CHAPTER 5

Introduction to ERS APIs

Prerequisites for Using the External RESTful Services API Calls

You must fulfill the following prerequisites before invoking an External RESTful Services API call:

- You must have enabled External RESTful Services from the GUI.
- You must have External RESTful Services Admin privileges.

You can use any REST client like JAVA, curl linux command, python or any other client to invoke External RESTful Services API calls.

External RESTful Services SDK

You can use the External RESTful Services SDK to start building your own tools. You can access the External RESTful Services SDK from the following URL: `https://<ISE-ADMIN-NODE>:9060/ers/sdk`.

External RESTful Services SDK can be accessed by the External RESTful Services Admin users only. The SDK consists the following components:

- Quick reference API documentation
- Complete list of all available API operations
- Schema files available for download
- Sample application in Java available for download
- Use cases in curl script format
- Use cases in python script format
- Instructions on using Chrome Postman

The following APIs are available in the SDK:

- Certificate template API
- Clear threats and vulnerabilities API
- Egress matrix cell API
- Endpoint API
- Endpoint certificate API
- Endpoints identity group API
- Guest location API

- Guest SMTP notification configuration API
- Guest SSID API
- Guest type API
- Guest user API
- Hotspot portal API
- IP-to-SGT mapping API
- IP-to-SGT mapping group API
- ISE service information API
- Identity group API
- Identity sequence API
- Internal user API
- My device portal API
- Native supplicant profile API
- Network device API
- Network device group API
- Node details API
- PSN node details with RADIUS service
- Portal API
- Portal theme API
- Profiler profile API
- SMS server API
- SXP connection API
- SXP local binding API
- SXP VPN API
- Security group API
- Security group ACL (SGACL) API
- Self registered portal API
- Sponsor group API
- Sponsor group member API
- Sponsor portal API
- Sponsored guest portal API

External RESTful Services API Authentication and Authorization

The External RESTful Services APIs are based on HTTPS protocol and REST methodology and uses port 9060.

The External RESTful Services APIs support basic authentication. The authentication credentials are encrypted and are part of the request header.

The ISE administrator must assign special privileges to a user to perform operations using the External RESTful Services APIs.

To perform operations using the External RESTful Services APIs (except for the Guest API), the users must be assigned to one of the following Admin Groups and must be authenticated against the credentials stored in the Cisco ISE internal database (internal admin users):

- External RESTful Services Admin—Full access to all ERS APIs (GET, POST, DELETE, PUT). This user can Create, Read, Update, and Delete ERS API requests.
- External RESTful Services Operator—Read Only access (GET request only).

If you do not have the required permissions and still try to perform operations using the External RESTful Services APIs, you will receive an error response.