Enhanced Endpoint: Migration Guidelines

What is the enhanced endpoint?

Customers using the OPEN Platform can now benefit from a new and enhanced endpoint, providing significantly quicker failovers between our data centers and other stability improvements. Customers are strongly encouraged to upgrade as soon as possible to benefit from the improvements offered.

Pre-migration validation steps

Prior to switching to the enhanced endpoint, customers will have to complete the three (3) following validation steps:

1) Remove restrictions on connectivity to outbound IP addresses

Organizations restricting outbound connectivity to specific IP addresses or ranges (commonly referred to as 'IP whitelisting') will be required to remove these restrictions for all application servers connecting to the new enhanced endpoint.

This only applies to outbound connections from your systems to the OPEN Platform; inbound connectivity from the OPEN Platform to your organization (such as webhooks) will require no changes.

2) Validate cipher suites

Some TLS v1.2 cipher suites that are supported by the legacy endpoint are not supported by the enhanced endpoint. Customers will be required to review the list of cipher suites supported by the enhanced endpoint to ensure they support at least one of the listed cipher suites.

Note that there are no changes to supported TLS v1.3 cipher suites.

3) Check certificate

The enhanced endpoint uses a different certificate than the one used by the legacy endpoint. Customers should validate that systems connecting to the new endpoint are set up with the root certificate that signed our server certificate. Our server certificate is signed by Let's Encrypt; further information on this certificate is available here.

Note that the root certificate for Let's Encrypt was recently changed; see this article for more information.

Additionally, note that certificates will be updated on a quarterly basis going forward, with a maximum certificate length of 90 days. This change protects both your organization and the Open Payment Platform from the security risks associated with long-lived certificates. Any customers that require certificate pinning will be required to ensure that they update their certificates on this more regular schedule.

Targeting the enhanced endpoint

Once you have completed the validation steps listed above, you can quickly and easily switch over by targeting the new endpoint domains shown below.

Environment	Current Domain (Legacy Endpoint)	New Domain (Enhanced Endpoint)
Production	https://oppwa.com/	https://eu-prod.oppwa.com/
Customer Test (Staging)	https://test.oppwa.com/	https://eu-test.oppwa.com/