# Universal Routing Reference

## URS REST API Security Considerations and Basic Hardening Steps

5/3/2025

# URS REST API Security Considerations and Basic Hardening Steps

In addition to the information provided in the Security section, on page number 59 of the Universal Routing 8.1 Deployment Guide, the following recommendation is to be considered for the REST API.

> **Important**
>
> The REST API is an internal API and should be appropriately protected because it does not support common security headers in HTTP and does not have built in protections for features normally implemented in firewalls (such as DoS). The REST API is not intended to be exposed to untrusted parties.

It is possible that through the REST API provided by URS, sensitive data stored in strategies processing interactions might be accessed, and URS forced to perform resource-consuming activities (DoS attack).

Major security limitations of the RESTful API implementation are:

- No ability to provision HTTP responses with security headers of any kind.
- No firewall features of any kind (rate throttling, etc.).

Given the above, securing access to the URS web API is important.

## Hardening Steps for URS REST API

You can perform the following steps to harden the URS REST API:

1. Provision TLS/SSL transport-level security for communications via HTTP and SOAP ports. This is configured in the Server Info tab of the router application as described in the Genesys Security Deployment Guide.
2. Configure the firewall to allow connections to URS ports only from 100% trusted zones with no exceptions. This is very important because, access to the URS HTTP port means access to all features of the URS REST API.