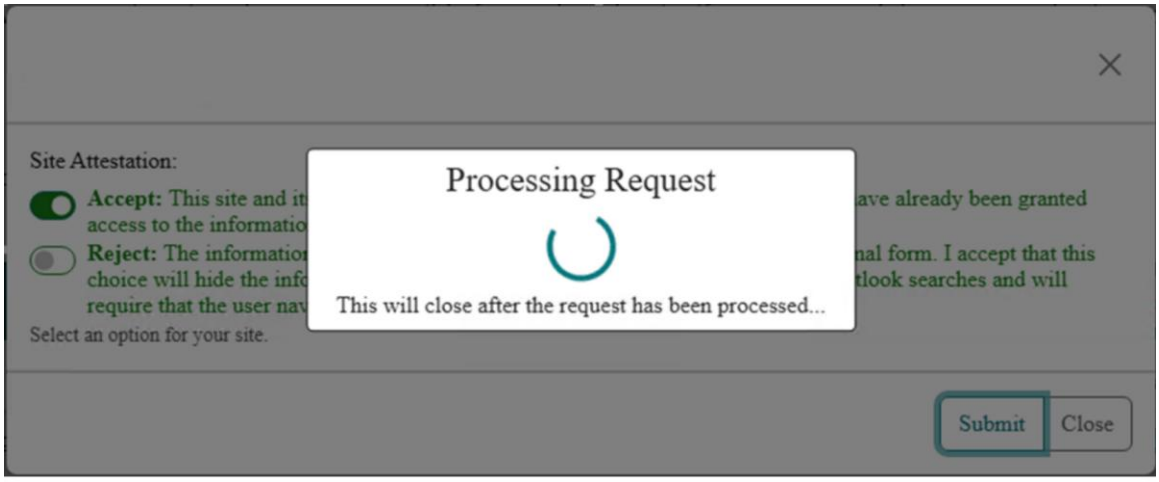
# SPARK Runbook
# Function App Custom Domain + PKI Certificate + CORS Update
# (Proxy “Wheel of Doom” Fix)

*Scope: SPARK Attestation Portal (SPFx) → Azure Function App endpoints impacted by enterprise proxies that block default *.azurewebsites.* hostnames.*



# 1. Overview

This runbook documents the field fix used during the DISA SPARK deployment to address a proxy-driven client failure where the SPARK attestation submit action “spins” indefinitely (the “Wheel of Doom”). The fix moves SPARK’s browser-to-Function-App traffic from the default Azure Functions hostname to an organization-owned custom domain, bound to a PKI-issued TLS certificate, and updates CORS + the SPFx web part to use the new origin.

## 1.1 Symptom

- Users can load the SPARK Attestation Portal but when they submit an attestation action, the UI hangs/spins (no completion).
- In affected networks, enterprise proxy policy blocks calls to the Function App default hostname (e.g., func-*.azurewebsites.us / .net), preventing required POST/GET calls.

## 1.2 Targeted outcome

- Browser traffic is sent to a Function App hostname within the customer-controlled domain space (CNAME).
- TLS is terminated with an approved PKI certificate (SAN includes the custom hostname).
- Function App CORS allows the new custom origin(s).
- SPARK Attestation Portal web part is configured to call the Function App via the custom domain.

## 2. Preconditions & access

### 2.1 Required access / roles

- Ability to manage Azure Function App custom domains and TLS bindings in the target subscription/resource group.
- Ability to create/validate DNS records in the customer domain space (or coordinate with the customer DNS authority).
- Ability to request and receive a PKI-issued certificate for the custom hostname (including private key).

### 2.2 Required inputs

- Custom hostname to use for the Function App (example used at DISA: spark-disa.apps.mil).
- PKI certificate with SAN matching the custom hostname and exportable private key (PFX).
- List of SPARK Function App endpoints used by the Attestation Portal that must work over the new hostname (at least: fx-spark-getsparksites and fx-spark-updatesparksites).

### 2.3 Notes from the field

- The custom domain does not need to become the “primary” domain for the Function App; it must be bound and listened on via CNAME, and the SPFx client must be updated to use that hostname.
- At DISA, using the certificate directly from Key Vault did not work in practice due to managed identity access limitations; the certificate was instead imported into the Function App certificate store (“shared resources”) and bound there.

## 3. Procedure

### 3.1 Add / verify the Function App custom domain (CNAME)

- Begin by attempting to add a custom domain name to the function app; Azure will provide verification records (observed: CNAME + TXT) that must be added in DNS. You will not be able to complete this step yet. Rather you must add the CNAME record and the TXT record to your local DNS.
- Create a DNS CNAME record in the customer-controlled domain space for the desired hostname, pointing to the Function App default hostname.
  - Example: spark.mydomain.mil
- Add the provided TXT record to the customer-controlled domain space as well.
- Return to Azure and complete Azure domain ownership verification as prompted; The Azure provided verification records (observed: CNAME + TXT) should now turn green.
- Finish the custom-domain mapping so the Function App accepts traffic for the custom hostname.

### 3.2 Obtain PKI certificate and bind TLS to the custom domain

- Generate a certificate request (CSR). Some organizations utilize Azure Key Vault (field method used).
- Have the authorized PKI agent issue a certificate for the custom hostname.
- Optionally, import the issued certificate (with private key) into Key Vault.
- Optionally, export the certificate WITH private key (PFX) from Key Vault.
- Import the PFX certificate into the Function App certificate store (“shared resources”).
- Bind the custom domain hostname to the imported certificate so HTTPS uses the PKI certificate.

### 3.3 Update Function App CORS

- Add the custom hostname as an allowed CORS origin in the Function App CORS configuration.

### 3.4 Update SPARK Attestation Portal (SPFx web part) configuration

- Update the SPARK Attestation Portal web part configuration to use the Function App base URL with the custom hostname instead of the default *.azurewebsites.* hostname.
  - Example: spark.mydomain.mil
- Field note: the Function App URL is set in web part properties; no code changes were required for the hostname swap in that implementation.

## 4. Verification & evidence collection

### 4.1 Browser developer tools validation

- Open browser developer tools (Network tab) while performing an attestation submit action.
- Confirm SPFx calls to the custom hostname return HTTP 200.
- Field validation explicitly observed HTTP 200 for at least: fx-spark-getsparksites and fx-spark-updatesparksites after the change.

### 4.2 Operational confirmation

- Collect initial user reports from affected orgs/segments that previously observed the spin/hang behavior.
- Confirm successful attestations across representative org networks (proxy paths).
- Continue monitoring for regressions after rollout.

### 4.3 Artifacts / screenshots referenced during implementation

- Default domain capture screenshots were shared in the implementation thread for reference.
- A “Processing Wheel of Doom” screenshot was also referenced during troubleshooting.

## 5. Rollback & troubleshooting

### 5.1 Rollback

- Revert the SPFx web part configuration to the prior Function App base URL (default hostname).
- Remove the custom origin(s) from Function App CORS if required by policy.
- Unbind or remove the custom domain and certificate binding if required (note: coordinate with DNS owners before removing DNS records).

### 5.2 Common failure points (observed or implied by field notes)

- DNS ownership verification not completed (missing TXT/CNAME verification record).
- Certificate SAN mismatch (custom hostname not included).
- Certificate cannot be used via Key Vault in the target environment due to managed identity access constraints (workaround: import into Function App certificate store).
- CORS missing the custom hostname origin (include both with and without trailing slash if required by the client behavior).
- SPFx still pointing to the old hostname in web part properties.