Authentication

Authentication is via an API Key and Secret. The API Key is our shared secret[1] and the Secret[2] is your password. API keys always begin with the letter **K** and secrets always begin with the letter **S**. Tokens are not used and revocation is immediate if credentials are ever compromised.

Passing Key and Secret

To authenticate, send your API key and secret in the HTTP headers of your request.

Key and Secret Set in Headers

```
POST / HTTP/1.1
Host: 0h.md;
Content-Type: application/json
x-api-key: K5QC27FSK4192W86JXM73ZZTTWT0F2Y4Z8P9D8MXB911CDTNNCCW0
x-api-secret: S42F818NB579A8AWP9ZXK0NYT6X7X9MWHD3QH885A26HM80DVQVXW
...
```

Your actual host endpoint is determined at the time you onboard.

IP Address

When you onboard OhMD will authorize you to call the APIs using your API Key from one IP address or a range of IP addresses **no larger than 64 addresses** (a /26 mask). If you need to change your IP address range, contact OhMD. **OhMD has no facility to allow roaming users.**

Reissuing Credentials

If your key is compromised or your secret lost, OhMD **must reissue both your key and secret**. Due to internal controls, OhMD cannot recover your secret.

mTLS

mTLS can be optionally enforced for organizations demanding extra security. If you choose to use mTLS, OhMD will issue you a certificate and you will be required to import our root certificate into your trust bundle. Contact OhMD for more information.

[1] If you also subscribe to one of our notification services, this is the same `x-api-key` that appears in POSTs from OhMD at your subscribed endpoint. Protect this key like you do your secret.
[2] The secret is hashed in OhMD's systems and not disclosed to staff. However, it is still a symmetrical share. For organizations wishing to employ true asymmetrical security, mTLS is optionally available.

Organizational Context

Your API key may allow access to more than one organization. For example, your team may develop solutions for more than one practice, each with a distinct EHR and distinct OhMD environment. In those cases, OhMD will authorize your keys for multiple organizations. This concept is often referred to as tenanting.

Because OhMD must isolate healthcare systems[3] data, you will send an `organizationIdentity` object in your request body **or** an `x-ohmd-organization-id` header to identify which organization you are referencing on a particular request. **Even if you will be calling the API for only one organization, the organization context is (usually) required.**

A few API functions do not require organizational context when context is not needed or would be contradictory. In these cases we only need to identify you as a requestor via API Key. For example, you are not required to set organizational context to list the organizations you have access to.

Organizational Context Not Required	Description
destinationsList	Retrieves a list of all destinations created by the requestor.
httpExchangeRetrieve	Retrieves details of an HTTP request and response exchange between you and OhMD.
httpExchangesList	Lists HTTP exchanges between you and OhMD for a given date range.
organizationsList	Lists identifiers for the organizations you can access.
organizationRetrieve	Retrieves details for a given organization.
phoneNumberRetrieve	Provides basic phone details, such as Caller ID for a phone number without providing EHR-sourced PII.
openApiRetrieve	Retrieves the OpenAPI document for a given API and version.
subscriptionsList	Retrieves a list of all subscriptions held by the requestor.

Though not technically part of the authentication phase, unless authorized to access the organization referenced, you will receive a 403 HTTP response code from your request.

[3] Each OhMD organization is a logical secure silo and no information is shared between the silos. We consider patients distinct at each organization even if they are the same person and share the same MRNs.

Setting Organizational Context In a Request

```
POST / HTTP/1.1
Host: 0h.md;
Content-Type: application/json
x-api-key: K5QC27FSK4192W86JXM73ZZTTWT0F2Y4Z8P9D8MXB911CDTNNCCW0
x-api-secret: S42F818NB579A8AWP9ZXK0NYT6X7X9MWHD3QH885A26HM80DVQVXW
x-ohmd-organization-id: c95d9252-6ee2-4a7c-8a95-44b4ed008814
. . .
```

Organizational Context Set Via Header

```
POST / HTTP/1.1
Host: 0h.md;
Content-Type: application/json
x-api-key: K5QC27FSK4192W86JXM73ZZTTWT0F2Y4Z8P9D8MXB911CDTNNCCW0
x-api-secret: S42F818NB579A8AWP9ZXK0NYT6X7X9MWHD3QH885A26HM80DVQVXW
. . .
{
 . .
  "organizationIdentity": {
       "identifier": {
       "id": "0188bf4c-bd7d-2b3f-a575-3fb0891195c7"
       }
  },
 . .
}
```

Organizational Context Set In Request Body

Issuing Credentials

Contact api@ohmd.com for credentials. We do not issue API credentials online.