SAMSUNG Knox
Documentation

Home / Knox Cloud Authentication / API reference /

Knox Cloud Authentication API reference v1.0

Overview | Tutorial

Knox Cloud Authentication Servers

Region	Server	
EU	https://eu-kcs-api.samsungknox.com	
US	https://us-kcs-api.samsungknox.com	

Authentication

accesstoken

Receive the access token and sign it to authenticate your supported
    REST API requests.

REQUEST BODY SCHEMA: application/json
required

Public key and signed client identifier

base64EncodedStringPublicKey required	string Base64 encoded public key in the file downloaded from the Knox API Portal during first login
clientIdentifierJwt required	string

	Signed, unique Client identifier
`validityForAccessTokenInMinutes`	integer `[ 1 .. 30 ]` Default: `30` Time in minutes before the access token expires. If the value is not included, it will be set to 30 minutes. Any real number will be rounded to floor.

Responses

> **200**

successful operation

> **400**

Bad Request. Including Non-unique id on signed client identifier

> **403**

Authentication Fail. Signed client identifier expired

POST   /users/accesstoken

Request samples

Payload   Curl

Content type
application/json

Copy

```
{

    "base64EncodedStringPublicKey": "string",

    "clientIdentifierJwt": "string",

    "validityForAccessTokenInMinutes": 30

}
```

Response samples

200   400   403

Content type

application/json

Copy

```
{

    "accessToken": "string"

}
```

BACK TO GUIDE

Is this page helpful?

YES   No

KNOX DEVELOPER DOCUMENTATION

SUPPORT

SAMSUNG

PRIVACY POLICY | LEGAL