#### **Zscaler Training**

Recommended documents and activities to prepare Service Desk Technicians for Zscaler training:

Documentation that covers the most common issues end users will reach out to Service Desk about:

1. *Zscaler Deployment End User Quick Guide.*
2. *DOJ CSSP Service Support Reference Guide* (recommended).
3. *DOJ JETS Service Guide* (Recommended).

Service Desk should go through their inventory of playbooks/scripts and workflows in SNOW to identify which playbooks or workflows may be impacted by the implementation of Zscaler.  Typically, agencies will want to update their documentation to help the Tier 1 help desk analyst more efficiently triage the most common issues that an end-user would call/email about.

For example, if the end user is blocked from reaching a URL, your Service Desk would want to use updated procedures to triage the issue

1. Check if it is a Zscaler policy that is causing the block.
2. Escalate to an internal team (i.e., Cyber team) to approve or deny this user from getting access to this URL.
3. Once a decision is made, that change is submitted to DOJ as a service request.
4. DOJ will implement the policy change.

The above example is a common end user issue that can come up.  Essentially, your procedures or workflows just need to be adjusted so that DOJ JETS is engaged when

1. a change to policy/configuration needs to be made OR
2. there is an end-user issue that needs DOJ JETS (like a Tier 2/3) to investigate and troubleshoot.

Every agency has its own internal escalation procedure so it’s best that we start there, and we can advise on when DOJ would be contacted.

Notes: Proposed Training Schedule with DOJ

Requirements:

* 1. Register for Zscaler academy and have profile
  2. PUA for admin rights to the portal has to be processed
  3. Zscaler client installed on each machine
  4. **Optional:** Training in Bomgar and be installed on machines

1. **Full Training August 8, 2024, 10 am – 5 pm EST. –** Bruce, Mehdi, Brandon M, Kipp, Juju, Alphonso, Duane, Derek Watkins, David S. C. Gray Dany as TW, Nelly as Technical Trainer, and potential other techs (any technician that can follow along but does not all the requirements completed) can audit the training. (recorded)
2. **Full Training August 15, 2024, 10 am – 5 pm EST. –** Tier 2 (all day) (recorded)
3. **Condensed Training August 16, 2024, Time TBD –** Tier 1 (half day) (request to be recorded)

Tier I Support Team

|  |  |  |
| --- | --- | --- |
| Technician | Role | Training Date |
|  | Pathfinder |  |
|  | Pathfinder |  |

Tier II Support Team

|  |  |  |
| --- | --- | --- |
| Technician | Role | Training Date |
|  | Pathfinder |  |
|  | Pathfinder |  |

Other Groups

|  |  |  |
| --- | --- | --- |
| User | Role | Training Date |
| Dany Garcia | Technical Writer |  |
| Nelly Casseus | Technical Trainer |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | User | Email | Training Topic | Training Date |
|  |  |  |  |  |
|  |  |  |  |  |

#### **Zscaler Support Topics**

The SD Technicians will work with other CFPB internal groups. Those groups will work directly with internal CFPB departments/groups/individuals and the DOJ, an External Federal Agency (EFAs). DOJ to provide comprehensive support. CFPB internal groups/teams will include Desktop Engineering (DE), System Engineering, Network Management, Active Directory (AD) Management, Incident Management, and Cybersecurity (CSIRT).

End-User Self Service

Provides self-service resolutions for CFPB end-users.

1. **Enrolling on Zscaler Client Connector QRG \***Not Needed now, the system automatically
2. **Common Support Issues (FAQs)**
   1. Logging in to Zscaler
   2. Blocked Website
   3. Slowness with Zscaler Service
   4. Unable to connect while at HQ
   5. Website Blocked due to incorrect categorization in Zscaler URL Database

Service Desk Triage and Escalation

Provides triage, resolution, or escalation processes for CFPB Service Desk Technicians.

1. **Enrolling on Zscaler Client Connector QRG for Service Desk Technicians**
2. **Common Support Issues (FAQs)**
   1. Logging in to Zscaler
   2. Blocked Website (Blacklisted, Website Blocked due to incorrect categorization in Zscaler URL Database,)
   3. Slowness with Zscaler Service
   4. Unable to connect while at HQ
   5. and white listed
3. **Zscaler Client Connector (ZCC) QRG for Service Desk Technicians**
4. **Zscaler Troubleshooting** (user calls and techs walk them through the steps, techs remote in)
5. Troubleshooting Zscaler in Windows
6. Troubleshooting Zscaler in macOS
7. Troubleshooting Zscaler in iOS
8. **Common Zscaler Connector Issues**
9. Zscaler Client Connector Error Messages
10. Zscaler Client Connector Cloud Authentication Error Codes
11. Zscaler App Cloud Error Codes
12. Zscaler App Portal Error Codes
13. Report an Issue Error Codes
14. **Zscaler Digital Experience (ZDX) Navigation Guide for Service Desk**
15. **Helpful Web Links**
16. List sites

Notes

* **Topic** – Description.

Zscaler Support Topics (closed Zscaler tickets)

|  |  |  |
| --- | --- | --- |
| Incident Number | Topic | Resolution |
| [INC0132277](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3Dad90a1a01b7a4214a7ca433ee54bcbdf) | Certificate | **Symptoms:** Can not make aws cli call: SSL validation failed  **Resolution: :** Internal issue. The Zscaler certificate provided by Michael Erps helps to resolve the problem.   * Manually specify a custom path with the provided Zscaler certificate to use when establishing SSL/TLS connections. * Zscaler was supposed to populate the certificate at the default path, but for unknown reasons it did not. |
| [INC0125853](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3D11c295b647e5ca1073f9bd51026d43b9)  [INC0124833](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3D93bbb63b1b918610dbc743f1f54bcb12%26sysparm_stack%3D%26sysparm_view%3D)  [INC0125157](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3Df1dff0241bedc210a7ca433ee54bcb9d)  [INC0125157](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3Df1dff0241bedc210a7ca433ee54bcb9d)  [INC0126195](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3D2fb47f1f47edce10d1785ff2e16d4301%26sysparm_stack%3D%26sysparm_view%3D) | Configuration | **Symptoms**: CFPB Domain error. CFPB Network Check message every day. It says "x days since CFPB Domain Network Detection. Connect to the Full VPN, or Dock your Computer as soon as possible for Security Updates."  **Resolution:** The domain connectivity fix for Agency Alerts has been deployed to Zscaler users and they should no longer see the warning message. |
| [INC0126696](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3D57c3e18947b5ca50d1785ff2e16d435d) | Remote Access | **Symptoms:** I am unable to remote desktop to wdcdeviqdw01 and I think it is due to ZScaler issue  **Resolution:** Not resolved, David spoke with user. |
| [INC0125143](https://cfpbprod.servicenowservices.com/now/nav/ui/classic/params/target/incident.do%3Fsys_id%3D95962d941b2182106c5f0f67624bcb08%26sysparm_stack%3D%26sysparm_view%3D) | Whitelisting | **Symptoms:** Can't access Treasury API via Postman.  **Resolution:** Issue was resolved through Whitelisted with the DOJ |
|  |  | **Symptoms:**  **Resolution:** |
|  |  | **Symptoms:**  **Resolution:** |

**Notes from Zscaler Triage and Escalation Workflow middle**

Short term goal is to be operational by August 21, 2024, need to work through PUAs

MS Entra - Ali is currently adding Walter Riddle to the group to add users, as George is leaving.

(Ali, Jeff, and Walter can handle access, they will add Will and Corey)

Ali went through the following topics

**Admin groups**

* Zscaler
* ZDX
* ZIA
* ZPA

**ZCC menus**

* 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
* 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?

**Tools**

**ip.zscalergov.com** - Use this tool to verify if a user is logged on, we will have to document the error messages as we come across them, (like off ip.zscalergov.com) and capture the screenshot.

**https://trust.zscaler.com/zscaler.net** -

**ZIA –** Public access

**ZPA** – Private access

**Blocked sites** – grab screenshots, try drive.google.com.

* If you click on the link to request a review, you are sent to the Zscaler link and sending the request there will get it rejected.
* Sudip will look into updating where the customer is sent with DOJ.
* This will help with reducing users calling the SD.
* Looking to see if we can add additional language.

iOS roll out ***after*** macOS & Windows devices are done.

* Once devices are on Zscaler, all traffic will go through Zscaler, vs by app.

ip.zscalergov.com - Use this tool to verify if a user is logged on, we will have to document the error messages as we come across them, (like off ip.zscalergov.com) and capture the screenshot.

The Zscaler Cloud Performance Monitoring app did not work, Ali will look into it.

Cloud Health for speed testing and outages.

<https://trust.zscaler.com/zscaler.net> -

Meeting with Ali to talk about ZDX console and what screengrabs and steps must be documented.

As per Sudip: The registered users with DOJ for read only access goes to ICAM - to further add them to Entra ID group

Sudip will meet with me to discuss.

#### **Zscaler Documentation**

The ServiceNow Knowledgebases will contain the following documents:

Customer Knowledgebase

This knowledgebase has articles to provide self-service for CFPB end-users.

1. [KB0014228](https://cfpbprod.servicenowservices.com/kb_view.do?sysparm_article=KB0014228) *Reconnect to Always On VPN Zscaler on Windows.*
2. [KB0014229](https://cfpbprod.servicenowservices.com/kb_view.do?sysparm_article=KB0014229) Connect to Zscaler VPN for Macs
3. Zscaler FAQ for End-Users
4. Zscaler End User Quick Reference Guide

ServiceDesk Knowledgebase

This knowledgebase has articles for the CFPB ServiceDesk technicians to assist users.

1. Zscaler ServiceDesk SOP
2. Zscaler End User Quick Reference Guide ServiceDesk Edition
3. Zscaler FAQ for Technicians
4. Zscaler Client Connector Error Codes

Notes

* **Topic** – Description.