API People Get v4

> This is the latest version of the APIs.

Contents:

Retrieve the platform account information for a user specified by userId.

Version: `v4`

Required Permissions

The authenticated user must be an admin.

> **NOTE:** Each request to the Trifacta® platform must include authentication credentials. See *API Authentication*.

Request

Request Type: `GET`

Endpoint:

```
/v4/people/<id>
```

where:

Parameter	Description
`<id>`	Internal identifier of the user to retrieve.

Request URI - Example:

```
/v4/people/4
```

Query parameter reference:

The following query parameters can be submitted with this endpoint:

Query Parameter	Data Type	Description
embed	string	Comma-separated list of objects to include part of the response.
includeDeleted	string	If set to `true`, response includes deleted objects.

The following parameters are supported specifically for this endpoint:

Query Parameter	Data Type	Description
preventNameFetch	string	If `true`, Name and emailAddress values are not returned.
uuid	string	Universal user identification value
workspaceId	string	Workspace identifier. This value is typically `1`.

For more information, see *API Common Query Parameters v4*.

Request Body:

Empty.

Response

Response Status Code - Success: `200 - OK`

Response Body Example:

```
{
    "id": 2,
    "email": "joe@example.com",
    "name": "Joe Guy",
    "ssoPrincipal": null,
    "hadoopPrincipal": null,
    "isAdmin": false,
    "isDisabled": false,
    "forcePasswordChange": false,
    "state": "active",
    "lastStateChange": null,
    "createdAt": "2019-02-12T09:04:52.073Z",
    "updatedAt": "2019-02-12T09:04:52.073Z",
    "outputHomeDir": "/trifacta/queryResults/joe@example.com",
    "fileUploadPath": "/trifacta/uploads",
    "lastLoginTime": "2019-05-19T10:53:11.014Z",
    "awsConfig": null
}
```

Reference

Property	Description
id	Internal user identifier
email	Email address (and loginId) for the user
name	Display name for the user
ssoPrincipal	(If SSO is enabled) Principal value of the user for single-sign on provider
hadoopPrincipal	(If secure impersonation is enabled) Hadoop principal value for the user, which determines permissions on the cluster
isAdmin	If `true`, the user account is an administrator account.
isDisabled	If `true`, the account is disabled.
forcePasswordChange	(if enabled) When set to `true`, the user must change the account password on next login.

state	Current state of the user account: • `active` - user is active and usable in the workspace • `hidden` - user account has been hidden from use.
lastStateChange	Timestamp for when the value of the `state` parameter was changed.
createdAt	Timestamp for when the user account was created
updatedAt	Timestamp for when the user account was last modified
outputHomeDir	Home directory where the user's generated results are written
fileUploadPath	Path on backend datastore where files uploaded from the user's desktop are stored for use as imported datasets.
lastLoginTime	Timestamp for when the user last logged in to the product.
awsConfig	(If AWS integration is enabled) Value contains the S3 credentials, default bucket, and any extra buckets to which the user has access

For more information on roles, see *Manage Users*.