U.S. Department of Justice
Office of the Chief Information Officer

# Service Guide for the Justice Edge Trust Service (JETS)

## Department of Justice (DOJ) Cybersecurity Shared Services Program (CSSP)

## December 27, 2022

# Table of Contents

# 1 Introduction

This document is the official guide for the Department of Justice (DOJ) Cybersecurity Shared Services Program (CSSP) Justice Edge Trust Service (JETS) offering, which is part of the Justice Managed Security Services (JMSS). This guide will provide information about how the service is deployed, maintained, monitored, and supported. In addition, the roles and responsibilities of DOJ and the External Federal Agency (EFA) customer are defined within this guide to develop a clear delineation and understanding for all stakeholders. Use of this guide will ensure the EFA customer is well-informed and is able to successfully utilize the JETS.

## 1.1 Scope

This document only covers the JETS provided through the DOJ CSSP. 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.

# 2 Roles and Responsibilities

There are several roles within DOJ and the EFA 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. It is understood that each EFA will have its own internal organization, lines of authority, and support mechanisms. This guide does not require any changes to these existing definitions and relationships but should guide EFA customers in determining which internal roles, teams, or groups should be aligned to the roles defined herein based on which ones are best suited to each. The goal is to ensure that each EFA customer has a clear understanding of how to get the maximum value out of JETS.

## 2.1 JETS Service Owner

The Service Owner is responsible for defining the vision for the service offering and ensures that there is a service lifecycle roadmap aligned to this vision. The Service Owner is the individual within DOJ who is ultimately accountable for service delivery to all customers and ensures that internal DOJ business operations necessary to deliver and advance the service roadmap are occurring as necessary. The Service Owner is responsible for the Inter-Agency Agreement between the EFA and DOJ.

## 2.2 DOJ Customer Success Manager

The Customer Success Manager (CSM) is the individual within DOJ who is the EFA customer's primary point of contact. They lead the on-boarding process for the service with the EFA, manage regular reporting, track issues to resolution, and ensure that various stakeholders within the EFA customer organization understand the full capability of the service in order to ensure they can get the most out of it. They're an advocate for the EFA customer with regards to the service offering.

## 2.3 DOJ Engineering Team

The DOJ Engineering Team is responsible for the ongoing Operations and Maintenance (O&M) of the service as well as for Development, Modernization, and Enhancement (DME) efforts that are initiated to advance the service lifecycle roadmap for the Service Owner. The DOJ Engineering Team handles Information Technology (IT) incident resolution, service requests, and requests for changes in accordance with procedures defined for the service.

## 2.4 DOJ Service Desk

The DOJ Service Desk is the Tier 1 IT service point of contact, which is responsible for handling the intake of all IT service incidents, service requests, and changes. Communication regarding all of these is coordinated through the DOJ Service Desk to ensure full visibility and traceability.

## 2.5 DOJ Justice Security Operations Center (JSOC)

The DOJ JSOC is the 24x7x365 Security Operations Center that manages the JSOC blocklist, which is a curated CTI feed leveraging open and classified sources. The DOJ blocklist consists of a customer URL category that is added applied to a role and is updated in near real time and currently consists of over 3,000+ IP/URL.

## 2.6 Customer Agency Service Lead

The Customer Agency Service Lead (CASL) is the individual within the EFA who is responsible for providing capabilities within the EFA organization, which DOJ's service offering is being implemented to provide.

## 2.7 EFA Technical Team

The EFA Technical Team is an important role with regards to the ongoing consumption of the service by the EFA. There are typically technical leads from various IT disciplines or groups included in the EFA Technical Team, such as Network Operations, Platform Services, and End User Services. The key responsibilities associated with this group include:

- Submitting requests to DOJ for changes to the service configuration
- Identifying, escalating, and working in collaboration to address IT service incidents
- Receiving service update and maintenance notifications, and coordinating any analysis or communication within the EFA organization that may be necessary
- Zscaler console using read-only access will allow, view all features in tenant, run reports, and monitor the status of the EFA tenant in the dashboard

## 2.8 EFA Service Desk

The EFA Service Desk is the Tier 1 IT support service point of contact within the EFA, which should be the likely first to encounter reports of service issues from users if any should arise. When any issues are related to the DOJ service being provided, they will be responsible for facilitating communication regarding the issue within the EFA (Technical Team and EFA end-users). For example, if an incident occurs, EFA Service Desk will report the incident to DOJ Service Desk and copy EFA Technical Team. DOJ will provide updates to the EFA Technical Team and EFA Service Desk via email. The EFA Service Desk will then need to ensure that this is disseminated to users who had reported an issue.

## 2.9 EFA Change Control Board

When the JETS team receives a Customer Support Request (CSR) it is assumed that this has already cleared the EFA Change Control Board for the EFA prior to submitting Customer Support Requests (CSRs).

# 3 Service Technical Overview

JETS provides a Secure Access Service Edge (SASE) platform managed with enhanced security configurations, specifically designed to meet the needs of Federal government organizations. It is integrated with DOJ's Security Operations Center as a Service (SOCaaS) offering, which unifies the management and monitoring capabilities of this key security technology for EFA customers working to move to a Zero Trust Architecture (ZTA). DOJ's Cyber Threat Intelligence (CTI) is directly integrated with the service offering to ensure that customers benefit from a well-architected platform that serves the needs of their mobile and cloud-centric workforce while protecting the organization's business and mission. DOJ's Endpoint Detection and Recovery (EDR) service is directly integrated with JETS to ensure that customers benefit from secure, conditional access to applications based on device health, while also ensuring zero-day threats are identified, analyzed, and remediated.

## 3.1 Service Components

The components of this service are:

- Zscaler Client Connector (ZCC)
- Zscaler App Connector
- Zscaler Management Platform

### 3.1.1 Zscaler Client Connector (ZCC)

The ZCC is an endpoint agent, which EFA customers deploy to any device that is intended to receive services through JETS. It is a lightweight application which can be deployed to laptops, mobile devices, desktops, kiosk systems, and others and acts as a Policy Enforcement Point (PEP). ZCC forwards traffic to the closest Zscaler service edge, where the traffic can then be routed to the internet, cloud services, or internal application in accordance with organizational policies.

### 3.1.2 Zscaler App Connector

Zscaler App Connectors provide the secure authenticated interface between a server and the ZPA cloud. App Connectors are deployed on-premises in datacenters or cloud environments to provide access to a customer's internal or 3rd Party resources. There are three potential App Connector deployment models that are relevant to delivery of this service. Each of the three models is based on: the Zscaler design best practice recommendation to place an App Connector as close as possible to the application(s) for which it controls access; and the fact that EFA customers will generally need to access applications which they host, or which are hosted by DOJ or a 3rd Party. These deployment models are defined in Table 1, which provides a summary description of the use case where the deployment model is relevant and depicts the organization with primary responsibility for O&M support of the App Connector(s).

*Table 1: Summary of Zscaler App Connector Deployment Options and Associated Responsibilities*

| Option | Description | Responsibility |
|---|---|---|
| DOJ-hosted | These are used to provide access to internal DOJ applications, which support other DOJ shared services when the EFA customer subscribes to these other shared services. | DOJ |
| EFA-hosted | These are used to provide access to EFA internal applications hosted in EFA datacenters or offices. | EFA |
| 3rd Party-hosted | These are used to provide access to internal applications hosted by the 3rd party in cases where the EFA customer subscribes to shared services or interconnects to systems hosted by the 3rd party. | 3rd Party Organization |

For all these models, the DOJ Engineering Team will support the deployment of the App Connectors, monitor the health of App Connectors, and perform updates to the App Connector software. However, for EFA-hosted and 3rd Party-hosted App Connectors, DOJ will not be responsible for maintaining the configuration and/or updates for the underlying Operating System where the App Connector software is installed, nor the surrounding infrastructure and connectivity which are outside the scope of DOJ's control. However, DOJ will work with the customer and 3rd Party organization as necessary to resolve issues with App Connectors even if primary responsibility for restoring functionality is outside of DOJ's control.

### 3.1.3 Zscaler Management Platform

The Zscaler Management Platform is the management console for the service, which provides management of the access control policies and security features implemented to provide real-time protection and visibility for customer systems. The Zscaler Management Platform consists of the features described in the following subsections.

#### *3.1.3.1 Zscaler Internet Access (ZIA)*

ZIA provides a full security stack as a service via globally distributed cloud infrastructure, which brings the internet gateway closer to the user for a faster experience. Protections for all offices or users can be easily scaled regardless of location while minimizing network and appliance infrastructure. The security stack provided through ZIA includes key features such as:

- Web proxy with native SSL inspection
- Intrusion Prevention System (IPS)
- Malware sandbox
- Data Loss Prevention (DLP)
- Cloud-based firewall and traffic control

#### *3.1.3.2 Zscaler Private Access (ZPA)*

ZPA is the world's most deployed ZTNA platform, applying the principles of least privilege to give users secure, direct connectivity to private applications running on-prem or in the public cloud while eliminating unauthorized access and lateral movement. As a cloud native service built on a holistic security service edge (SSE) framework, ZPA is designed to replace Virtual Private Networks (VPNs) and other legacy remote access technologies.

#### *3.1.3.1 Zscaler Digital Experience (ZDX) – optional*

ZDX Flow

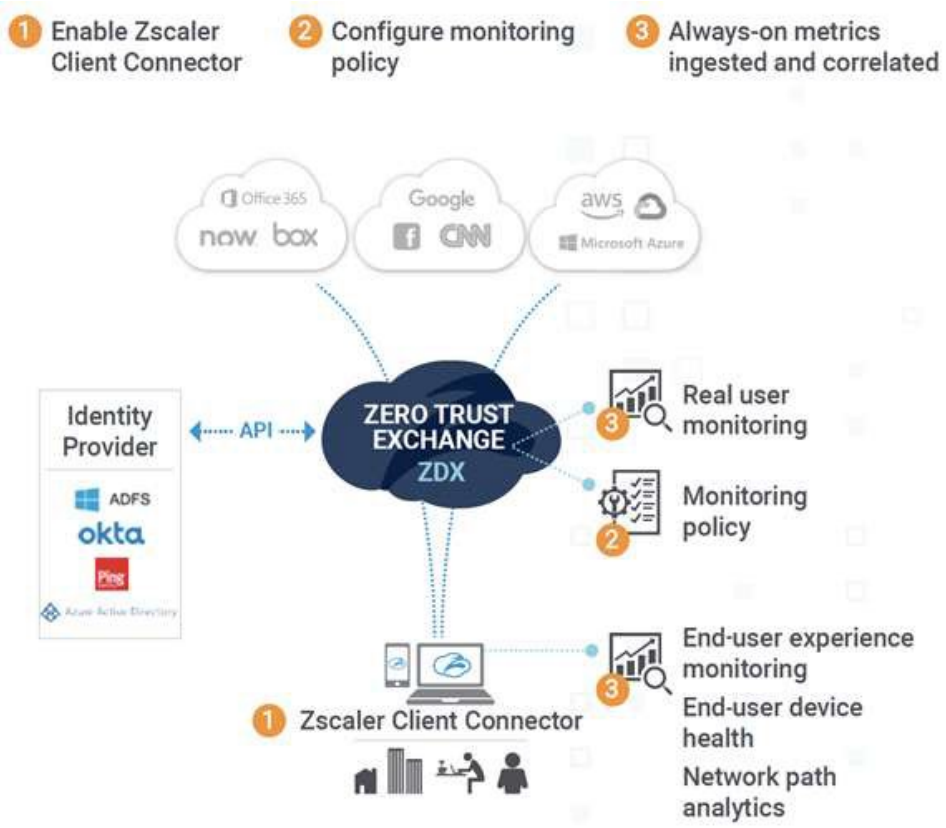



*Figure 1: ZDX Flow*

## 3.2 Technical Architecture

JETS is deployed in a multi-tenant architecture in order to ensure consistent and effective management as well as segregation of EFA customer tenants, configurations, and data. This is achieved through the use of a Partner Administration Tenant with child tenants for individual EFA customers. This architecture is shown in Figure 1.

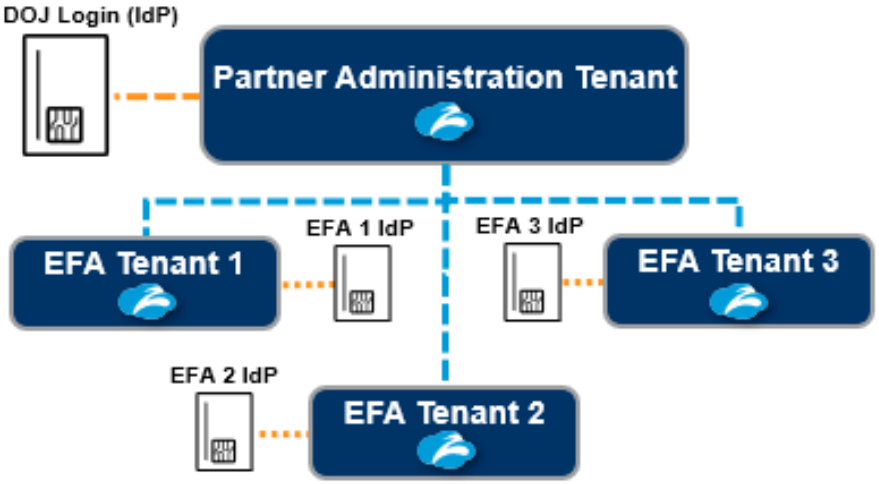



*Figure 2: Multi-Tenant JETS Architecture*

### 3.2.1 Partner Administration Tenant

The DOJ Partner Administration Tenant is a tenant used to simplify access and management to individual EFA Tenants. DOJ's Partner Administration Tenant configured to authenticate users on the DOJ Engineering Team through the DOJ Login Identity Provider (IdP), which is Okta. Upon request by DOJ Engineering Team, Zscaler will provision a new EFA Tenant under the DOJ's Partner Administration Tenant. After the tenant is provisioned by Zscaler, DOJ Engineering Team will change the default admin account password and store the admin account password securely. DOJ Engineering Team conducts initial configurations as necessary.

However, if an EFA customer has already implemented Zscaler and is attempting to leverage the JETS to take over day-to-day O&M, work will need to be coordinated to ensure the integration is performed correctly. DOJ Engineering Team will perform a review of the EFA's existing tenant configurations, identify any issue/gaps/concerns, and recommended changes to align to DOJ's standards.

Ultimately, the relationship established between tenants allows the DOJ Engineering Team to authenticate to the Partner Tenant, and then leverage the ability to federate their access into EFA

Tenants. This federated access gives DOJ Engineers the ability to manage EFAs via the Partner Administration Tenant.

### 3.2.2 EFA Tenant

Within the EFA Tenant, the DOJ Engineering Team will be responsible for the management of the root administrator account(s) and roles implemented for the tenant management portals. The DOJ Engineering Team will work with the EFA to implement the initial configuration of their IdP, provide O&M support for the configuration within the EFA Tenant, and will perform troubleshooting as required. The EFA maintains responsibility for the ongoing O&M of the IdP solution as well as the account management process for EFA users who will ultimately be provisioned within the IdP and thereby granted use of the JETS. The EFA customer will be provided access to the EFA Tenant portals through read-only accounts. The read-only access will allow designated users to view all features in the tenant, run reports, and monitor the status of the tenant in the EFA dashboard.

## 3.3 Out of Scope

JETS does not include the following services unless they have also specifically been provisioned by the EFA:

- Security monitoring services
- Cyber threat hunting
- Internet access as typically provided by an Internet Service Provider (ISP)

# 4 Service Description

## 4.1 Configuration and Change Management

All routine maintenance performed by the DOJ Engineering Team will be communicated to the customer. Changes expected to have customer impacts will be communicated in advance and confined to defined maintenance windows.

The DOJ Engineering Team will be responsible for implementing all configuration changes to the EFA Tenant managed through the JETS which includes but is not limited to:

- URL and Application block/allow lists
- Firewall settings
- DNS settings
- Sandboxing
- DLP
- File type controls
- Nanolog Streaming Service (NSS) configuration
- Log Streaming Service (LSS) configuration
- Application and Application Segment configuration
- Access policies
- Sever and Server Group configuration

Configuration changes are expected to adhere to EFA customer internal Configuration and Change Management policies and procedures as well as those which govern service management of the JETS. At a summary level, this means that changes requested by the EFA are expected to go through the Change Control Board (CCB) within the EFA's internal organization before being submitted to DOJ as a Customer Support Request (CSR) for implementation. DOJ's services adhere to International Standards Organization (ISO) 20000 (20K) and 27000 (27K) processes and procedures, which are beyond the scope of this document. However, it's expected that a complete and approved CSR from the customer will be submitted to DOJ via the workflow depicted in Section 5.2 for processing with minimal changes or adjustments.

## 4.2 Health and Performance Monitoring

DOJ is responsible for performing Health and Performance Monitoring for various aspects of JETS. However, certain aspects of monitoring, particularly where health or performance issues must be investigated, will require support and collaboration from the EFA customer.

DOJ will perform ongoing monitoring of the health and performance of the JETS. This includes monitoring of all underlying technical components of the service. The customer is able to view limited health information via their read-only access to their EFA Tenant portals, but DOJ maintains responsibility for performing monitoring of service health at this level as well and is ultimately responsible for reporting health issues to the customer in a timely manner.

The EFA customer will be responsible for:

- Ongoing health monitoring for EFA-hosted App Connectors
- Ongoing health monitoring for platform and network infrastructure under their control which support EFA-hosted App Connectors
- Troubleshooting health issues in conjunction with the DOJ Engineering Team by running Zscaler Analyzer or visiting https://ip.zscaler.com, which are client troubleshooting tools

DOJ Engineering will regularly provide input and recommendations based on current configurations, utilization patterns, follow-on investigations related to incident after action reports, and other sources where there are possible improvements to be made to the health and performance of the system. This ongoing optimization is a feature of JETS, which is covered in Section 4.5.

## 4.3 Security Monitoring and Protection

As a customer of JETS, customer agencies will be integrated with certain security monitoring and protection capabilities. These security protections will enhance the organization's security posture and will provide EFA customers with the ability to achieve Federal compliance requirements.

### 4.3.1 Cloud Log Aggregation Warehouse (CLAW)

CLAW is a CISA-deployed architecture for the collection and aggregation of security telemetry data from agencies using commercial CSP services. While agency security telemetry data currently is aggregated on-premises at CISA, CLAW is deployed in the cloud to aggregate agency security data that originate in the cloud. CLAW presents a functional, module-based architecture to ingest, store, and analyze security and sensor data from agencies. It is geared toward enabling secure and efficient methods to process cloud security data in a manner that offers CISA a similar level of situational awareness provided by current EINSTEIN on-premises deployments. The JETS includes integration with DHS CLAW.

### 4.3.2 Domain Name System (DNS) Sink-holing/Protective DNS

DHS provides a DNS protection through EINSTEIN 3 Accelerated (E3A), which is a sink-holing capability that blocks access to malicious infrastructure by overriding public DNS records identified as harmful. As a result, endpoints will be prevented from accessing malicious sites by Fully Qualified Domain Name (FQDN). For EFAs that do not have native DNS sink-holing capabilities, DNS sink-holing may provided via DOJ-hosted DNS servers, which forwards traffic from EFA endpoints in scope for this service to E3A. E3A then rewrites DNS responses as necessary based on CTI collected and managed by DHS, and those responses are then returned to the endpoint through DOJ's infrastructure.

**NOTE:** *In the future, E3A will be replaced by Protective DNS, which is a similar but improved capability. DOJ will handle this transition once Protective DNS is available and tested.*

### 4.3.3 JSOC Integration

Customers of JETS are not required to also subscribe to DOJ's SOCaaS. However, for those that do subscribe, all logging data from the EFA Tenant will be captured and leveraged for detection and analysis, threat hunting, and other services provided by DOJ's SOCaaS. If the EFA customer does not also subscribe to DOJ's SOCaaS, then the DOJ Engineering Team will work with the customer to ensure this log data is configured to be fed to the customer agency Security Information and Event Management (SIEM) platform.

### 4.3.4 Web Content Filtering (JSOC Blocklist)

If the EFA customer is also a subscriber to DOJ's SOCaaS, they will also be protected by DOJ's Blocklist, which is a curated CTI feed leveraging open and classified sources. The DOJ blocklist consists of a customer URL category that is added applied to a role and is updated in near real time and currently consists of over 3,000+ IP/URL.

DOJ will also maintain custom content filtering configurations based on EFA customer requirements. This will include custom block and allow-listing as needed.

## 4.4 Log Collection

DOJ is responsible for ensuring that logs for the EFA Tenant under the JETS are configured to be delivered to the appropriate destination given the SIEM in use by the EFA customer. For customers who also subscribe to DOJ's SOCaaS, DOJ transparently configures and ensures logs are fed into the SIEM leveraged by DOJ for delivery of that service. For customers using an internal SIEM and SOC or a SIEM provided by a 3rd party SOC, DOJ will work with the customer to perform the technical integration necessary. This includes both NSS and LSS logging. Logs from the NSS and LSS VM are sent to a Splunk Log Forwarder, which then sends the logs into Splunk Cloud.  This architecture is shown in Figure 3.

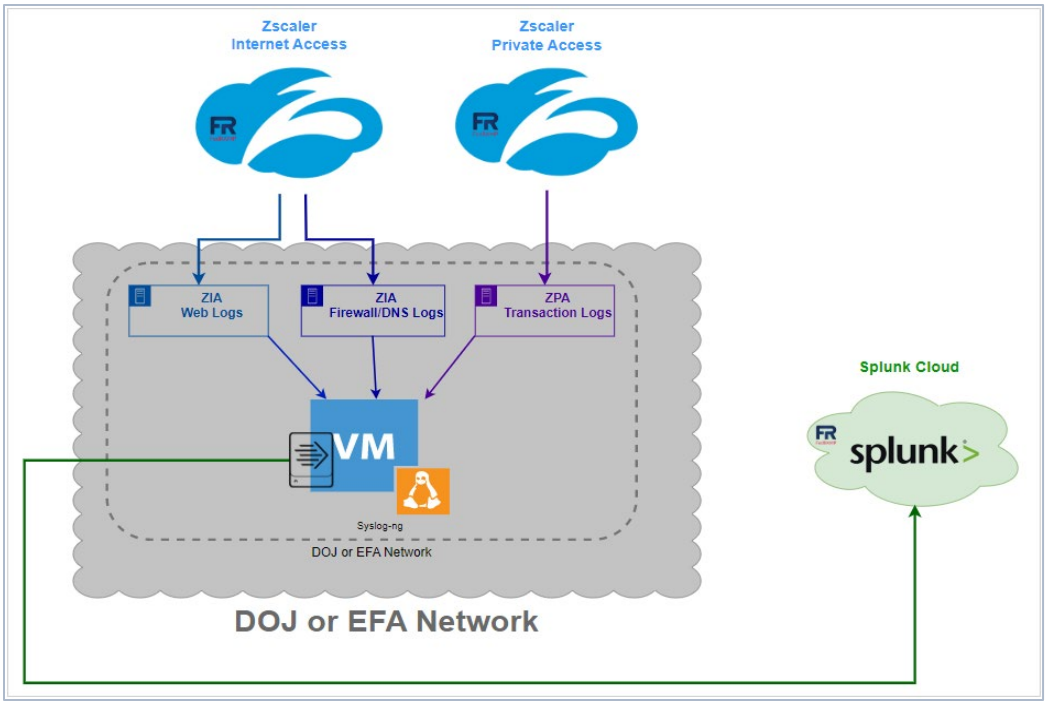



*Figure 3: LSS/NSS Architecture*

## 4.5 Optimization

DOJ will perform periodic reviews of ongoing performance, Zscaler insight reports, custom configurations, and will perform evaluation of services provided. Based on a thorough review, DOJ Engineering will make recommendations for optimization. Optimization can include, but not limited to, the following:

- ZIA
  - Policy review
  - Partner integrations
  - URL Categorization/Recategorization
  - Granular controls to reduce false positive alerts
  - New Service and Features
- ZPA
  - Application Segment refinement
  - Additional App Connectors
  - Additional App Connectors for Cloud hosted services (AWS/Azure)
  - Access/Timeout Policy refinement
  - Additional/Consolidation of Groups
  - New Service and Features
- ZCC

- Client updates
- App/Forwarding profile refinement
- Quarantine or remove noncompliant devices

DOJ will work with customers to review bandwidth utilization and make recommendations based on traffic trends.

The EFA customer is responsible for initiating changes based on the recommendations provided by the DOJ Engineering Team.

# 5 Use of Service

This section provides a high-level description of the standard process for EFA customers to report issues and make requests for support. **Note:** This process covers services that are post-deployment and are in production status.

## 5.1 End User Support

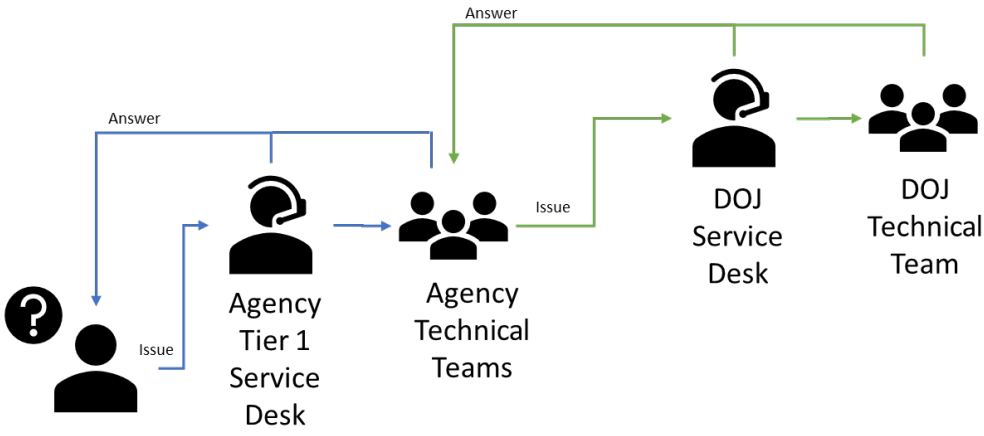
End user or deskside support is the sole responsibility of the EFA customer. Agency customers will provide their users with support for troubleshooting Zscaler Client and host-based issues.

## 5.2 Managed Service Support

### 5.2.1 Support Workflow

EFA customers can engage support by submitting a Customer Support Request (CSR) to the DOJ Service Desk. The technical support workflow is depicted in Figure 2.

*Figure 4: Customer Support Workflow*




### 5.2.2 Contacting Support

CSRs should be submitted by the customer agency via email but they can also be created via phone. Email and phone points of contact are:

- Email
  - To: DOJ.Service.Desk@usdoj.gov
  - Cc: DOJ.SharedServicesEngineering@usdoj.gov
- Phone: 202.616.7100

### 5.2.3 Escalation

CSRs may be escalated if the situation warrants it. The point of contact (POC) who submitted the CSR can contact DOJ Services Desk via email or phone to request the CSR be expedited. If requesting via email, please include the verbiage to “expedite” the request and a brief

explanation of the need to have the CSR expedited. If requesting via phone, please make sure you have your CSR number available to be referenced. The DOJ Service Desk agent will ask for your CSR number and the explanation supporting the need to escalate the CSR.

**NOTE:** *If the CSR is due to a critical issue and/or service outage, please call the service desk and request immediate support. The DOJ Service Desk has playbooks to execute to contact the DOJ Engineering Team to engage in critical issue resolution and/or service restoration.*

### 5.2.4 Hours of Operation

Standard business hours are defined as 8am to 5pm Eastern Standard Time (EST) Monday through Friday excluding Federal holidays. The DOJ Engineering Team will follow up on all CSRs submitted during normal business hours within one hour of DOJ Service Desk creating a ticket number. All CSRs submitted after-hours will be handled the next business day unless they are critical issues and/or service outages that are escalated using methods provided in Section 5.2.3.

### 5.2.5 Common Customer Support Request Use Cases

The following are common issues or requests for which the EFA would submit a CSR to DOJ for support.

- Applications unable to connect to the internet
- URL blocked due to incorrect categorization in Zscaler
- URL blocked due to incorrect categorization in Zscaler Security Database
- Service status error messages in ZCC
- Authentication error codes
- Unable to reach application through ZPA
- Add new applications segments

After the EFA sends an email or calls the DOJ Service Desk and DOJ Engineering Team is notified of the issue or request, DOJ will aim to resolve a non-emergency CSR within 24 hours. The resolution time is dependent on a number of factors including but not limited to the time of day the request was received, time for DOJ Service Desk to assign ticket to DOJ Engineering Team, quality of information provided in the CSR, and complexity of the CSR. For critical issues requiring immediate support, the EFA may follow the escalation procedure in Section 5.2.3.

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

This section provides a detailed breakout of the major roles and responsibilities related to JETS. The RASCI model is used to delineate lines of responsibility related to the service.

- **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 2 depicts important activities related to JETS including the role different parties play in relation to each. The following roles, which were introduced in Section, are identified in the matrix by abbreviation:

- DOJ Service Owner (SO)
- 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)

*Table 2: JETS RASCI Matrix*

| Activity | DOJ | | | | EFA | | |
|---|---|---|---|---|---|---|---|
| | SO | CSM | DET | JSD | CASL | ETT | ESD |
| EFA Tenant account management | A | S | R | | C | I | |
| EFA 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 | | S | S | | A | R | I |
| Implement initial policy and configuration settings | | S | A,R | | A | C,S,I | |
| Installation, configuration, and O&M support of App Connectors for DOJ-hosted applications | | S | A,R | | I | I | |
| Installation, configuration, and O&M support of App Connectors for EFA-hosted applications | | S | C,S,I | | A | R | |
| Installation, configuration, and O&M support of App Connectors for 3rd party-hosted applications | | S | C,S,I | | A | S | |
| Configure and manage deployment for direct peering to cloud applications and internet | | S | A,R | | A | C,S | |
| Policy maintenance and tuning | | S | A,R | | | C,S,I | |

| Activity | DOJ | | | | EFA | | |
|---|---|---|---|---|---|---|---|
| | SO | CSM | DET | JSD | CASL | ETT | ESD |
| Refinement of policies and configuration settings | | S | A,R | | | C,S,I | |
| Conduct testing and validation of traffic flows and policies | | S | A,R | | | S,C | |
| Configure and maintain Application Programming Interface (API) with CISA CLAW for cloud telemetry data sharing | | S | A,R | | | | |
| Authorize and establish CLAW data sharing parameters with CISA | A | S | | | I | R | |
| Create, evaluate, and approve CRs through EFA CCB | | S | | | A | R | I |
| Submit EFA-approved CSRs to DOJ for implementation | | S | | I | | A,R | I |
| Intake, evaluate, and implement EFA CSRs | | S | A,R | I | | I | I |
| Troubleshoot end user issues (endpoint support such as general connectivity issues and Zscaler client connector) | | S | S | I | I | R* | I,S |
| Troubleshoot issues with Zscaler platform (Software as a Service) | | S | A,R | I | I | S,I | I |
| Customer support and issue management | A | S | R | I | I | S | I,S |
| Configure logging to SIEM | A | S | R | I | | | |
| Maintenance, health, and performance monitoring | A | S | R | I | I | I | |
| Assess and propose modernization and optimization recommendations | A | S | R | I | I | C | |

*DOJ will develop and share with ESD knowledge artifacts, such as vendor documentation and/or troubleshooting guide, etc, that can assist EFA Tier 1 help desk with triaging end user issues that may be Zscaler-related.