Prepare your organization's network for Displayforce SaaS Platform

DISPL Network Architecture

🔹 Overview

The Displayforce SaaS platform (by DISPL) is hosted in the cloud and accessed via domains ending in **.displayforce.ai** and **.displ.com**. To ensure stable and secure access to the platform, the following network configurations must be applied within your organization's infrastructure.

✅ Required Network Access

Ensure your corporate network allows outbound access to the following domains and IP addresses:

Purpose	Domains / Hostnames	Ports	Notes
Core platform access	*.displayforce.ai, *.displ.com	443	HTTPS
Authorization and login	id.displayforce.ai	443	HTTPS
API access	api.displayforce.ai	443	HTTPS
Media and static content	storage.displayforce.ai	443	HTTPS

Additionally, ensure these IP addresses are reachable:

- **20.56.93.184**
- **108.141.167.74**

⚠️ These IPs are associated with DSPL platform infrastructure. DNS resolution should still be used as primary lookup; IPs can change as part of cloud infrastructure scaling.

🛡️ Certificate Validation and TLS Support

Access to the DSPL platform is secured via HTTPS. To validate the platform's TLS certificates, client devices and services in your network must be able to reach external Certificate Authorities (CAs). The primary CA for DSPL services is **GlobalSign**.

Make sure the following domains are accessible:

Purpose	Domains	Ports
OCSP (certificate status)	ocsp.globalsign.com	80, 443
CRL (certificate revocation)	crl.globalsign.com	80, 443
Intermediate/root certs	secure.globalsign.com	443

DNS must be able to resolve these domains, and firewalls must not block the HTTP/S traffic required for certificate chain validation.

🔍 About SSL Inspection and DPI

If your organization uses **SSL inspection**, **deep packet inspection (DPI)**, or **TLS termination via proxy**, the following must be ensured:

- The internal CA (used for inspection) must be trusted by all clients.
- Alternatively, disable TLS interception for:
  - *.displayforce.ai
  - *.displ.com
  - *.globalsign.com

Failure to properly handle certificate chains may lead to inability to access the DSPL platform due to failed TLS handshakes.

🌐 DNS Considerations

DNS resolution must be functional for all mentioned domains. The recommended setup:

- Allow DNS lookups for *.displayforce.ai, *.displ.com, and GlobalSign-related domains.
- Avoid blocking or filtering public DNS traffic that could interfere with name resolution.
