API Overview

https://campus.barracuda.com/doc/93193014/

> The Barracuda Email Security Service API is a beta release and not yet generally available. The APIs in the beta endpoint are currently in preview and subject to change.

The Barracuda Email Security Service REST API provides the ability to interact with the Barracuda Email Security Service (ESS). This article gives a brief description of REST API and the API methods you can use to access your Barracuda Email Security Service.

Representational State Transfer (REST) is a stateless architecture that runs over HTTP. REST API is a simple web service API you can use to interact with Barracuda Email Security Service. For more information on REST API, visit http://en.wikipedia.org/wiki/Representational_state_transfer.

> The Barracuda Email Security Service API is currently only available for accounts in the US region.

Getting Started

You will need an active Barracuda Cloud Control account and your application registered in the Barracuda Token Service in order to receive the required Client ID and Client Secret. The Client Secret is used to sign and validate access tokens for authentication and to gain access to API endpoints.

For more details, review our Getting Started information.

Authorization Requirements

All endpoints will require an access token. Access tokens are generated from the token endpoint.

Use the API

The base URL is: `https://api.barracudanetworks.com/`

The following endpoints are available:

Accounts

- List accounts
- Get account

Domains

- List domains
- Get domain

Statistics

- Get statistics

Paging

Sometimes ESS API requests will return a large number of results. Rather than retrieve them all at once, which may affect your application's performance, you can use paging to retrieve the results in batches. For more information, see Paging.

Scopes

The scope constrains the endpoints to which a client has access, and whether a client has read or write access to an endpoint.

As a general rule, choose the most restrictive scope possible and avoid requesting scopes that your application does not need.

Available scopes:

Name	Description
ess:account:read	Allow read-only access to account information.

HTTP response codes

HTTP code	Status	Description

200	OK	The request was successful.
400	Bad Request	The request was invalid and/or not formed properly.
401	Unauthorized	There is a missing or incorrect API token in header.
403	Forbidden	The client did not have permission to access the requested resource.
404	Not Found	The URI requested is invalid or the resource requested does not exists.
406	Not Acceptable	The request specified an invalid format.
410	Gone	This resource is gone. Used to indicate that an API endpoint has been turned off.
429	Too Many Requests	Returned when a request cannot be served due to the application’s rate limit having been exhausted for the resource.
500	Internal Server Error	Something went wrong.
502	Bad Gateway	The service is down or being upgraded. Try again later.
503	Service Unavailable	The service is up, but overloaded with requests. Try again later.
504	Gateway Timeout	Servers are up, but the request couldn’t be serviced due to some failure within our stack. Try again later.