



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

API Reference

Authentication

Authentication

Contents

- [1 Authentication](#)
 - [1.1 Configuration](#)
 - [1.2 Basic Authentication](#)

The Web Engagement History REST API supports the following authentication scheme:

- Basic HTTP Authentication (see <http://www.ietf.org/rfc/rfc2617.txt>).

⚠ HTTP authentication should be used with Secured HTTP communication (HTTPS).

Configuration

The REST API security is configured in the **security** section of the Web Engagement Backend Server application. The following configuration options are mandatory to enable authentication:

- **auth-scheme**
- **user-id**
- **password**

Note: If authentication is used, every REST API client must support that authentication type and the clients must know the authentication credentials. You must configure authentication for Interaction Workspace (see **Configure Authentication** in the Interaction Workspace Plug-in deployment). If your SCXML strategies use the REST interface, you must also add your authentication credentials (see **Configure Authentication in the default strategy**).

Basic Authentication

This authentication scheme passes unencrypted credentials, so it is unsafe unless you use a secured connection (HTTPS).