Codes 22](#_Toc174434082)

[6 Responsible, Accountable, Supported, Consulted, Informed (RASCI) Matrix 23](#_Toc174434083)

[6.1 Appendix C: Justice Edge Trust Service Roles & Responsibilities 23](#_Toc174434084)

[7 Related Controls 26](#_Toc174434085)

[7.1 Control Activity Summary 26](#_Toc174434086)

[7.2 Records Management 26](#_Toc174434087)

[8 Approvals 27](#_Toc174434088)

[9 Appendices 28](#_Toc174434089)

[Appendix A: Key Terms and Acronyms 28](#_Toc174434090)

[Appendix B: <<Insert Appendix Title>> 29](#_Toc174434091)

# Table of Figures

[Figure 1: Detailed Design Diagram 5](#_Toc174368873)

[Figure 2: Flow Diagram 6](#_Toc174368874)

[Figure 3: Zscaler Troubleshoot menu (Windows) 15](#_Toc174368875)

[Figure 4: Zscaler Troubleshoot menu (macOS) 15](#_Toc174368876)

[Figure 5: Zscaler Troubleshoot menu (iOS) 15](#_Toc174368877)

# Table of Tables

[Table 1: Revision History iv](#_Toc174367662)

[Table 2: Roles and Responsibilities Summary 2](#_Toc174367663)

[Table 3: Primary Points of Contact Summary 3](#_Toc174367664)

[Table 4: Related Documents Summary 3](#_Toc174367665)

[Table 5: Related Links 4](#_Toc174367666)

[Table 5: Justice Edge Trust Service Roles and Responsibilities 17](#_Toc174367667)

[Table 6: Control Activities Summary 20](#_Toc174367668)

[Table 7: Records Management Summary 20](#_Toc174367669)

[Table 8: Key Terms and Acronyms 22](#_Toc174367670)

Revision History

Table : Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Approved By | Effective | Change Summary | Author |
| 1.0 |  | June 2024 | Initial Release | <<Insert POC Name>> |

# Introduction

This document defines the scope and roles and responsibilities for the Cybersecurity Services that the Consumer Financial Protection Bureau (“CFPB” or the “Bureau”) has provisioned from the Department of Justice (DOJ) and Zscaler. As an outcome of the Discovery Project that CFPB and DOJ completed, DOJ will provide recommendations for the deployment of its Justice Edge Trust Service (JETS) tailored to CFPB technical and operating environment. JETS is built on top of a secure and scalable infrastructure that provides end to end encryption and strong authentication to ensure the confidentiality and privacy of transmitted data. Based on the information gathered during the Discovery project, CFPB selected capabilities will be listed on scope of work and defined.

To successfully integrate cloud computing and Software-as-a-Service (SaaS) for almost all its requirements, the CFPB is implementing a Zero Trust Architecture (ZTA). The general ZTA plan is to outsource market-supported commodity work and shift practically all current computing and data workloads to AWS. Legacy applications will also be replaced with comparable SaaS services. This will eventually enable the Bureau to lessen and scale back its reliance on the Local Area Network (LAN) and conventional network security models in order to access vital technological services and instead adopt key Zero Trust principles such as Never trust and always verify based on identity with multi-factor authentication, device trust, and important security attributes like location, micro segmentation, and least privilege.

The Bureau will utilize DOJ JETS for the administration of CFPB's Zscaler tenants. DOJ will have the responsibility to make all configuration and policy changes that have been approved and requested by CFPB.

## Purpose

The purpose of this Standard Operating Procedures (SOP) is to provide overview and instruction how to triage and escalate requests and incidents as it relates to the Discovery Project deployment of JETS and Zscaler. There may be references to other services provided through this program, but this document only references other services in defining how the JETS operates. The scope of this document does not include definition of those related services.

## Intended Audience

The CFPB Service Desk which includes, Service Desk (Tier I), Desktop Support (Tier II), Active Directory (AD) Management, and Incident Management teams. The Zscaler Support team includes Desktop Engineering, Systems Engineering, and Network Management. Desktop Support (Tier II) will escalate to Zscaler Support and Zscaler Support will escalate to DOJ.

## Roles and Responsibilities

There are several roles within CFPB that are involved in the delivery and consumption of services within the scope of JETS. This section defines these roles and outlines the responsibilities associated with each. This SOP should serve as a guide in determining which internal roles, teams, or groups should be aligned to the roles defined below.

Table : Roles and Responsibilities Summary

|  |  |
| --- | --- |
| Role | Responsibility |
| **System Owner** | * Providing oversight and system owner function for the solution. |
| **Tier I (Service Desk)** | * First User contact * Provide initial triage of incidents * Assist users to the correct Request Catalog |
| **Tier II (Deskside Support)**  **AD Management Team**  **Incident Management** | * Further troubleshooting and documenting issues, including capture screen shots and logs. |
| **\*Desktop Engineering** | * 3rd level support for the Zscaler Client for macOS and Windows |
| **\*Systems Engineering** | * Sudip will talk with Kevin Cline |
| **\*Network Management** | * Deep dive into Network related issues, including capturing screen shots and logs (if necessary; escalate to DOJ or resolve) |
| **ETS Mobility** | * 3rd Tier Support for Zscaler client issues on iOS devices. |

\*Zscaler Support Group – They reach out to DOJ if needed.

## Primary Points of Contact

Table : Primary Points of Contact Summary

|  |  |  |
| --- | --- | --- |
| Role | Point of Contact | Contact Topics |
| **System Owner**  \*Must be a Lead or higher | Name: Ali Sadeghi  Title: Senior Infrastructure Engineer  T&I Office: Infrastructure | * Providing oversight and system owner function for the solution. |
| **Network Management** | Name: Walter Riddle Title: Network Engineer | * Network Engineering SME |
| **Desktop Engineering** | Name: Cesar Carvajal  Title: Infrastructure End-User Strategy Lead | * Desktop Engineering SME |
| **Service Desk** | Name: Cathy Hurkamp  Title: Sr Service Desk Specialist | * Tier I/II support |
| **Cyber Security** | James William and Tyrone Whitfield |  |
| **DOJ Customer Success Manager (CSM)** | Samantha Williams Samantha.A.Williams@usdoj.gov |  |
|  | Stephen J. Ramesh ([Stephen.J.Ramesh@usdoj.gov](mailto:Stephen.J.Ramesh@usdoj.gov)) |  |

## Related Support Documents

Table : Related Documents Summary

|  |  |  |
| --- | --- | --- |
| Document Name | Description | Notes |
| **Zscaler SOP Template** | Includes all the information of the project. |  |
| [**KB0014254**](https://cfpbprod.servicenowservices.com/kb_view.do?sysparm_article=KB0014254) **BeyondTrust (Bomgar) Remote Support User Guide** | The BeyondTrust representative console can be deployed via SCCM via the UDA - Bomgar External Console collection. | \*Update title to include Bomgar |
| [**KB0014228**](https://cfpbprod.servicenowservices.com/kb_view.do?sysparm_article=KB0014228) **Reconnect to Always On VPN Zscaler on Windows** | The **Zscaler Test – AnyConnect Profile** – Switcher utility was created to allow Windows laptops to disconnect from the VPNs while maintaining internet connectivity in support of Zscaler Pilot Phase. | \*Will stay active until all users are on Zscaler |
| [**KB0014229**](https://cfpbprod.servicenowservices.com/kb_view.do?sysparm_article=KB0014229) **Connect to Zscaler VPN for Macs** | The **Zscaler Test – AnyConnect Profile** – Switcher utility was created to allow Mac laptops to disconnect from the VPNs while maintaining internet connectivity in support of Zscaler Pilot Phase. | \*Will stay active until all users are on Zscaler |

## Related Website Links

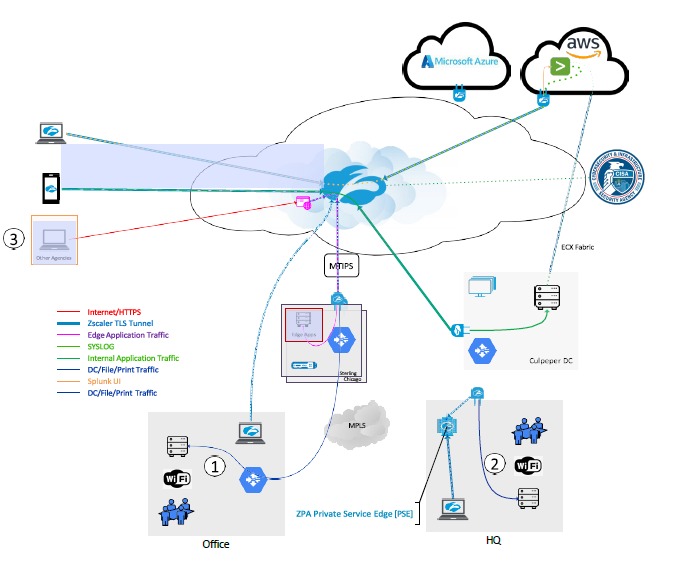
Table : Related Links

|  |  |
| --- | --- |
| Website | URL |
| **Using Zscaler Client Connector** | <https://help.zscaler.com/zscaler-client-connector/using-zscaler-client-connector> |
| **Enrolling in the Zscaler Service on Zscaler Client Connector** | <https://help.zscaler.com/zscaler-client-connector/enrolling-zscaler-service-zscaler-client-connector> |
| **Troubleshooting Zscaler Client Connector** | <https://help.zscaler.com/zscaler-client-connector/troubleshooting-zscaler-client-connector> |
| **Zscaler Client Connector: Connection Status Errors** | <https://help.zscaler.com/z-app/zscaler-app-connection-status-errors> |
| **Zscaler Client Connector Errors** | <https://help.zscaler.com/z-app/zscaler-app-errors> |

# Diagrams

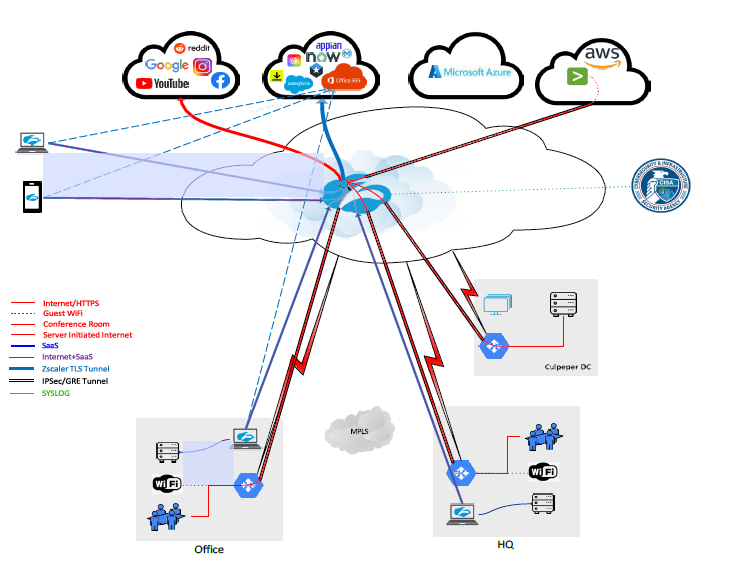
## Detailed Design

Figure 1: Detailed Design Diagram



## Flow

Figure : Flow Diagram



# Service CI

**Service CI -** [Zscaler JETS Prod](https://cfpbprod.servicenowservices.com/cmdb_ci_service.do?sys_id=0cecd4cd1b75691044f587fbe54bcbca&sysparm_record_target=cmdb_ci_service&sysparm_record_row=1&sysparm_record_rows=1&sysparm_record_list=nameCONTAINSzscaler%5EORDERBYname)

# Zscaler Client Connector (ZCC)

ZCC is an application installed on all CFPB Windows, macOS, and iOS mobile end-user devices to ensure internet traffic and access to internal apps are secure and in compliance with Bureau policies, even when you're off a CFPB network. The app accomplishes this by disabling its services temporarily and re-enabling itself after you've had a chance to complete the steps necessary to connect.

## Service Components

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.

## Installation Packages

The following installation packages are in the System Center Configuration Manager (SCCM) application for Windows devices and JamF on macOS devices.

* **Windows**
  + UDA - Zscaler (AOVPN Cutover)
  + UDA – Zotero v6.0.6 Install Collection
* **macOS**
  + Migrate from AOVPN to Zscaler (Self Service)

# Triaging End-User Zscaler Issues

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

### 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. (Is this going to 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

**Starting a New Diagnostics Session**

To start a new Diagnostics session:

1. Perform one of the following actions:

* In the ZDX Admin Portal, go to Diagnostics > Start New Diagnostics Session.
* On the User Details page, click the Start New Diagnostics Session button.

**Note:** This opens a new Start New Diagnostics Session window with the username and device details prefilled.

* On the User Overview page, click the Start New Diagnostics Session button in the user's row.

**Note:** This opens a new Start New Diagnostics Session window with the username prefilled.

* On the Diagnostics page, copy an existing session using the Copy icon.

**Note:** This opens a new Start New Diagnostics Session window with all details of an existing session copied. All fields are editable. If the device has a session in progress or is no longer associated with the user, it is not copied.

Graphical user interface, text, application, website

Description automatically generatedThe Start New Diagnostics Session window appears.

1. In the Start New Diagnostics Session window:

* **Name:** Enter a name for the session. (Need a name the team agrees with, as well as where to store the screenshots.)
* **User:** Choose the user for this session from the drop-down menu.
* **Device:** After selecting a user, choose the device for this session from the drop-down menu.

**Note:** If the device has an ongoing troubleshooting session or there is a version incompatibility, the device appears grayed out in the menu. To learn more, see [Supported Versions & Feature Compatibility](https://help.zscaler.com/zdx/supported-versions-feature-compatibility).

Graphical user interface, application

Description automatically generated

* What would you like to run?**Choose among the selections:**

Graphical user interface, application

Description automatically generated

**Note:** Depending on which type of session you select, the minimum versions of Zscaler Client Connector and ZDX Module are required. To learn more, see [Supported Versions & Feature Compatibility](https://help.zscaler.com/zdx/supported-versions-feature-compatibility).

* + Deep Tracing - (Cannot select as an add-on to **Bandwidth Testing**)
  + Bandwidth Testing (Cannot select as an add-on to **Deep Tracing**)
  + Packet Capture Probing - Select as an add-on with **Deep Tracing**, or **Bandwidth Test**. If there are no compatible devices for selection, then you cannot select this option.

**Note:** If you select **Bandwidth Test** or **Packet Capture Probing**, *choose* 5 minutes, 15 minutes, 30 minutes, or 60 minutes for the Run Session For option, however, devices are not shown if Applications and Probes do not run for at least 30 minutes.

1. Click Next to start configuring the session if you chose **Deep Tracing** or **Packet Capture Probing** as an option. If you chose only Bandwidth Testing, proceed to the next step.
   * [Deep Tracing](https://help.zscaler.com/zdx/starting-new-diagnostics-session#DeepTracing)
   * [Bandwidth Testing](https://help.zscaler.com/zdx/starting-new-diagnostics-session#BandwidthTesting)
   * [Packet Capture Probing](https://help.zscaler.com/zdx/starting-new-diagnostics-session#PacketCaptureSettings)
2. Click Save to create and start the session.

After you click Save, you see the session in the In Progress table on the Diagnostics page. As the session progresses, its status is updated, and it eventually moves to the History table. You can view session results by clicking the View icon. To learn more, see [Viewing Diagnostics Session Results](https://help.zscaler.com/zdx/viewing-diagnostics-session-results).

### 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

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

## ZCC Troubleshooting Menu

* Private Access - Internal sites
* Internet Security – External sites, needs to be on.
* Digital Experience (ZDX)

**Troubleshooting for Connectivity and Slowness issues** (ZCC troubleshooting menu options)

* Check Private Access
* Internet Security
* Troubleshooting menus options:
* **Restart Service -** Restarting Zscaler Client Connector doesn't impact security enforcement. When users select Repair App, the app attempts to repair itself by reinstalling app drives and services.
* **Repair App -**

ZDX console on admin.zdxgov.net (Preferred method. ZCC is secondary)

* Gives an indicator on the performance Dash by app to see if there is an issue with the user. User dash lets you zero in on an app or all apps by user or all users over a timeframe.
* Shows you if a connection is good, bad, or otherwise under ZDX Score User Distribution.
* Issue with machine and gateway
* Gateway and ISP, issue is ISP.
* Need a definition chart?

### Troubleshooting Zscaler in Windows

Following are further details about the Troubleshoot menu features of the Zscaler App.

Figure : Zscaler Troubleshoot menu (Windows)

**Graphical user interface, application

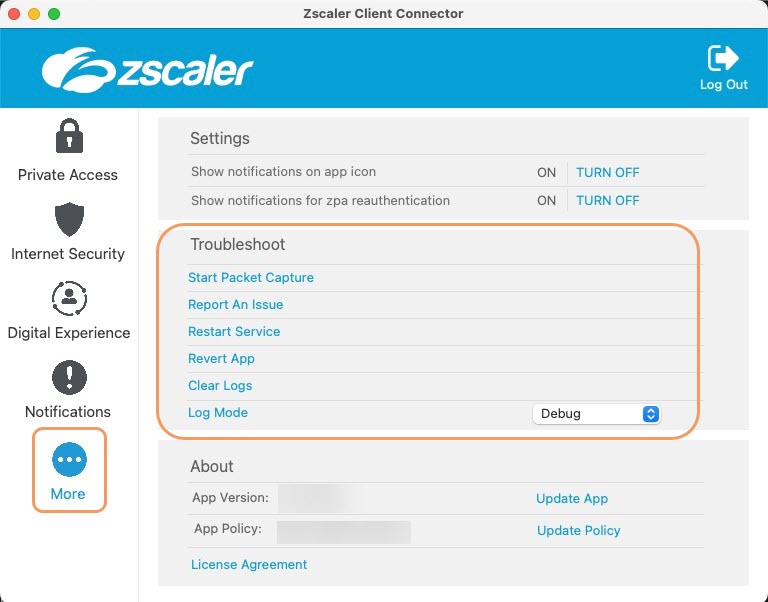
Description automatically generated**

* **Start Packet Capture:** If your organization's admin enabled packet captures, you can use this feature when reproducing an issue. To learn more, see [Using the Start Packet Capture Option](https://help.zscaler.com/client-connector/enabling-packet-capture-zscaler-client-connector).
* **Export Logs:**
* **Restart Service:** You can click to restart the app. Restarting does not impact security enforcement.
* **Repair App:** If you select this option, the app will attempt to repair itself by reinstalling app drivers and services. Zscaler recommends trying this option before reporting an issue.
* **Clear Logs**: You can clear stored logs.
* **Log Mode:** You can change the mode in which Zscaler Client Connector generates logs, but the change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by your organization. Below is a description of each log mode.
  + - **Error:** Logs only when the app encounters an error and functionality is affected.
    - **Warn:** Logs when the app is functioning but is encountering potential issues, or logs when conditions for the Error log mode are met.
    - **Info:** Logs general app activity, or logs when conditions for the Warn log mode are met.
    - **Debug**: Logs all app activity that could assist Zscaler Support in debugging issues, or logs when conditions for the Info log mode are met.

### Troubleshooting Zscaler services in macOS

Following are further details about the Troubleshoot menu features of the macOS version of the

Zscaler App.

Figure : Zscaler Troubleshoot menu (macOS)

* **Start Packet Capture:** Captures packets; use this feature when reproducing an issue. To learn more, see [Using the Start Packet Capture Option](https://help.zscaler.com/z-app/enabling-packet-capture-zscaler-app#using-start-packet-capture).
* **Export Logs:**
* **Restart Service:** You can click to restart the app. Restarting does not impact security enforcement.
* **Repair App:** If you select this option, the app will attempt to repair itself by reinstalling app drivers and services. Zscaler recommends trying this option before reporting an issue.
* **Clear Logs**: You can clear stored logs.
* **Log Mode:** You can change the mode in which Zscaler Client Connector generates logs, but the change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by your organization. Below is a description of each log mode.
  + - **Error:** Logs only when the app encounters an error and functionality is affected.
    - **Warn:** Logs when the app is functioning but is encountering potential issues, or logs when conditions for the Error log mode are met.
    - **Info:** Logs general app activity, or logs when conditions for the Warn log mode are met.
    - **Debug**: Logs all app activity that could assist Zscaler Support in debugging issues, or logs when conditions for the Info log mode are met.

### Troubleshooting Zscaler services in iOS

Following are the Troubleshoot menu features of the iOS version of the Zscaler Client Connector:

Figure : Zscaler Troubleshoot menu (iOS)

Graphical user interface, text, application

Description automatically generated

* **Start Packet Capture:**If your organization's admin enabled packet captures, use this feature when reproducing an issue. For instructions on using this option, see [Using the Start Packet Capture Option](https://help.zscaler.com/z-app/enabling-packet-capture-zscaler-app#using-start-packet-capture).
* **Report An Issue**: If your organization’s admin enabled in-app support access, use this feature to report an issue. When you submit the form, depending on your organization’s setup, the app may either send an email to your organization’s support admin or submit a ticket directly to Zscaler Support. Your support admin receives a copy of this ticket as well. After you submit the form, you receive an email acknowledging the support request. For instructions on completing the form, see [Reporting an Issue with Zscaler Client Connector.](https://help.zscaler.com/zscaler-client-connector/reporting-issue-zscaler-client-connector#ios)
* **Restart Service**: Tap this option to restart the app. Restarting does not impact security enforcement.
* **Export Logs**: Tap this option to export logs to a .enc file, then email that file to your organization’s support admin.
* **Clear Logs**: Tap this option to clear stored logs.
* **Log Level**: Change the mode in which the app generates logs. The change is effective for that connection session only. At the start of the next connection session, the app returns to the default log mode set by your organization. The following is a description of each log mode.
  + **Error**: Logs only when the app encounters an error and functionality is affected.
  + **Warn**: Logs when the app is functioning but is encountering potential issues or when conditions for the Error log mode are met.
  + **Info**: Logs general app activity or when conditions for the Warn log mode are met.
  + **Debug**: Logs all app activity that could assist Zscaler Support in debugging issues or when conditions for the info log mode are met.

### Zscaler Common Error Codes

Zscaler Client Connector Error Messages

# Responsible, Accountable, Supported, Consulted, Informed (RASCI) Matrix

## Appendix C: Justice Edge Trust Service Roles & Responsibilities

Table # provides a draft roles and responsibility for Justice Edge Trust Services (JETS). See Appendix A for RASCI definitions. The JETS deployment will be a complex tool deployment, providing transformational network changes for CFPB. There will be many lessons learned during the piloting and initial deployments. As a result, the roles and responsibilities matrix will evolve over time, with additional activities being added through the development of pilot and deployment plans. With Zscaler’s multi-tenant model, CPB will retain the ability to define their policies and configuration settings, but implementation will be performed in coordination with DOJ.

* **Responsible:** The stakeholder in charge of a decision or task
* **Accountable:** The stakeholder who has overriding authority over decisions and direction, but is typically not involved in the implementation of specific tasks
* **Support:** The stakeholder who is required to be involved in a task or decision, but is not ultimately in charge of it
* **Consulted:** The stakeholder who is likely to have important input that needs to be considered in decisions
* **Informed:** The stakeholder who needs to be provided with updates on progress, risks, issues, or other elements of tasks and decisions

The RASCI matrix in Table # depicts important activities related to JETS including the role different parties play in relation to each other. The following roles, which were introduced in Section #, are identified in the matric by abbreviation.

* DOJ Service Owner (SO)
* Customer Success Manager (CSM)
* DOJ Engineering Team (DET)
* DOJ Service Desk (JSD)
* CFPB Service Desk Leads (SDL)
* CFPB Deskside Support (DSS)
* CFPB Service Desk (SD)

Table : Justice Edge Trust Service Roles and Responsibilities

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **DOJ** | | | | **CFPB** | | |
| **SO** | **CSM** | **DET** | **JSD** | **SE** | **TT** | **SD** |
| CFPB Tenant account management | A | S | R |  | C | I |  |
| CFPB Tenant IdP configuration and group-to-role configuration |  | S | R |  | A | C | I |
| User account management for end users of service |  |  |  |  |  | R | S |
| Provisioning and configuration of EFA Tenant | A | S | R |  | C,I | C,I |  |
| Deploy ZCC to EFA endpoints |  |  |  |  |  |  |  |
| Implement initial policy and configuration settings |  |  |  |  |  |  |  |
| Installation, configuration, and O&M support of App Connectors for DOJ-hosted applications |  |  |  |  |  |  |  |
| Installation, configuration, and O&M support of App Connectors for EFA-hosted applications |  |  |  |  |  |  |  |
| Installation, configuration, and O&M support of App Connectors for 3rd party-hosted applications |  |  |  |  |  |  |  |
| Configure and manage deployment for direct peering to cloud applications and internet |  |  |  |  |  |  |  |
| Policy maintenance and tuning |  |  |  |  |  |  |  |
| Refinement of policies and configuration settings |  |  |  |  |  |  |  |
| Conduct testing and validation of traffic flows and policies |  |  |  |  |  |  |  |
| Configure and maintain Application Programming Interface (API) with CISA CLAW for cloud telemetry data sharing |  |  |  |  |  |  |  |
| Authorize and establish CLAW data sharing parameters with CISA |  |  |  |  |  |  |  |
| Create, evaluate, and approve CRs through EFA CCB |  |  |  |  |  |  |  |
| Submit EFA-approved CSRs to DOJ for implementation |  |  |  |  |  |  |  |
| Intake, evaluate, and implement EFA CSRs |  |  |  |  |  |  |  |
| Troubleshoot end user issues (endpoint support such as general connectivity issues and Zscaler client connector) |  |  |  |  |  |  |  |
| Troubleshoot issues with Zscaler platform (Software as a Service) |  |  |  |  |  |  |  |
| Customer support and issue management |  |  |  |  |  |  |  |
| Configure logging to SIEM |  |  |  |  |  |  |  |
| Maintenance, health, and performance monitoring |  |  |  |  |  |  |  |
| Assess and propose modernization and optimization recommendations |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| Role | Responsibility |
| **DOJ Service Owner (SO)** |  |
| **DOJ Customer Success Manager (CSM)** |  |
| **DOJ Engineering Team (DET)** |  |
| **DOJ Service Desk (JSD)** |  |
| **Customer Agency Service Lead (CASL)** |  |
| **EFA Technical Team (ETT)** |  |
| **EFA Service Desk (ESD)** |  |
| **Service Desk (Tier I)** | * First User contact * Provide initial triage of incidents * Assist users to the correct Request Catalog |
| **Deskside Support (Tier II)**  **AD Management Team**  **Incident Management** | Further troubleshooting and documenting issues, including capture screen shots and logs. |
| **Desktop Engineering** | 3rd level support for the Zscaler Client for MACs and Windows |
| **Network Management** | Deep dive into Network related issues, including capturing screen shots and logs (if necessary; escalate to DOJ or resolve |
| **ETS Mobility** | * 3rd Tier Support for Zscaler client issues on IOS and Android devices. * Android devices – Desktop Audiocode phones located in limited (Director’s office and SCC). |

# Related Controls

## Control Activity Summary

<<List any control activities that are described in the content sections above or otherwise related to the topic of this SOP.>>

Table : Control Activities Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Control Activity | Responsibility | Timing | Key Output(s) |
| **<<Name of control activity>>** | <<Position titles of those responsible for the activity>> | <<Required timing of the activity (e.g., weekly, monthly, quarterly)>> | <<Key documents or other outputs created as a result of the activity>> |
|  |  |  |  |

## Records Management

<<List any official Bureau records that are created as a result of this SOP process/topic. You may also include other key outputs that are not official records, but that Bureau users may need assistance in locating.>>

Table : Records Management Summary

|  |  |  |
| --- | --- | --- |
| Record/Document Type | Retention Requirement | Storage Location |
|  |  |  |
|  |  |  |
|  |  |  |

# Approvals

Document Owner Date

T&I Team Lead Date

CIO (or Delegate) Date

# Appendices

1. Key Terms and Acronyms

Table : Key Terms and Acronyms

|  |  |
| --- | --- |
| Term/Acronym | Definition |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. <<Insert Appendix Title>>