ByAllAccounts REST API
Advanced

Document Version:	RESTAPI-0.02-20240523
Document Issue Date:	May 23, 2024

Technical Support:	(866) 856-4951 Option 1
	Byallaccounts-support@morningstar.com
Web:	byallaccounts.morningstar.com

Table of Contents

About this document

This guide is in indented for those who want to access the ByAllAccounts^{SM} (BAA) data aggregation service with their own front end, using our REST API.

Information is included here for using session-based Single Sign-on (SSO) using our DataConnect API and Morningstar JWT SSO authentication using Morningstar Authentication.

Changes in this release

For information about changes in this and prior releases, refer to

Introduction

This guide is an expansion of our other REST API guide, which describes using our REST API with our ByAllAccounts Connect Account Linking component interface. For that guide, refer to https://www.byallaccounts.net/Manuals/DataConnect/BAA_REST_API.pdf.

This guide includes additional REST API endpoints and describes how the additional endpoints can be used to implement a complete User Interface for provisioning accounts for aggregation in the ByAllAccounts system, including:

- Provisioning the system to aggregate accounts available via OAUTH and LOGIN authentication mechanisms
- Maintaining account provisioning
- Adding more accounts to previously provisioned credentials
- Refreshing accounts

Endpoints described in both guides are those to:

- Delete an account from the system
- Monitor the status of asynchronous authentication or aggregation activities
- Request aggregation of accounts for an authenticated investor
- Retrieve credentials including account information when available
- Delete a credential and all associated accounts from the system
- Register a new user
- Retrieve profile data associated with a user ID
- Get a collection of all positions

Additional optional capabilities are supported by the REST API but not fully detailed here include:

- Requesting a new Financial Institution
- Manually entering Account Numbers for a Financial Institution that does not support Account Discovery

BAA Rest API URL

The BAA REST API is accessed by a URL invocation point. The following are for the production environment:

- BAA server   https://www.byallaccounts.net/api/v1
- With Morningstar Authentication   https://www.us-api.morningstar.com/aggapi/v1

Authentication

- Single Sign On (SSO) using the DataConnect API
  - Authenticate and obtain values for jsessionId and csrfToken by calling the DataConnect API SESSIONAUTHRQ request.
  - Use the jsessionId and csrfToken to invoke the REST API endpoint(s), sending the jsessionId in the URI and the csrfToken in a request header.
  - **Note**: The DataConnect Ultra SESSIONAUTHRQ operation has an optional <READ_ONLY> tag. When it is present, the REST API enforces read-only functionality for the Account Summary component. The purpose of the tag is to limit the functionality for an investor that self-authenticates in read-only mode or an administrator that is authenticated as an investor in read only mode. When the session is READ_ONLY, data cannot be modified even if the target investor has write permissions. Endpoints that manipulate data (such as DELETE accounts and POST new Person) are fully disabled. For details about SESSIONAUTHRQ, refer to the *DataConnect V4 Ultra User Guide* at http://www.byallaccounts.net/Manuals/DataConnect/DataConnect_V4_Ultra_User_Guide.PDF.
  - For more details about DataConnect SSO, refer to http://www.byallaccounts.net/Manuals/DataConnect/DataConnect_V4_Ultra_User_Guide.PDF.
- Single Sign On (SSO) using Morningstar Authentication
  - Implementations that use Morningstar Authentication for SSO use UIM JWT for authentication.
  - When using Morningstar Authentication, the request and response URIs will be Morningstar Authentication-based.
  - Morningstar Authentication issues a JSON web token (JWT) string, which then needs to be submitted to the REST API.
  - When UIM JWT is used to access the REST API, the other existing authentication tokens are not expected nor required. If others are used, there is a precedence order: 1) UIM JWT, 2) DataConnect SSO.
  - The UIM JWT is submitted to the API endpoints using the authorization header with the header value "Bearer *token-value*".
  - The JWT will expire after a pre-determined amount of time (the expiration time is set in the JWT itself by UIM). Requests with expired tokens will receive an error from the REST API indicating that the token has expired. The Morningstar Authentication can then be used to obtain a new token.

Request Headers

The following table contains information about headers that are applicable to all endpoints with exceptions noted. The X-CSRF-Token header is used only with certain forms of authentication.

Name	Mandatory	Description	Usage
Authorization	Yes*	Used to provide the UIM JWT value, prepended with "Bearer ". *Only used for UIM authentication.	Authorization
X-CSRF-Token	Yes*	CSRF Token for REST API. *Only used for SSO authentication model for endpoints requiring authentication.	Refer to Sample Code for SSO page 3.
Content-type	No*	Indicates media type of resource. *Only required for POST endpoints where content is expected in the POST body. When not required can be omitted or left empty.	application/json
Accept	Yes	Content type client is requesting. Supported type is application/json.	application/json

Sample Code for SSO using DataConnect

This example shows passing the credentials for the summary endpoint. In this example:

- var myCsrfToken = "AD30BFA5CD5B5450515A40ACAF852D66F7456D5432C4DA14"
- var myJsessionId = "CE2D0A6E7C60394ED1D9F46AFC02E632.s1a"
- The url shown as https://www.byallaccounts.net is for production environment

```
  var xhttpGetSummary = new XMLHttpRequest();
 .
 .
 .
function getSummaryState() {
    var href = "https://www.byallaccounts.net/api/v1/activities/summary;jsessionid=" + myJsessionId;
    xhttpGetSummary.open("GET", href, true);
    xhttpGetSummary.setRequestHeader("X-CSRF-TOKEN", myCsrfToken);
    xhttpGetSummary.setRequestHeader("Accept", "application/json");
    xhttpGetSummary.send();
}
```

Sample Code for JWT SSO using Morningstar Authentication

This code example assumes that JWT is being used for Morningstar Authentication

- To access the REST API, this example maps to the URL for the Morningstar Authentication server for PROD, which is https://www.us-api.morningstar.com/aggapi/v1
- Any URIs returned in the JSON REST API response bodies will also reference this base URL.

```
var xhttpGetSummary = new XMLHttpRequest();
.
.
.
function getSummaryState() {
   var href = "https://www.us-api.morningstar.com/aggapi/v1/activities/summary";
   xhttpGetSummary.open("GET", href, true);
   xhttpGetSummary.setRequestHeader("Authorization", "Bearer "+myUIMJWT);
   xhttpGetSummary.setRequestHeader("Accept", "application/json");
   xhttpGetSummary.send();
}
```

WORKFLOWS

This section describes critical workflows for provisioning and interacting with the aggregation system, which endpoints to use to accomplish those workflows, and important details about the endpoint payloads. This document does not cover workflows for adding Financial Institution Requests or for handling of Financial Institutions that do not support Account Discovery.

Selecting a Financial Institution

Adding new accounts to the aggregation system always begins with choosing a Financial Institution (FI). A Financial Institution supports either OAUTH or LOGIN authentication. The workflows and endpoints used will vary based on whether the FI is OAUTH or LOGIN.

Please refer to the following endpoint sections for information about listing FIs, determining if they are OAUTH or LOGIN, and the detailed credentialing requirements for LOGIN FIs. See:

-
-

You will not be able to add accounts at the following:

- OAUTH FIs where FI.configuredOAuth is false
- FIs where FI.licensed is false

Contact ByAllAccounts for assistance with enabling these FIs.

The following FI fields should be considered for incorporation into your UI:

- setupInstructions – Critical setup instructions that the user will need to successfully set up accounts at the FI.
- knownConnectionIssue – Short term issues with connectivity to this FI that may prevent the user from successfully connecting.
- knownConnectionIssueLongTerm - Long term issues with connectivity to this FI that may prevent the user from successfully connecting.

For sample FIs for testing different scenarios, refer to

Adding Credentials for an OAUTH FI

An FI that supports OAUTH authentication is very easy to get set up. Once accounts are added they will refresh automatically according to your firm's refresh configuration.

Step	Endpoint	Parameters	Notes
1. Add the credential	POST /api/v1/credentials		Prerequisite: The GET /api/v1/fis/{id} endpoint should show that configuredOAuth value for the FI is true. If it is not, then the next step will fail. Returns {credentialId} for next steps
2. Initiate the OAUTH authorization flow	POST /api/v1/credentials/{credentialId}/authenticate	startOauth:true	Returns {ticket} for next steps. Refer to Workflow error situations below.
3. Get initial setup info	GET/api/v1/authentications/{ticket}		Returns oauthMicrositeURL for next step
4. Launch the FIs OAUTH Microsite in a browser window			The user will complete the OAUTH authorization flow in that window and that will call back to the aggregation system server to complete.
5. Poll for completion of the user's OAUTH authorization flow (#4)	GET/api/v1/authentications/{ticket}		Wait for the operation to complete. Refer to Workflow error situations below.
6. Add authorized accounts to the system	POST /api/v1/credentials/{credentialId}/aggregate		Discovers, adds, and aggregates the accounts authorized by the user.

7. [Poll for completion of the aggregation]	GET /api/v1/aggregations/{ticket}		Optional step. Aggregation completes asynchronously.

Workflow error situations

Some of the workflow error situations replated to the table above include the following:

Related to Step	Error	How Detected	Recommended Action
#2	Unable to initiate the OAuth authorization flow	Error returned by step 2	Examine the detailed error type information returned in the response to determine the cause of the problem. Configuration is required for your firm to use OAuth at each FI and if that configuration is not complete then this step will fail. Additional error detail is provided in the endpoint definition.
#5	User does not complete the OAuth authorization at the Microsite within the allotted time	Error returned by step #5	Repeat the process starting at step 2
#5	User completes the OAuth authorization at the Microsite within the allotted time but some error occurs in the BAA backend with completing the authorization to the Financial Institution.	Error returned by step #5	Repeat the process starting at step 2. If the problem recurs, then report to BAA Technical Support.

Adding Credentials for a LOGIN FI

An FI that supports LOGIN authentication can have more complex worfklows. In addition to requiring a login and password type inputs, it may also require the user to complete different types of security challenges such as Security Questions (SQA) or In-Session Activate Codes (ISAC).   Other conditions may occur when logging into the Financial Institution that require a user action that is separate from security challenges and that are not facilitated by this API. For example, if the user is required to accept Terms and Conditions agreements then the user must separately log into the FI and complete that interaction. This API provides messaging for those cases but does not facilitate those interactions. All security challenges and additional required user actions must be completed before accounts can be aggregated.

Step	Endpoint	Parameters	Notes
1. Obtain FI required fields for user to enter	GET /api/v1/fis/{id}		Returns info about which fields you must prompt the user to enter to complete the credential.
2. Add the credential	POST /api/v1/credentials	Body contains all base elements required by the FI for authentication such as Login and Password.	Returns {credentialId} for next steps
3. Attempt to log into the FI	POST /api/v1/credentials/{credentialId}/authenticate	allowUserInput:true	Returns {ticket} for next steps
4. Poll for completion of login attempt	GET/api/v1/authentications/{ticket}		The basic authentication attempt with login/password may fail, or it may succeed and encounter SQA and/or ISAC security challenges.

If authenticationStatusErrorCode has value 1005 or 1006 then this indicates success.
If authenticationStatusErrorCode has the value 1007 this indicates an authentication failure. To determine what to do next:

Check authenticationStatusInfoType value: |

			sqaCannotConnectBadSqa then go to step 5 SQA Challenge workflow. sqaCannotConnectIsac then go to step 6 ISAC Challenge workflow otherwise - if error than reprompt the user for original inputs, if success go to step 7.
5. [SQA Challenge]			See SQA Challenge Workflow, page 10.
6. [ISAC Challenge]			See ISAC Challenge Workflow, page 11.
7. Discover Accounts	POST /api/v1/credentials/{credentialId}/discover		Returns {ticket} for next steps
8. Poll for completion	GET /api/v1/discoveries/{ticket}		Returns the available accounts.
9. Allow user to choose which accounts to add			
10. Add Accounts	POST /api/v1/credentials/{id}/discovered-accounts		Returns created account URIs.
11. Aggregate Accounts	POST /api/v1/credentials/{credentialId}/aggregate		Aggregate just the accounts for this credential.
12. [Poll for completion of the aggregation]	GET /api/v1/aggregations/{ticket}		Optional step. Aggregation completes asynchronously.

If your user experience does not include allowing the user to choose which accounts to add, you can skip steps 7-10. Step 11 will discover, add, and aggregate all available accounts. Users can delete accounts later using DELETE /api/v1/accounts/{id}.

Please refer to the following section for additional detail on the types of authentication situations that can occur and will need to be handled in your UI: Special Situations for Credentials and Accounts, page 42.

SQA Challenge Workflow

The SQA Challenge Workflow enables the user to resolve security question challenges presented by the FI. An FI can present a single security question or multiple security questions at one time, or it may present a subset of security questions at the initial login and additional question(s) at each subsequent login until all security questions have been answered. This behavior is determined by the FI.

This workflow is triggered when GET/api/v1/authentications/{ticket} returns an error indicating that a Security Question Challenge has been encountered. The response will resemble this:

```
{
 "status": "Complete",
          "statusTimestamp": "2019-04-15 14:26:29 PM",
          "credentialId": 23737,
          "authenticationStatusErrorCode": 1007,
          "authenticationStatusInfoType": "sqaCannotConnectBadSqa",
          "authenticationStatusInfo": "Cannot connect. The answer to a security question is incorrect.",
          "lastAuthenticationAttempt": "2019-04-15 12:00:00 AM",
     "sqa": [
      {
        "id": 85542,
        "question": "In what city did you meet your spouse for the first time?",
        "answer": ""
      }
     ]
    }
```

The response includes questions that the user must answer in the "sqa" section.

Answer a Single Security Question

Step	Endpoint	Parameters	Notes
1. Prompt the user for an answer to the questions and save the user's answer.	PATCH /api/v1/sqas/{id}	Id of the SQA provided in the response as shown above. Answer to the question in the body.	There may be multiple SQAs in the response above.
2. Return to step 3 in the main workflow for "Adding Credentials for a LOGIN FI" on page 8			

Answer Multiple Security Questions

You also have the option at any point to query for any unanswered or incorrectly answered questions on a credential and obtain new answers from the user for those:

Step	Endpoint	Parameters	Notes
1. Obtain the list of unanswered or incorrectly answered security questions.	GET /api/v1/sqas	incorrectOnly:true	
2. Prompt the user for answers to the questions and save the answer for each question separately.	PATCH /api/v1/sqas/{id}	Id of the SQA provided in the response as shown above. Answer to the question in the body.	
3. Return to step 3 in the main workflow for "Adding Credentials for a LOGIN FI" on page 8.			

ISAC Challenge Workflow

In-Session Activation Code (ISAC) challenges require the user to provide a code sent to the user via a previously registered phone number or email address. Completing an ISAC challenge requires you to prompt the user for the required information and provide this to the aggregation service which in turn provides it to the FI in a live session. This interaction must be completed in a timely manner. If not, then the ISAC will time out and need to be started again. The information requested and the form in which it is requested (radio buttons, input text values, etc.) varies by Financial Institution.

If an ISAC is triggered by the authentication attempt (POST /api/v1/credentials/{credentialId}/authenticate), the response will contain a status of "Waiting for User Input" and additional data describing what the user needs to provide to complete the challenge. Note that to complete an ISAC there are typically going to be at least two steps: 1) to prompt the user for which channel they want to use to receive the code, 2) to prompt the user for the code. We use *userinput* to refer to the set of fields that is exchanged to complete the ISAC in all cases. The API provides the *userinput* object to request those inputs, and you will return that same (or abbreviated form of) that *userinput* object to provide the user's responses.

The response also includes the userInputTimeoutInterval in milliseconds. You must either send the full userinput response or a keepalive call at or before this much time has passed. If neither of these is sent the ISAC interaction will time out and will have to be restarted. You will need to repeat sending of the keepalive call at each subsequent time interval until the entire ISAC times out or you have provided the requested userinput.

The userinput that is outstanding at the current point of the ISAC workflow can always be obtained by calling GET /api/v1/authentications/{ticketId}/userinputs..

You can proactively cancel an ISAC workflow using DELETE /api/v1/authentications/{ticketId}/userinputs.

The following is an example response from POST /api/v1/credentials/{credentialId}/authenticate. requesting *userinput*:

```
{
  "status": "Waiting for User Input",
  "statusTimestamp": "2019-05-20T14:54:06.120-04:00",
  "credentialId": 24906,
  "userInput": [
    {
      "inputType": "instructions",
      "instructionText": "How would you like to receive your security code?"
    },
    {
      "inputType": "inputRadioGroup",
      "identifier": 1,
      "value": 2,
      "inputRadio": [
        {
          "instructionText": "xxx-xxx-8989",
          "identifier": 2,
          "label": "Text"
        },
        {
          "identifier": 3,
          "label": "Voice"
        },
        {
          "instructionText": "xxx-xxx-7777",
          "identifier": 4,
          "label": "Text"
        },
        {
          "identifier": 5,
          "label": "Voice"
        },
        {
          "instructionText": " ",
          "identifier": 6,
          "label": "r...y@comcast.net"
        },
        {
          "identifier": 7,
          "label": "Call to get a code"
        }
      ]
    },
    {
      "inputType": "instructions",
      "instructionText": "If none of the above methods work, please contact technical support for assistance."
    }
  ],
  "userInputURI": "/api/v1/authentications/7360686845587335937/userinputs",
  "userInputTimeoutInterval": 90000,
  "userInputExpirationTime": "2019-05-20T15:24:02.000-04:00"
}
```

The following table documents a typical ISAC workflow. It assumes the ISAC has already been triggered by a previous call to POST /api/v1/credentials/{credentialId}/authenticate.

#	Step	Endpoints	Parameters	Notes
1a	Send a keepalive message prior to the userInputTimeoutInterval (milliseconds) to prevent the ISAC from timing out.	POST /api/v1/authentications/{ticketId}/userinputs	No post body.	

1b	Prompt the user for responses to the userinput constructs and submit.	PATCH /api/v1/authentications/{ticketId}/userinputs	The body can be the full original userinput construct with "value" items filled in with user response or it can be a stripped down version of the original userinput with only the element ids and "value".	
2	Poll for the next step	GET/api/v1/authentications/{ticket}		Another userinput prompt should be provided in this response. Repeat 1a/1b with this response.
3	Return to step 3 in the main workflow for "Adding Credentials for a LOGIN FI" on page 8			

Userinput JSON

ISAC Challenges will provide you with Userinput JSON in the response:

```json
{
  "status": "Waiting for User Input",
  "statusTimestamp": "2019-05-20T14:54:06.120-04:00",
  "credentialId": 24906,
  "userInput": [
    {
      "inputType": "instructions",
      "instructionText": "How would you like to receive your security code?"
    },
    {
      "inputType": "inputRadioGroup",
      "identifier": 1,
      "value": 2,
      "inputRadio": [
        {
          "instructionText": "xxx-xxx-8989",
          "identifier": 2,
          "label": "Text"
        },
        {
          "identifier": 3,
          "label": "Voice"
        },
        {
          "instructionText": "xxx-xxx-7777",
          "identifier": 4,
          "label": "Text"
        },
        {
          "identifier": 5,
          "label": "Voice"
        },
        {
          "instructionText": " ",
          "identifier": 6,
          "label": "r...y@comcast.net"
        },
        {
          "identifier": 7,
          "label": "Call to get a code"
        }
      ]
    },
    {
      "inputType": "instructions",
      "instructionText": "If none of the above methods work, please contact technical support for assistance."
    }
  ],
  "userInputURI": "/api/v1/authentications/7360686845587335937/userinputs",
  "userInputTimeoutInterval": 90000,
  "userInputExpirationTime": "2019-05-20T15:24:02.000-04:00"
}
```

The response includes the current status and timestamp of the ISAC interaction along with the credential ID. It contains a userInput section which is a series of text and controls (text input, checkbox, radio button group) that you present to the user for their feedback, and finally it contains information about the ISAC challenge expiration and timeout interval.

The "userInput" section includes a series of userInput objects where each is one of:

▪ **instructions**

This contains instructional text only that should be displayed to the user. The sequence order is significant. There is no user input required for this item.

```
{
 "inputType": "instructions",
 "instructionText": "The institution needs to send you an identification code."
}
```

- **inputText**

  This is an input text field. It has a label and unique identifier for the field. It optionally has instruction text. If the Financial Institution gives a default value then this is included in the value field.

  ```
  {
  "inputType": "inputText",
  "instructionText": "Use the code 'ABC123', otherwise a 1007 error will be returned.",
   "identifier": 1,
  "label": "Enter Code : ",
  "value": ""
  }
  ```

- **inputCheckBox**

  This is an input checkbox field.   It has a label and unique identifier for the field. It optionally has instruction text. If the Financial Institution gives a default value then this is included in the value field.

  ```
   {
  "inputType": "inputCheckbox",
  "instructionText": "Check the box, otherwise a 1007 error will be returned.",
  "identifier": 2,
  "label": "2345",
  "value": false
  }
  ```

- **inputRadioGroup**

  This is a radio button group field. Each radio button in the group has a label and unique identifier for the field, and optionally has instruction text. If the Financial Institution gives a default value then this is included in the value field for the group.

  ```
   {
   "inputType": "inputRadioGroup",
    "identifier": 3,
      "value": 2,
    "inputRadio": [
    {
   "instructionText": "Select one of the options, otherwise a 1007 will be returned",
  "identifier": 4,
  "label": "xxbar@xxxxxxfoobar.com"
  ```

```
   },
   {
   "identifier": 5,
   "label": "XXX-XXX-7890"
   }
   ]
   }
```

These input instructions and fields correspond to the original FI prompts provided on the web site for the challenge.   This information does not include which, if any, of the input fields are required.

Aggregating Accounts

Once accounts are established in the system they will be aggregated according to the configuration for your firm. This may be once every 24 hours or less frequently.   You need not request that the accounts be aggregated. You may force an aggregation "on demand" (within the limits of demand refreshes allowed for your firm) using one of the endpoints:

- POST /api/v1/credentials/{credentialId}/aggregate
- POST /api/v1/accounts/aggregate

Both operations run asynchronously. You can poll for completion status using GET /api/v1/aggregations/{ticket}.

Maintaining Credentials

The GET /api/v1/credentials/accounts/summary endpoint provides all the essential information your user will need to understand the status of their accounts in the aggregation system, including error status values and recommended user actions.

Account credentials may need maintenance by the user, for example if the user changes their password for a LOGIN FI or an FI introduces new security challenges. Maintaining credentials in these situations is usually a minor variation on the workflows documented for adding new credentials to the system.

For LOGIN type credentials:

- Login or Password has changed –
    - Prompt the user to enter the base required information
    - POST /api/v1/credentials/{credentialId}/authenticate to reattempt authentication
- New Security Question challenge
    - GET /api/v1 /sqas with the incorrectOnly:true parameter to get the list of questions requiring answers
    - PATCH /api/v1/sqas/{id} to provide answers.
    - POST /api/v1/credentials/{credentialId}/authenticate to reattempt authentication to see if there are any other failures or security challenges.
- ISAC challenge - use the flow documented in ISAC Challenge Workflow**,** page 11 to resolve it.

For OAUTH type credentials:

- Repeat the OAuth authorization flow as described in [Adding Credentials for an OAUTH FI](#), page 6.

Adding Accounts to Existing Credentials

Automatic aggregation does not add more accounts to an existing credential. You can enable users to add more accounts on demand as follows:

1. LOGIN - Incremental account discovery –

   - with user input – use the same series of calls as described in the first-time case to determine if there are new accounts available and to add them to the system.

   - without user input – use [POST /api/v1/credentials/{credentialId}/aggregate](#) with the *forceDiscovery* parameter set to true to cause new accounts to be added to the system and aggregated.

2. OAUTH credentials – repeat the OAUTH authorization flow as documented in section [Adding Credentials for an OAUTH FI](#), page 6.

Test Financial Institutions (FIs) for Workflows

BAA has test FIs that have specific requirements for logging in to add accounts.

Test FI	Description
DataConnect Account Discovery/Credential Test FI 001 - No SQA	Requires a login and password for account access.
DataConnect Account Discovery/Credential Test FI 002 - SQA	Requires an answer to a single security question (SQA).
TEST: ByAllAccounts Demonstration FI #2 (SQA)	Requires an answer to a single security question (SQA).
DataConnect Account Discovery/Credential Test FI 0011 – Multiple Sequential SQA/Validate PW	Requires answers to multiple questions, one at a time, and validates after receiving each answer.
DataConnect Account Discovery/Credential Test FI 003 – Multiple SQA	Requires answers to multiple questions but does not validate the answers until all of the answers have been received.
TEST: ByAllAccounts Demonstration FI #3 (ISAC)	Requires in-session activation code (ISAC) to log in, with the typical two-step process.
DataConnect Activation Code Test 003 - Single Prompt	Requires in-session activation code (ISAC) to login, with a single prompt.
DataConnect Account Credential Test FI 001 - No SQA	Does not support account discovery; requires an account number.
DataConnect Account Credential Test FI 005 - Account Number 2 Field	Does not support account discovery; requires two account numbers.
DataConnect Oauth Test FI 002	Requires OAuth authorization.

Note: When using a test FI, click the question mark ⓘ to the right of each field to see the credentials you need.

Other Considerations

This section provides information on other things to think about when building your own UI for aggregation:

- **Multiple credentials at the same FI, duplicate credentials** – the system will NOT prevent you from establishing more than one credential at the same institution, nor will it prevent you from creating the same credential at an FI (same login) multiple times. You can prevent this by searching for existing credentials at an FI once the user chooses an FI to work with during the account setup process, and then prompting the user to see if they want to reuse an existing credential or add a new credential at that FI. Use the *GET /credentials* endpoint to get a list of credentials for an investor.
- **New accounts available on existing credentials** – the automated aggregation process does not include discovering newly available or newly authorized accounts on existing credentials. If you wish to add accounts to a credential you should follow the process described above for the type of credential.
- **Change the FI ID for an existing credential** – we recommend that you do NOT provide a way for your users to switch the FI ID for an existing credential. Doing so can lead to complex situations with the credential information and status that will be difficult to communicate effectively to the user.

ENDPOINTS

This table is a guide to help you find descriptions of the endpoints.

Category	Name	Endpoint	Page
Account Operations	DELETE accounts	DELETE /api/v1/accounts/{id}	
Activities Operations	GET activities summary	GET /api/v1/activities/summary	
Aggregation Operations	POST aggregate accounts	POST /api/v1/accounts/aggregate	
	GET aggregation result	POST /api/v1/aggregations/{ticket}	
	POST new aggregation on a credential	POST /api/v1/credentials/{credentialId}/aggregate	
Credential Operations	POST credentials	POST /api/v1/credentials	
	GET credentials	GET /api/v1/credentials	
	GET credentials by ID	GET /api/v1/credentials/{id}	
	GET credentials and accounts	GET /api/v1/credentials/accounts/summary Note: This endpoint replaces GET /api/v1/credentials/accounts which is being deprecated.	
	PATCH credential	PATCH /api/v1/credentials/{id}	
	DELETE credentials	DELETE /api/v1/credentials/{id}	
Credential Authentication Operations	POST user inputs	POST /api/v1/authentications/{ticketId}/userinputs	
	POST a new request for authentication	POST /api/v1/credentials/{credentialId}/authenticate	
	GET authentication result	GET/api/v1/authentications/{ticket}	
	GET user inputs	GET /api/v1/authentications/{ticketId}/user inputs	
	PATCH user input result	PATCH /api/v1/authentications/{ticketId}/userinputs	
	DELETE the authentication operation	DELETE /api/v1/authentications/{ticketId}	
	DELETE user input interaction	DELETE /api/v1/authentications/{ticketId}/userinputs	
Discovery Operations	POST account discovery for a specific credential	POST /api/v1/credentials/{credentialId}/discover	

	POST discovered accounts of a specific credential	POST /api/v1/credentials/{id}/discovered-accounts	
	GET discovery result	GET /api/v1/discoveries/{ticket}	
Financial Institution Operations	GET Financial Institution	GET /api/v1/fis	
	GET Financial Institution by ID	GET /api/v1/fis/{id}	
Person Operations	POST new Person	POST /api/v1/persons	
	GET person ID	GET /api/v1/persons/{id}	
	GET person	GET /api/v1/persons/me/networth	
	GET person summary	GET /api/v1/persons/me/summary	
	DELETE person	DELETE /api/v1/persons	
Position Operations	GET positions	GET /api/v1/positions	
Security Question and Answer (SQA) Operations	GET all SQA entries for a credential	GET /api/v1/sqas	
	PATCH a Security Question and Answer (SQA)	PATCH /api/v1/sqas/{id}	
Transaction Operations	GET transactions	GET /api/v1/transactions	
Deprecated Endpoint	GET credentials including account info when available	GET /api/v1/credentials/accounts	

Account Operations

DELETE accounts

DELETE /api/v1/accounts/{id}

Implementation Notes

Use this endpoint to delete from the system the account identified by the *id* parameter.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id	yes		The unique identifier of an account	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
204	No Content		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

Activities Operations

GET activities summary

GET /api/v1/activities/summary

Implementation Notes

Use this endpoint to determine whether any asynchronous activities for the authenticated investor are in progress in the BAA service. The endpoint can monitor activities for just the current session, or it can include other sessions of the user depending on the scope parameter setting.

Asynchronous activities include:

- authenticating credentials

- discovering, adding, and aggregating accounts

- aggregating accounts

This endpoint returns a single Boolean value for *activityInProgress* that indicates whether asynchronous activities are in progress for the user.

The applicable scope of this endpoint is always a single authenticated investor. This endpoint can provide information on asynchronous activity for the current session or for all activity in the system. Use the *scope* parameter with value *session* to request information about activity initiated during the current session. Use the *scope* parameter with value *global* to request information for all activity in the system. When scope is *global*, asynchronous activity progress will be available for terminated sessions up to 15 minutes after completion of that activity. If the scope parameter is not provided, the endpoint will report on activity for the current session if there is one. If there is no current session (Morningstar Authentication) then it will report on all activity for the authenticated investor.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
scope	no	*session* for session-based users and *global* for users authenticated by Morningstar Authentication	Value can be *session*, to include only session-specific activity progress, or *global* to also include activity progress from other sessions for this user. Cannot be set to *session* for Morningstar Authentication users. Note: the *global* setting currently does not return status for accounts aggregating outside the current session.	query	String. Can be either *session* or *global*.

Response

The JSON response for the endpoint is one of the following, depending on whether there is activity in progress or not:

{"activityInProgress":false}

OR

{"activityInProgress":true}

If scope is not set or is set to *session*, the value is true if any asynchronous activity is in progress for the session for at least one credential. If scope is set to *global*, the value is true if any asynchronous activity is in progress for the session for at least one credential or if authenticate or discovery/add/aggregate is in progress for accounts aggregating for at least one credential outside the current session.

When all activity completes then the value of activityInProgress will be false.

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok	See Response above.	
401	Not Authorized		
403	Forbidden		
500	Internal Server Error		

Aggregation Operations

POST aggregate accounts

POST /api/v1/accounts/aggregate

Implementation Notes

Use this endpoint to request aggregation of accounts for the authenticated investor from a Financial Institution. Use the *class* parameter to restrict which accounts to aggregate by specifying one or more class values: investment, noninvestment, or other.

Aggregation gathers holdings and transactions for the accounts from associated Financial Institutions. It does not discover new accounts that are available to the user from those Financial Institutions. The request will not attempt to aggregate any account that is disabled due to a login error as repeated retries with incorrect credentials could cause an account to be locked out.

Aggregation runs asynchronously. This endpoint validates inputs and locates target accounts for aggregation. If either of these operations fails, an error code is returned. If both operations succeed, the aggregation is submitted. Progress of the aggregation activity can be monitored using the GET /api/v1/activities/summary endpoint (page 22) and the GET /api/v1/credentials/accounts/summary endpoint on page 37.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
class	no		If no class is specified, then all account types are returned.	query	List of one or more of the following classes of investor accounts: ▪ **investment** which includes BAA account types prefixed with INVESTMENT_ and INSURANCE_ ▪ **nonInvestment** which includes BAA account types CREDITCARD and all those prefixed with BANKING_, HEALTHACCOUNT_, and LOAN_ ▪ **other** which includes BAA account types: OTHER, UNKNOWN, and NULL For the list of Account Types, refer to Table of Account Types page 52.

Response Messages

HTTP Status Code	Reason	Response Model	Headers
201	Created		
400	Bad request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

POST new aggregation on a credential

POST /api/v1/credentials/{credentialId}/aggregate

Implementation Notes

Use this endpoint to initiate the aggregation operation for the given credential. For LOGIN type credentials this operation will aggregate existing accounts, and if forceDiscovery is set to true it will discover, add, and aggregate any accounts newly available on the credential. For OAUTH type credentials this operation will only aggregate existing accounts. Note that this operation does not require any post body nor does it return one. On success (200) the Location header will contain the temporary location to use to poll for status.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
credentialId	yes		Credential ID for aggregation	path	integer
forceDiscovery		false	If true, additional accounts (if any exist) will be discovered and added even for non-Oauth credentials that already have accounts	query	Boolean

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
201	Created		
400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

GET aggregation result

GET /api/v1/aggregations/{ticket}

Implementation Notes

Use this endpoint to obtain the result of an aggregation operation.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticket	yes		Universal unique identifier associated with this aggregation (provided as part of URL returned in Location header when aggregation operation was first submitted)	path	string

Response Body

```
{
  "id": 80524,
  "status": "Complete",
```

```
    "statusTimestamp": "2023-10-17T16:08:58.512-04:00",
    "accounts": [
      {
        "id": 857641,
        "name": "DataConnect Account Credential Test FI 001 - No SQA 830",
        "accountUpdateStatusErrcode": 1005,
        "lastUpdated": "2023-10-17T16:05:52.000-04:00",
        "lastUpdateAttempt": "2023-10-17T16:05:52.000-04:00",
        "marketValue": {
          "amount": 50000,
          "currencyCode": "USD"
        }
      }
    ]
  }
```

Response Model

The response structure is as follows.

Label	Req'd?	Type	Description
{			The result of a credential aggregation, which will incorporate status information from individual accounts
id	yes	integer	Account credential ID
status	yes	string	Account Credential ID associated with this authentication. Example: In Progress.
statusTimestamp	yes	string	Status timestamp. Example: 2023-05-24T01:23:45.67 -0400
accountDiscoveryStatusErrcode	yes	integer	Status code for the account discovery operation; will be null (absent) if account discovery not performed
accountDiscoveryStatusInfo	yes	string	Status info for the account discovery operation; will be null (absent) if account discovery not performed. Example: Account discovery successful
accountDiscoveryStatusTimestamp	yes	string	Status info for the account discovery operation; will be null (absent) if account discovery not performed. Example: 2023-05-24T01:23:45.67 -0400
accounts			List of aggregated accounts associated with this credential
[			
id		integer	Account ID
name	yes	string	Account name

Label	Req'd?	Type	Description
accountUpdateStatusErrcode		integer	Status code for this account (1005 indicates success)
accountUpdateStatusInfo		string	Status info for this account (null on success)
lastUpdated		string	Timestamp of the last successful update. Example: 2023-05-24T01:23:45.67 -0400
lastUpdateAttempt		string	
marketValue {			
amount		number	Total market value of the account.
currencyCode		string	ISO 4217 currency code for the position, such as USD
}			
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See [Response Model](#), page 27	
400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

Credential Operations

POST credentials

POST /api/v1/credentials

Implementation Notes

Use this endpoint to add a new account credential to the system. The fields required to create a complete account credential vary by Financial Institution. Check the Financial Institution object to determine these requirements.

Request Headers

The POST body parameters listed in are to be submitted in JSON format as shown in this example for a LOGIN type credential:

```
POST /api/v1/credentials
{
 "fiId": 12484,
 "accountLogin": "username",
 "accountPin": "pin"
}
```

Here is an example for an OAUTH type credential:

```
POST /api/v1/credentials
{
 "fiId": 12485
}
```

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
{			Credentials provided to BAA for authentication to a third party Financial Institution.		
name			Name of the Account Credential	body	string
fiId			ID of the Financial Institution.	body	string
accountLogin			Account Login	body	string
accountLogin2			Account Login 2	body	string

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
accountPin			Account PIN	body	string
accountSecondPin			Account Second PIN	body	string
}					

Response Body

URI to new resource. For example:
{
  "uri": "https://www.byallaccounts.net/api/v1/credentials/12345"
}
Where 12345 is the BAA Credential Id for the new Credential.

Response Messages

HTTP Status Code	Reason	Response Model	Headers

200	OK	{
		  "data": {}
		}	

400	Bad Request		
401	Not Authorized		
403	Forbidden		
500	Internal Server Error		

GET credentials

GET /api/v1/credentials

Implementation Notes

Use this endpoint to get the collection of all credentials.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
fiId			Get only the account credentials for the specified FI ID.	query	integer
page		0	Page number	query	integer
size		25	Number of records per page	query	integer

Response Body

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 1,
  "totalElements": 1,
  "isFirst": true,
  "isLast": true,
  "summary": {},
  "data": [
   {
     "id": 778899,
     "profileId": 5566,
     "name": "DataConnect Account Credential Test FI 001 - No SQA 151",
     "fiId": 12484,
     "accountLogin": "username",
     "accountPinPresent": false,
     "accountSecondPinPresent": false,
    "isCredentialComplete": true,
     "lastAuthenticationAttempt": "2018-05-21 2:52:23 AM",
     "authenticationStatusErrorCode": 1006,
     "authenticationStatusInfoType": "cannotConnectMissingLoginPW",
     "authenticationStatusInfo": "Cannot connect. Missing Login or Password.",
     "authType":"Login",
     "hasAccounts": true,
```

```
      "incompleteISAC": false,
      "creationDate": "2022-08-01",
      "maskedAccountNumbers": "x-1234,x-5678"
    }
  ]
}
```

Response Model

The response structure is as follows.

Label	Req'd?	Type	Description
{			A page of data records
pageSize		integer	Number of records per page
pageNumber		integer	Page number of this page
totalPages		integer	Total number of pages in result set
totalElements		integer	Total number of elements in result set
isFirst		Boolean	True if and only if this is the first page of data in the result set
isLast		Boolean	True if and only if this is the last page of data in the result set
summary { }			
data [			Credentials provided to BAA for authentication to a third party Financial Institution. The credential may be linked to an established 3rd party Financial Institution by providing the appropriate fiId, or the fiRequestName and fiRequestURL fields may be provided to request support for a new Financial Institution.
{			
id	yes	integer	ID of the Account Credential
profileId	yes	integer	Financial profile ID of the credential owner
Name	yes	string	Name of the Account Credential
fiId		integer	ID of the Financial Institution. Either the fiId field or the fiRequestName field will be provided (and not both).
firequestName		string	The name of the requested FI. Either the fiId field or the fiRequestName field will be provided (and not both).
firequestURL		sting	The URL of the requested FI. Will only be provided when the fiRequestName is provided (and the fiId field is not provided).
accountLogin		string	Account Login

Label	Req'd?	Type	Description
accountLogin2		string	Account Login 2
accountPinPresent		Boolean	Account PIN Present = true or false
accountSecondPinPresent		Boolean	Account Second PIN Present = true or false
authType	yes	string	The type of authentication supported by this Financial Institution. One of: Oauth or Login.
oauthTokenId		string	Internal BAA unique identifier for an OAuth token if an OAuth authorization has been completed for this credential.
isCredentialComplete	yes	Boolean	Credential complete = true or false
lastAuthenticationAttempt		string	Date of the last authentication attempt. Example: 2023-05-21 2:52:23 AM
authenticationStatusErrorCode		integer	Error code from the latest authentication attempt
authenticationStatusInfoType		string	Type of status information from the latest authentication attempt. Example: cannotConnectMissingLoginPW
authenticationStatusInfo		string	Status information from the latest authentication attempt (simplified). Example: Cannot connect. Missing Login or Password.
hasAccounts	yes	Boolean	Indicates whether this account credential has any associated accounts. Example: true.
incompleteISAC	yes	Boolean	Indicates whether the ISAC process is complete
creationDate	yes	string	Credential creation date. Example: 2023-08-01
maskedAccountNumbers		string	Comma separated list of masked account numbers associated with the requested Financial Institution. Example: x-1234,x-5678
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See Response Model, page 32	
400	Bad Request		

HTTP Status Code	Reason	Response Model	Headers
401	Not Authorized		
404	Not Found		
500	Internal Server Error		

GET credentials by ID

GET /api/v1/credentials/{id}

Implementation Notes

Use this endpoint to get an account credential by ID.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id	yes		The ID of the account credential requested.	path	integer
includeMaskedAccountNumbers		false	If True then include masked account numbers in there response, otherwise no account numbers will be included.	query	Boolean

Response Body

```
{
    "id": 778899,
    "profileId": 5566,
    "name": "DataConnect Account Credential Test FI 001 - No SQA 151",
    "fiId": 12484,
    "accountLogin": "username",
    "accountPinPresent": false,
    "accountSecondPinPresent": false,
    "isCredentialComplete": true,
    "lastAuthenticationAttempt": "2018-05-21 2:52:23 AM",
```

```
"authenticationStatusErrorCode": 1006,
"authenticationStatusInfoType": "cannotConnectMissingLoginPW",
"authenticationStatusInfo": "Cannot connect. Missing Login or Password.",
"authType":"Login",
"hasAccounts": true,
"incompleteISAC": false,
"creationDate": "2022-08-01",
"maskedAccountNumbers": "x-1234,x-5678"
}
```

Response Model

The response structure is as follows.

Label	Req'd?	Type	Description
{			Credentials provided to BAA for authentication to a third party Financial Institution.
id	yes	integer	ID of the Account Credential
profileId	yes	integer	Financial profile ID of the credential owner
name	yes	string	Name of the Account Credential
fiId		integer	ID of the Financial Institution. Either the fiId field or the fiRequestName field will be provided (and not both).
firequestName		string	The name of the requested FI. Either the fiId field or the fiRequestName field will be provided (and not both).
firequestURL		sting	The URL of the requested FI. Will only be provided when the fiRequestName is provided (and the fiId field is not provided).
accountLogin		string	Account Login
accountLogin2		string	Account Login 2
accountPinPresent		Boolean	Account PIN Present = true or false
accountSecondPinPresent		Boolean	Account Second PIN Present = true or false
authType	yes	string	The type of authentication supported by this Financial Institution. One of: Oauth or Login.
oauthTokenId		string	Internal BAA unique identifier for an OAuth token if an OAuth authorization has been completed for this credential.
isCredentialComplete	yes	Boolean	Credential complete = true or false
lastAuthenticationAttempt		string	Date of the last authentication attempt. Example: *2023-05-21 2:52:23 AM*

Label	Req'd?	Type	Description
authenticationStatusErrorCode		integer	Error code from the latest authentication attempt
authenticationStatusInfoType		string	Type of status information from the latest authentication attempt. Example: cannotConnectMissingLoginPW
authenticationStatusInfo		string	Status information from the latest authentication attempt (simplified). Example: Cannot connect. Missing Login or Password.
hasAccounts	yes	Boolean	Indicates whether this account credential has any associated accounts. Example: true.
incompleteISAC	yes	Boolean	Indicates whether the ISAC process is complete
creationDate	yes	string	Credential creation date. Example: 2023-08-01
maskedAccountNumbers		string	Comma separated list of masked account numbers associated with the requested Financial Institution. Example: x-1234,x-5678
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See Response Model, page 35	
400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

GET credentials and accounts

GET /api/v1/credentials/accounts/summary

Note: This endpoint replaces GET /api/v1/credentials/accounts page A-1, which is being deprecated.

Implementation Notes

This endpoint retrieves credentials and any associated accounts for the authenticated investor. Credentials that have no associated accounts are also included. The response is a single-page collection of data organized into the following groups to provide a comprehensive view *specifically for real-time display to an end user*:

- IN_PROGRESS group – credentials for which newly added accounts are being aggregated
- NEEDS_USER_ACTION group – credentials that need user action
- MAIN_GROUP group – all credentials and accounts for the investor
- FI_REQUEST group – Financial Institution requests

This response also includes information about asynchronous activities that are in progress for the credentials and accounts. This endpoint can provide information on asynchronous activity for the current session or for all activity in the system. Use the *scope* parameter with value *session* to request information about activity initiated during the current session. Use the *scope* parameter with value *global* to request information for all activity in the system. When *scope* is *global*, asynchronous activity progress will be available for terminated sessions up to 15 minutes after completion of that activity. If the *scope* parameter is not provided, then the endpoint will report on activity for the current session if there is one. If there is no current session (Morningstar Authentication) then it will report on all activity for the authenticated investor.

You can specify the number of the page to return and the number of records per page.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
page	No	0	Page number	query	integer
size	No	25	Number of records per page	query	integer

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
scope	No	*session* for session-based users and *global* for users authenticated by Morningstar Authentication	Scope of activity for the authenticated user. Values can be *session*, to include only session-specific information, or *global* to also include information from other sessions for this user.	query	String. Either *session* or *global.*
view	No	institution	Selects the organization of the information in the response to be either by *Institution* or by *AccountType*.	query	string

Response Body

The following is a simple sample response body that shows the overall structure of the response as well as the differing content in each of the separate data sections (IN_PROGRESS, NEEDS_USER_ACTION, MAIN_GROUP, FI_REQUEST).

```
{
    "pageSize": 25,
    "pageNumber": 0,
    "totalPages": 1,
    "totalElements": 6,
    "isFirst": true,
    "isLast": true,
    "activitySummary": {
        "activityInProgress": true
    },
    "summary": {
        "inProgressTotal": 1,
        "needsUserActionTotal": 1
    },
    "data": [
        {
            "id": 72143,
            "group": "IN_PROGRESS",
```

```
        "financialInstitution": {
          "id": 47031,
          "name": "Bank of America",
          "icon":
"https://www.byallaccounts.net/WebPortfolio/vendorResources/Default/assets/fi/icons/Banking_Icon.svg
"
        }
      },
      {
        "id": 71704,
        "group": "NEEDS_USER_ACTION",
        "unifiedStatusInfoType": "cannotConnectBadLoginPwSqa",
        "unifiedStatusInfoActionableType": "userActionable",
        "unifiedStatusInfoMiniType": "cannotConnect",
        "unifiedStatusInfoActionType": "reAuthenticate",
        "financialInstitution": {
          "id": 31244,
          "name": "Chase",
          "icon":
"https://www.byallaccounts.net/WebPortfolio/vendorResources/Default/assets/fi/icons/Banking_Icon.svg
"
        }
      },
      {
        "id": 72142,
        "group": "MAIN_GROUP",
        "credentialComplete": true,
        "creationDate": "2023-03-06",
        "lastAuthenticationAttempt": "2023-03-06T10:10:40.000-05:00",
        "authenticationStatusErrorCode": 1005,
        "activityInProgressStatus": "Complete",
        "account": {
          "id": 795280,
          "name": "Steve's Account",
          "marketValue": {
            "amount": 50000,
            "currencyCode": "USD"
          },
          "lastUpdated": "2023-03-06T10:10:40.000-05:00",
          "relativeLastUpdatedText": "Updated 3 mins ago",
          "aggregationStatusErrorCode": 1005,
          "creationDate": "2023-03-06",
          "maskedAccountNumber": "x-2653"
```

```
      },
      "financialInstitution": {
        "id": 31243,
        "name": "Wells Fargo Bank",
        "supportsOauth": false,
        "loginTerm": "Login",
        "pwTerm": "Password",
        "accountNumberTerm": "Account Number",
        "icon":
"https://www.byallaccounts.net/WebPortfolio/vendorResources/Default/assets/fi/icons/Banking_Icon.svg
"
      }
    },
    {
      "id": 71704,
      "group": "MAIN_GROUP",
      "credentialComplete": true,
      "creationDate": "2023-03-01",
      "lastAuthenticationAttempt": "2023-03-01T11:56:59.000-05:00",
      "authenticationStatusErrorCode": 1007,
      "unifiedStatusInfoType": "cannotConnectBadLoginPwSqa",
      "unifiedStatusInfoActionableType": "userActionable",
      "unifiedStatusInfoMiniType": "cannotConnect",
      "unifiedStatusInfoActionType": "reAuthenticate",
       "unifiedStatusInfoMsg": "We cannot connect to this institution. The Login, Password, or answer
       to a security question is incorrect. Re-authenticate.",
      "activityInProgressStatus": "Complete",
      "financialInstitution": {
        "id": 31244,
        "name": "Chase",
        "supportsOauth": false,
        "loginTerm": "Login",
        "pwTerm": "Password",
        "accountNumberTerm": "Account Number",
        "icon":
"https://www.byallaccounts.net/WebPortfolio/vendorResources/Default/assets/fi/icons/Banking_Icon.svg
"
      }
    },
    {
      "id": 72143,
      "group": "MAIN_GROUP",
      "credentialComplete": true,
```

```json
        "creationDate": "2023-03-06",
        "lastAuthenticationAttempt": "2023-03-06T10:13:09.000-05:00",
        "authenticationStatusErrorCode": 1005,
        "unifiedStatusInfoType": "cannotLoadDataCheckLater",
        "unifiedStatusInfoActionableType": "nonUserActionable",
        "unifiedStatusInfoMiniType": "cannotConnect",
        "unifiedStatusInfoActionType": "checkBackLater",
        "unifiedStatusInfoMsg": " We are having trouble accessing this institution. Check back later.",
        "activityInProgressStatus": "In Progress",
        "account": {
          "id": 795281,
          "name": "Joe's Checking Account",
          "marketValue": {
            "amount": 0,
            "currencyCode": "USD"
          },
          "creationDate": "2023-03-06",
          "maskedAccountNumber": "x-1234"
        },
        "financialInstitution": {
          "id": 47031,
          "name": "Bank of America",
          "supportsOauth": false,
          "loginTerm": "Login",
          "pwTerm": "Password",
          "accountNumberTerm": "Account Number",
          "icon":
"https://www.byallaccounts.net/WebPortfolio/vendorResources/Default/assets/fi/icons/Banking_Icon.svg
"
        }
      },
      {
        "id": 71703,
        "group": "FI_REQUEST",
        "creationDate": "2023-03-01",
        "fiRequestName": "Cornerstone Bank (MA) - Personal",
        "maskedAccountNumbers": "x-6789"
      }
    ]
  }
```

Response Model

Special Situations for Credentials and Accounts

Credentials and accounts in the aggregation system are complex objects for which the following statements are true:

- Credentials or accounts can be incomplete, meaning they do not contain enough information to access data from the Financial Institution. This situation can occur if the user has not yet provided all necessary information (e.g. has not yet provided their password or completed OAUTH authorization).

- The aggregation system may encounter a variety of errors when attempting to use a credential or an account to access data from a Financial Institution. These errors can occur because the information in the object is incorrect (e.g. a wrong password), there are problems with the aggregation system's support (e.g. Financial Institution web site has changed and we need to update our support), or there are problems at the Financial Institution (e.g. site not available).

These conditions are not errors from an application perspective, but rather they are "normal" things that can happen in the day-to-day of aggregation activities. It is important to properly represent these conditions to the end user and, whenever possible, help the user to understand when they must take action to resolve the condition or when the solution is not under their control. Although these error conditions can be complex. ByAllAccounts is continually improving ways to present them clearly to users. This endpoint provides both organization of the information into groups as well as a concise field set that explains the status of the credential or account for presentation to the user. The fields also include whether a user action is required to resolve the issue (or not), and also the specific recommended action.

In addition to these situations, the system may be asynchronously performing activities that the user requested, directly or indirectly, on credentials and accounts. For example, if a request was made to obtain the latest data for an account, then an asynchronous aggregation process is going on in the background and we want the end user to understand that it is in process and when that process completes. This endpoint includes information at the individual object level (credential or account) as well as the summary level (for the collection) to aid in the presentation of this information to the user. Note also that any asynchronous activity can result in the clearing of an error condition or the encountering of a new condition, so that information should be queried and redisplayed upon completion of the asynchronous activity.

Account and Credential Error Information

Credentials and Accounts can be incomplete (missing required information like a login, or an account number), or they can be complete and have errors as reported by the custodian when the credentials are used to attempt to access a customer's data at the custodian. These errors could include wrong login/password, account number could not be found, etc.

The unifiedStatusInfoType field indicates an error condition that should be relayed to the user. If unifiedStatusInfoType is absent, then no error condition exists at the present time. The unifiedStatusInfoMsg field will contain a suggested text form of the message for presentation to the user.

For more information about unifiedStatusInfoType, refer to Table of Authentication/Aggregation Status Messages on page 51. Note that some errors listed may not occur frequently, but they are included for completeness.

There are other fields in the response that contain a variety of information about status, but these fields should not be used. They are present for historical reasons and are superseded by unifiedStatusInfoType. The following fields should NOT be used to determine whether a credential or account is incomplete or has another type of error:

- aggregationStatusErrorCode
- authenticationStatusErrorCode
- credentialComplete

Activity in progress information

As described above, this endpoint can return information about server "activity in progress" for objects in the response collection. Activity in progress includes:

- testing that a credential authenticates at a custodian
- discovering accounts available for a credential at a custodian
- aggregating data for accounts from the custodian

These operations are initiated and running in the ByAllAccounts server while the UI or API caller is awaiting the results of those operations. This activity information can be provided for two different scopes: SESSION or GLOBAL. The default is SESSION if you have a session, and GLOBAL if you do not (some forms of authentication do not use a session). If you have a session, you can request GLOBAL using the scope query parameter. For session scope, the progress information is reported for the above operations that were initiated during the current session. For global scope, the information will be reported for all activity initiated through the REST API for the target objects (regardless of who initiated that activity).

The activityInProgress field at the top of the response will have a value of "true" if there is activity in progress for any object in the collection, otherwise "false".

For each object, the activityInProgressStatus field:

- is absent if no activity occurred for the scope of the request (as determined by the query parameter *scope*).
- if present and value is:
  - "In Progress" then authentication or aggregation activity is currently occurring for this object within the ByAllAccounts Server for the scope of the request (as determined by the query parameter *scope*).
  - "Complete" then authentication or aggregation activity has completed for this object within the ByAllAccounts Server for the scope of the request (as determined by the query parameter *scope*).

While asynchronous activity is occurring for objects in the response, the error status on objects can change multiple times and additional objects can be added to the response. For example, if a new credential was added and account discovery was initiated (e.g. by the BAA ConsumerUI), then as accounts are discovered they will appear in the response, and subsequently data for those accounts will be aggregated and their market value will appear.

The IN_PROGRESS group will contain credential details when new accounts have just been added and are being aggregated for the first time. If there are no new accounts being aggregated but possibly existing accounts are being aggregated, then credential details for these accounts will be excluded from the IN_PROGRESS group.

;

The response model contents for this endpoint are shown in separate tables, with each one corresponding to a different group:

-
-
-
-

The response structure is as follows, with paging and summary information at the top followed by the four optional groups of credential/account information. Paging information applies to all the rows in the data section.

```
{
    "pageSize": 25,
    "pageNumber": 0,
    "totalPages": 1,
    "totalElements": 5,
    "isFirst": true,
    "isLast": true,
    "activitySummary": {
        "activityInProgress": true
    },
    "summary": {
        "inProgressTotal": 1,
        "needsUserActionTotal": 1
    },
    "data": [
     [IN_PROGRESS GROUP]
     [NEEDS_USER_ACTION GROUP]
     [MAIN_GROUP]
     [FI_REQUEST]
    ]
}
```

Paging and Summary Fields

<table>
<tr><th colspan="4">Paging and Summary Fields</th></tr>
<tr><th>Label</th><th>Required
?</th><th>Type</th><th>Description</th></tr>
<tr><td>{</td><td></td><td></td><td></td></tr>
<tr><td>pageSize</td><td></td><td>integer</td><td>Number of records per page</td></tr>
<tr><td>pageNumber</td><td></td><td>integer</td><td>Page number of this page</td></tr>
<tr><td>totalPages</td><td></td><td>integer</td><td>Total number of pages in result set</td></tr>
<tr><td>totalElements</td><td></td><td>integer</td><td>Total number of elements in result set</td></tr>
<tr><td>isFirst</td><td></td><td>Boolean</td><td>True or false. True if and only if this is the first page of data in the result set</td></tr>
<tr><td>isLast</td><td></td><td>Boolean</td><td>True or false. True if and only if this is the last page of data in the result set</td></tr>
<tr><td>activitySummary {</td><td></td><td></td><td></td></tr>
<tr><td>   activityInProgress</td><td></td><td>Boolean</td><td>If scope=*session* (or not set), then true indicates aggregation or authentication is in-progress for at least one credential in the session. If scope=*global*, then true indicates aggregation or authentication is in-progress for at least one credential in the session or authentication or discover/add/aggregate is in progress for at least one credential outside the current session.</td></tr>
<tr><td>}</td><td></td><td></td><td></td></tr>
<tr><td>summary {</td><td></td><td></td><td></td></tr>
<tr><td> inProgressTotal</td><td></td><td>integer</td><td>The total number of credentials that are in progress</td></tr>
<tr><td> needsUserActionTotal</td><td></td><td>integer</td><td>The total number of credentials that need user action</td></tr>
<tr><td>}</td><td></td><td></td><td></td></tr>
</table>

Group: In Progress

<table>
<tr><td colspan="4" align="center">**Group: In Progress**</td></tr>
<tr><td>**Label**</td><td>**Required ?**</td><td>**Type**</td><td>**Description**</td></tr>
<tr><td>data
[{</td><td></td><td>array</td><td>Credential-account pair. Either an account and its related credential or a credential that has no accounts associated with it.</td></tr>
<tr><td>id</td><td>yes</td><td>integer</td><td>ID of the account credential.</td></tr>
<tr><td>group</td><td>yes</td><td>string</td><td>Identifies the group in which the data is organized. Can be one of: NEEDS_USER_ACTION, MAIN_GROUP, IN_PROGRESS, or FI_REQUEST. For this data group the value will be IN_PROGRESS.</td></tr>
<tr><td>}</td><td></td><td></td><td></td></tr>
<tr><td>financialInstitution {</td><td></td><td></td><td></td></tr>
<tr><td>id</td><td>yes</td><td>integer</td><td>The ID of the financial institution.</td></tr>
<tr><td>name</td><td></td><td>string</td><td>Name of the financial institution.</td></tr>
<tr><td>icon</td><td></td><td>string</td><td>The path to the icon for the financial institution. If the financial institution is requested (not supported) it is the path to a default icon.</td></tr>
<tr><td>}]</td><td></td><td></td><td></td></tr>
</table>

Group: Needs User Action			
Label	**Required ?**	**Type**	**Description**
data [{		array	Credential-account pair. Either an account and its related credential or a credential that has no accounts associated with it
id	Yes	integer	ID of the account credential
group	Yes	string	Identifies the group in which the data is organized. Can be one of: NEEDS_USER_ACTION, MAIN_GROUP, IN_PROGRESS, or FI_REQUEST. For this data group the value will be NEEDS_USER_ACTION.
unifiedStatusInfoType		string	Type of status information from the combination of the latest authentication and aggregation attempt. See Table of Authentication/Aggregation Status Messages page 51.
unifiedStatusInfoActionableType		string	If present, the value is userActionable which indicates that a user can act.
unifiedStatusInfoMiniType		string	When present, this is a short message describing the error. Can be one of: cannotConnect, cannotProcess, or noAccountsConnected.
unifiedStatusInfoActionType		string	This field provides the recommended user action for resolving the issue identified in unifiedStatusInfoType. If present, can be one of: authenticate, completeRequest, connectAccounts, reAuthenticate, or reauthorize.
financialInstitution {			
id	yes	integer	The ID of the financial institution
name		string	Name of the financial institution
icon		string	The path to the icon for the financial institution. If the financial institution is requested (not supported) it is the path to a default icon.
}]			

Group: Main Group			
Label	**Required ?**	**Type**	**Description**
data [{		array	Credential-account pair. Either an account and its related credential or a credential that has no accounts associated with it.
id	yes	integer	ID of the account credential.
group	yes	string	Identifies the group in which the data is organized. Can be one of: NEEDS_USER_ACTION, MAIN_GROUP, IN_PROGRESS, or FI_REQUEST. For this data group the value will be MAIN_GROUP.
credentialComplete	yes	Boolean	True or false. Indicates whether the credential contains enough information to perform authentication. This field can be ignored. Instead refer to unifiedStatusInfoType and see Account and Credential Error Information page 42 regarding best practices on understanding the state of the accounts and credentials.
creationDate		string	Date and time stamp of creation of the account credential.
lastAuthenticationAttempt		string	Identifies when the last authentication attempt was made.
authenticationStatusErrorCode		integer	Error code from the latest authentication attempt. *This field can be ignored.* Instead refer to unifiedStatusInfoType and see Account and Credential Error Information page 42 regarding best practices on understanding the state of the accounts and credentials.
unifiedStatusInfoType		string	Type of status information from the combination of the latest authentication and aggregation attempt. See Table of Authentication/Aggregation Status Messages page 51.
unifiedStatusInfoActionableType		string	Indicates whether and where a user can act. Can be one of: nonUserActionable, userActionable, externallyUserActionable.
unifiedStatusInfoMiniType		string	When present, this is a short message describing the error. Can be one of:

Group: Main Group			
Label	**Required ?**	**Type**	**Description**
			cannotConnect, cannotProcess, or noAccountsConnected.
unifiedStatusInfoActionType		string	This field provides the recommended user action for resolving the issue identified in unifiedStatusInfoType. When present, can be one of: accountClosed, authenticate, checkBackLater, completeRequest, connectAccounts, contactProvider,, externalActionRequired, reauthenticate, or reauthorize.
unifiedStatusInfoMsg		string	Long message for unifiedStatusInfoType. See [Table of Authentication/Aggregation Status Messages](#) page 51.
activityInProgressStatus		string	Status of authentication or aggregation. "In Progress" or "Complete".
account {			
id	yes	integer	An account identifier assigned by the service.
name		string	Name of the account.
accountType		string	Type of account. See [Table of Account Types](#) page 52.
marketValue {			
amount		number	Total market value of the account.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
lastUpdated		string	Date and time stamp of last update. For example: 2018-05-21 2:52:23 AM.
relativeLastUpdatedText		string	Describes how recently the account was updated, if it was relatively recent. For example, if it updated less than a minute ago, it will indicate it updated just now If it updated between 1 minute and 1 hours, it will indicate how many minutes ago it updated. If it updated more than 24 hours ago, it will give the date it updated.
aggregationStatusErrorCode		integer	Error code from the latest aggregation attempt. *This field can be ignored*. Instead refer to unifiedStatusInfoType and see [Account and Credential Error Information](#) on page 42

Group: Main Group			
Label	**Required ?**	**Type**	**Description**
			regarding best practices on understanding the state of the accounts and credentials.
creationDate		string	Date and time stamp of creation.
maskedAccountNumber		string	The account number is masked, with the last four digits unmasked.
}			
financialInstitution {			
id	yes	integer	The ID of the financial institution.
name		string	Name of the financial institution.
supportsOauth	yes	Boolean	True or false. Indicates whether the FI supports Oauth authorization
loginTerm		string	Term used for the login at this financial institution.
pwTerm		string	Term used for the password at this financial institution.
accountNumberTerm		string	Term used for the account number at this financial institution.
icon		string	The path to the icon for the financial institution. If the financial institution is requested (not supported) it is the path to a default icon.
}]			

Group: FI Request

Group: FI Request			
Label	**Required ?**	**Type**	**Description**
data [{		array	Credential-account pair. Either an account and its related credential or a credential that has no accounts associated with it.
id	yes	integer	ID of the account credential.
group	yes	string	Identifies the group in which the data is organized. Can be one of: NEEDS_USER_ACTION, MAIN_GROUP, IN_PROGRESS, or FI_REQUEST. For this data group the value will be FI_REQUEST.
creationDate		string	Date and time stamp of creation of the FI Request.
fiRequestName		string	Name of the requested financial institution.

Group: FI Request			
Label	**Required ?**	**Type**	**Description**
maskedAccountNumbers			Comma-separated list of masked account numbers. The last four digits remain unmasked.
}]			

Table of Authentication/Aggregation Status Messages

These status types and messages can be in the response of GET /api/v1/credentials/accounts/summary.

unifiedStatusInfoType	unifiedStatusInfoMsg
accountClosed	This account is closed.
aggCannotLoadDataCheckLater	We are having trouble accessing this institution. Please check back later.
badAccountCheckLater	We are having trouble accessing this institution. Check back later.
badAccountVerifyAccountNum	We are having trouble accessing this institution. Check back later.
cannotConnectBadLoginPw	We cannot connect to this institution. The {{loginTerm}} or {{passwordTerm}} is incorrect. Re-authenticate.
cannotConnectBadLoginPwIsac	We cannot connect to this institution. The {{loginTerm}}, {{passwordTerm}}, or activation code is incorrect. Re-authenticate.
cannotConnectBadLoginPwSqa	We cannot connect to this institution. The {{loginTerm}}, {{passwordTerm}}, or answer to a security question is incorrect. Re-authenticate.
cannotConnectBadLoginPwSqaIsac	We cannot connect to this institution. The {{loginTerm}}, {{passwordTerm}}, answer to a security question, or security code is incorrect. Re-authenticate.
cannotConnectMissingAcctNum	We are having trouble accessing this institution. Check back later.
cannotConnectMissingLoginPW	Authenticate to connect.
cannotConnectNotAuthorized	We cannot connect to this institution. Authorize access to connect.
cannotConnectOauthAcctNotAuthorized	Cannot connect. Account is not authorized.
cannotConnectOauthNotConfigured	Further configuration is required to connect to this institution. Contact your aggregation provider for assistance.
cannotConnectUserActionOnetimeCode	To allow the aggregation service to access your accounts, please login on your institution website and turn off the setting that requires identity verification at every login.
cannotConnectUserActionPersonalInfo	This institution requires you to update or verify personal information or preferences on their website and then re-authenticate.
cannotConnectUserActionSecurity	This institution requires you to set up additional security features on their website and then re-authenticate.
cannotConnectUserActionUserAgreement	This institution requires you to accept a user agreement on their website and then re-authenticate.
cannotLoadDataCheckLater	We are having trouble accessing this institution. Check back later.

unifiedStatusInfoType	unifiedStatusInfoMsg
cannotVerifyFiLimitation	We cannot verify your credentials due to institution limitation. Check back later.
credHasNoAccounts	No accounts have been connected. Connect accounts.
filoginCannotConnectBadLoginPw	Cannot connect. The {{loginTerm}} or {{passwordTerm}} is incorrect.
fiNotYetSupported	This institution is not yet supported.
fiRequestMissingElements	Additional inputs are required before this institution request can be processed.
isacCannotConnectBadIsac	Cannot connect. The information you provided is incorrect.
noConnectAttemptYet	Authenticate to connect.
specifiedAccountNotFound	Account not found.
sqaCannotConnectBadSqa	Cannot connect. The answer to a security question is incorrect.

Table of Account Types

Account Type	Group
BANKING_CD	ASSET_BANKING
BANKING_CHECKING	ASSET_BANKING
BANKING_CREDITLINE	LIABILITY_LOAN
BANKING_DEPOSIT	ASSET_BANKING
BANKING_MONEYMARKET	ASSET_BANKING
BANKING_OTHER	ASSET_BANKING
BANKING_SAVINGS	ASSET_BANKING
CREDITCARD	LIABILITY_CREDITCARD
HEALTHACCOUNT_FSA	ASSET_BANKING
HEALTHACCOUNT_HRA	ASSET_BANKING
HEALTHACCOUNT_HSA	ASSET_BANKING
HEALTHACCOUNT_OTHER	ASSET_BANKING
INSURANCE_ANNUITY	ASSET_INSURANCE
INSURANCE_LIFEINSURANCE	ASSET_INSURANCE
INSURANCE_OTHER	ASSET_INSURANCE
INVESTMENT_401A	ASSET_INVESTMENT
INVESTMENT_401K	ASSET_INVESTMENT
INVESTMENT_403B	ASSET_INVESTMENT
INVESTMENT_457B	ASSET_INVESTMENT
INVESTMENT_529	ASSET_INVESTMENT
INVESTMENT_BROKERAGE	ASSET_INVESTMENT
INVESTMENT_CASHMGMT	ASSET_INVESTMENT
INVESTMENT_COVERDELL	ASSET_INVESTMENT
INVESTMENT_IRA	ASSET_INVESTMENT

Account Type	Group
INVESTMENT_KEOGH	ASSET_INVESTMENT
INVESTMENT_MUTUALFUND	ASSET_INVESTMENT
INVESTMENT_OTHER	ASSET_INVESTMENT
INVESTMENT_PENSION	ASSET_INVESTMENT
INVESTMENT_PREPAIDTUITION	ASSET_INVESTMENT
INVESTMENT_PROFITSHARE	ASSET_INVESTMENT
INVESTMENT_RETIREMENT	ASSET_INVESTMENT
INVESTMENT_ROTHIRA	ASSET_INVESTMENT
INVESTMENT_SARSEP	ASSET_INVESTMENT
INVESTMENT_SAVINGSBOND	ASSET_INVESTMENT
INVESTMENT_SEPIRA	ASSET_INVESTMENT
INVESTMENT_TREASURYBOND	ASSET_INVESTMENT
INVESTMENT_TRUST	ASSET_INVESTMENT
INVESTMENT_UGMA	ASSET_INVESTMENT
INVESTMENT_UTMA	ASSET_INVESTMENT
LOAN_AUTO	LIABILITY_LOAN
LOAN_BANK	LIABILITY_LOAN
LOAN_BOAT	LIABILITY_LOAN
LOAN_HOMEEQUITY	LIABILITY_LOAN
LOAN_MORTGAGE	LIABILITY_MORTGAGE
LOAN_OTHER	LIABILITY_LOAN
LOAN_PERSONAL	LIABILITY_LOAN
LOAN_STUDENT	LIABILITY_LOAN
OTHER	ASSET_OTHER
UNKNOWN	ASSET_OTHER

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
400	Bad request		
401	Not Authorized		

HTTP Status Code	Reason	Response Model	Headers
500	Internal Server Error		

PATCH credential

PATCH   /api/v1/credentials/{id}

Implementation Notes

Use this endpoint to update an existing credential.

Request Headers

The PATCH body parameters listed in are to be submitted in JSON format as shown in this example:

PATCH /api/v1/credentials/{id}

```
{
 "accountLogin": "username",
 "accountPin": "pin",
}
```

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id	yes		Id of the credential to modify	path	integer
{			*Credentials provided to BAA for authentication to a third party Financial Institution.*		
name			Name of the Account Credential. It is not recommended that you update the value of this field.	body	string
fiId			ID of the Financial Institution. It is not recommended that you update the value of this field.	body	integer
accountLogin			Account Login	body	string

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
accountLogin2			Account Login 2	body	string
accountPin			Account PIN	body	string
accountSecondPin			Account Second PIN	body	string
}					

Response Body

None

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

DELETE credentials

DELETE /api/v1/credentials/{id}

Implementation Notes

This endpoint deletes the credentials specified by the *id* parameter. All accounts associated with the credentials are also deleted from the system.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id	yes		Unique identifier of the credential	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
204	No Content		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

Credential Authentication Operations

POST user inputs

POST /api/v1/authentications/{ticketId}/userinputs

Implementation Notes

Use this endpoint to sends the keepalive request to the user input process No POST body is required and none is returned.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticketId	yes		Unique identifier associated with this authentication (provided as part of URL in Location header when authentication operation is first submitted)	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
204	No Content		
401	Not Authorized		
404	If the ticket is not found or if there were never any user input prompts associated with this ticket		
410	Gone: returned if the ticket is valid and there was previously a user input prompt available but it is no longer available (this will be returned if the keep-alive is sent too late)		
500	Internal Server Error		

POST a new request for authentication

POST /api/v1/credentials/{credentialId}/authenticate

Implementation Notes

Use this endpoint to initiate the authentication operation for the credential specified by 'credentialId'. This operation does not require any payload nor does it return one. On success (200) the Location header will contain the temporary location to use to poll for status.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
allowUserInput		false	True if In-Session Activation Code (ISAC) prompts should be allowed.	query	Boolean
credentialId	Yes		The identifier of the credential for which to initiate authentication.	path	integer
startOauth		false	True indicates that OAuth should be initiated if this is an OAuth credential. The setting has no effect for non-OAuth credentials.	query	Boolean
oauthRedirectURL			Use in the body of the POST to specify a URL that should be redirected to after the user has completed OAuth authorization at the Financial Institution's web site. If not provided, then no redirect is issued and a self-closing HTML page is returned from the OauthCallbackHandler.	body	string
oauthRedirectType			Use in the body of the POST to specify the type of redirect (client or server) to use for oauthRedirectURL. ▪ "client" – When the OauthCallbackHandler is invoked at the end of the OAuth flow, an HTML page containing a JavaScript redirect to the oauthRedirectURL is returned	body	string

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
			(this is also the default behavior if oauthRedirectURL was specified and oauthRedirectType was not specified). ■ "server" – When the OauthCallbackHander is invoked at the end of the OAuth flow, an HTTP 302 redirect to the oauthRedirectURL is returned.		

Response Messages

HTTP Status Code	Reason	Response Model	Headers

200	OK	{
		  "data": {}
		}	

400	Bad Request. Additional detailed error types provided in response. Possible causes include: ■ startOauth is required for Oauth credentials ■ Credential is Oauth-type but FI does not support Oauth		
401	Not Authorized		
404	Credential Not Found		
500	Internal Server Error		

GET authentication result

GET/api/v1/authentications/{ticket}

Implementation Notes

Use this endpoint to obtain the current result of a credential authentication operation.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticket	yes		Universal unique identifier associated with this authentication. It is provided as part of the URL in the Location header when the authentication operation is first submitted.	path	string

Response Body

The response body can take various forms. The following examples show some of the most common response forms.

Example 1 – authentication failure due to bad login or password

```
{
  "status": "Complete",
  "statusTimestamp": "2019-04-15 14:26:24 PM",
  "credentialId": 23736,
  "authenticationStatusErrorCode": 1007,
  "authenticationStatusInfoType": "filoginCannotConnectBadLoginPw",
  "authenticationStatusInfo": "Cannot connect. The Login or Password is incorrect.",
  "lastAuthenticationAttempt": "2019-04-15 12:00:00 AM"
}
```

Example 2 – authentication failure due to security question:

```
{
  "status": "Complete",
  "statusTimestamp": "2019-04-15 14:26:29 PM",
  "credentialId": 23737,
  "authenticationStatusErrorCode": 1007,
  "authenticationStatusInfoType": "sqaCannotConnectBadSqa",
  "authenticationStatusInfo": "Cannot connect. The answer to a security question is incorrect.",
  "lastAuthenticationAttempt": "2019-04-15 12:00:00 AM",
```

```
    "sqa": [
     {
       "id": 85542,
       "question": "In what city did you meet your spouse for the first time?",
       "answer": ""
     }
    ]
   }
```

Example 3 – in session activation code (ISAC) challenge encountered:

```
   {
     "status": "Waiting for User Input",
     "statusTimestamp": "2019-04-29 08:40:46 AM",
     "credentialId": 24251,
     "userInput": [
      {
        "inputType": "instructions",
        "instructionText": "The institution needs to send you an identification code."
      },
      {
        "inputType": "instructions",
        "instructionText": "This is a time-sensitive process that may require more input from you."
      },
      {
        "inputType": "instructions",
        "instructionText": "Choose how you would like to receive the code:"
      },
      {
        "inputType": "inputText",
        "instructionText": "Use the code 'ABC123', otherwise a 1007 error will be returned.",
        "identifier": 1,
        "label": "Enter Code : ",
        "value": ""
      },
      {
        "inputType": "inputCheckbox",
        "instructionText": "Check the box, otherwise a 1007 error will be returned.",
        "identifier": 2,
        "label": "2345",
        "value": false
      },
      {
        "inputType": "inputRadioGroup",
```

```
      "identifier": 3,
      "inputRadio": [
       {
         "instructionText": "Select one of the options, otherwise a 1007 will be returned",
         "identifier": 4,
         "label": "xxbar@xxxxxxfoobar.com"
       },
       {
         "identifier": 5,
         "label": "XXX-XXX-7890"
       }
      ]
     },
     {
       "inputType": "instructions",
       "instructionText": "If none of the above methods work, please contact technical support for
   assistance."
     }
    ],
    "userInputURI":
   "https://www.byallaccounts.net/api/v1/authentications/6916770705117946947/userinputs",
    "userInputTimeoutInterval": 180000,
    "userInputExpirationTime": "2019-04-29 08:40:46 AM"
   }
```

Example 4 – OAUTH Initiated:

```
   {
      "status": "Waiting for Oauth",
      "statusTimestamp": "2023-10-17T14:54:45.293-04:00",
      "credentialId": 83568,
      "oauthMicrositeURL":
   "https://www.byallaccounts.net/WebPortfolio/OauthMicrosite.html?response_type=code&redirect_uri=htt
   ps://www.byallaccounts.net/WebPortfolio/OAUTHCallback&client_id=dbutil_clientId&state=d72424bc-
   0d83-4283-9dee-30af9d8e657d",
      "oauthExpirationTime": "2023-10-17T15:04:32.000-04:00",
      "next": "/api/v1/authentications/2797095223623863796"
   }
```

Response Model

The response structure is as follows.

Note: Different sets of these items will appear in the response depending on the error or security challenge encountered. See the examples in [Response Body](#) 60 for some of the possible groupings.

Label	Req'd?	Type	Description
{			*Credential Authentication final result object*
status	yes	string	Status of the authentication. Examples: "Complete" or "Waiting for User Input", or "Waiting for OAuth".
statusTimestamp	yes	string	Status timestamp
credentialId	yes	integer	Account Credential ID associated with this authentication
authenticationStatusErrorCode		integer	Status code from the authentication operation; 1006 indicates success
authenticationStatusInfoType		string	Type of status information from the latest authentication attempt. For example: *cannotConnectMissingLoginPW*
authenticationStatusInfo		string	Status info from the authentication operation (populated only if an error occurred). For example: "Cannot connect. The Login or Password is incorrect.",
lastAuthenticationAttempt		string	Date of the last authentication attempt. For example: *2023-05-21 2:52:23 AM*
oauthMicrositeURL {			
uri		string	The URL to the FIs OAuth Microsite.
}			
oauthExpirationTime		string	The time at which the OAuth expires. For example: *2023-10-17T15:04:32.000-04:00*
next {			
uri		string	The URI for the GET /authentications/{ticket} to poll for when the authentication is n the "Waiting for Oauth" state.
}			
sqa [{			*Security question that requires updating. Only included if a SQA issue caused an error.*
id		integer	ID of the Security Question and Answer (SQA)
question		string	The security question from the Financial Institution. Read only. Example: *In what city did you meet your spouse for the first time?*
answer		string	The answer to the security question. Read only. Example: Boston
}]			

Label	Req'd?	Type	Description
userInput [{			*User Input Prompt; only valued if status is 'Waiting for User Input'*
inputType	yes	string	Input type of the user input. For example: *inputCheckbox, inputRadioGroup*, *instructions*, or *inputText*. Refer to Userinput JSON, page 14
instructionText		string	Instruction text for the user input
identifier	yes	integer	Identifier of the user input
label		string	Label of the user input
value		string	*Pre-selected value for the User Input, if any*
inputRadio [{			*Only used when inputType is inputRadioGroup.*
identifier		integer	Identifier of the user input
instruction Text		string	Instruction text for the user input
label		string	Label of the user input
}]			
}]			
userInputTimeoutInterval		integer	User Input Timeout Interval is the interval of time in seconds in which a keep alive request or the user input result should be submitted. Only valued if status is 'Waiting for User Input'
userInputExpirationTime		string	User Input Expiration Time is the time after which ISAC will timeout regardless of whether it has been kept alive with keep alive requests. Only valued if status is 'Waiting for User Input'
userInputURI {			
uri		string	URI for the currently active userinput request, if any. This URI is relative.
}			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See Response Model, page 63	

HTTP Status Code	Reason	Response Model	Headers
400	Bad Request		
401	Not Authorized		
403	Forbidden		
500	Internal Server Error		

GET user inputs

GET /api/v1/authentications/{ticketId}/userinputs

Implementation Notes

Use this endpoint to retrieve the user input prompt if available.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticketId	yes		Unique identifier associated with this authentication (provided as part of URL in Location header when authentication operation is first submitted)	path	integer

Response Body

```
{
  "status": "Waiting for User Input",
  "statusTimestamp": "2019-04-29 08:40:46 AM",
  "credentialId": 24251,
  "userInput": [
   {
     "inputType": "instructions",
     "instructionText": "The institution needs to send you an identification code."
   },
   {
```

```json
      "inputType": "instructions",
      "instructionText": "This is a time-sensitive process that may require more input from you."
    },
    {
      "inputType": "instructions",
      "instructionText": "Choose how you would like to receive the code:"
    },
    {
      "inputType": "inputText",
      "instructionText": "Use the code 'ABC123', otherwise a 1007 error will be returned.",
      "identifier": 1,
      "label": "Enter Code : ",
      "value": ""
    },
    {
      "inputType": "inputCheckbox",
      "instructionText": "Check the box, otherwise a 1007 error will be returned.",
      "identifier": 2,
      "label": "2345",
      "value": false
    },
    {
      "inputType": "inputRadioGroup",
      "identifier": 3,
      "inputRadio": [
        {
          "instructionText": "Select one of the options, otherwise a 1007 will be returned",
          "identifier": 4,
          "label": "xxbar@xxxxxxfoobar.com"
        },
        {
          "identifier": 5,
          "label": "XXX-XXX-7890"
        }
      ]
    },
    {
      "inputType": "instructions",
      "instructionText": "If none of the above methods work, please contact technical support for
assistance."
    }
  ],
```

```
    "userInputURI":
  "https://www.byallaccounts.net/api/v1/authentications/6916770705117946947/userinputs",
    "userInputTimeoutInterval": 180000,
    "userInputExpirationTime": "2019-04-29 08:40:46 AM"
  }
```

Response Model

The response structure is as follows.

Label	Req'd?	Type	Description
{			
userInput [{			
inputType	yes	string	Input type of the user input. For example: *inputCheckbox, inputRadioGroup*, *instructions*, or *inputText*. Refer to Userinput JSON, page 14
instructionText		string	Instruction text for the user input
identifier	yes	integer	Identifier of the user input
label		string	Label of the user input
value		string	*Pre-selected value for the User Input, if any*
inputRadio [{			*Only used when inputType is inputRadioGroup.*
identifier		integer	Identifier of the user input
instruction Text		string	Instruction text for the user input
label		string	Label of the user input
}]			
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See Response Model, page 67	
401	Not Authorized		

HTTP Status Code	Reason	Response Model	Headers
404	If the ticket is not found or if there were never any user input prompts associated with this ticket		
410	Gone: returned if the ticket is valid and there was previously a user input prompt available, but it is no longer available		
500	Internal Server Error		

PATCH user input result

PATCH /api/v1/authentications/{ticketId}/userinputs

Implementation Notes

Use this endpoint to submit the user input result to the user input interaction.

Request Headers

The PATCH body parameters listed in are to be submitted in JSON format as shown in this example:

```
PATCH /api/v1/authentications/{ticketId}/userinputs
{
  "userInput": [
   {
     "inputRadio": [
       {
         "identifier": 1,
         "instructionText": "Use the code 'ABC123', otherwise a 1007 error will be returned.",
         "label": "xxbar@xxxxxxfoobar.com"
       }
     ],
     "inputType": "inputCheckbox",
     "instructionText": "Use the code 'ABC123', otherwise a 1007 error will be returned.",
     "identifier": 1,
     "label": "xxbar@xxxxxxfoobar.com",
     "value": false
```

```
      }
    ]
  }
```

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticketId	yes		Unique identifier associated with this authentication (provided as part of URL in Location header when authentication operation is first submitted)	path	integer
identifier			Identifier of the User Input	body	integer
instructionText			Instruction text for the user input	body	string
label			Label of the User Input	body	string
inputType	yes		Input type of the user input	body	string
instructionText			Instruction text for the user input	body	string
identifier			Identifier of the User Input	body	integer
label			Label of the User Input	body	string
value			Pre-selected value for the User Input, if any	body	string

Response Body

The location of the authentication:

```
  (
  /api/v1/authentications/{ticketId}
  }
```

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	{	

HTTP Status Code	Reason	Response Model	Headers
		"authenticationURI": "/api/v1/authentications/X XXXXXXXXXXXXXXXX" }	
204	No Content	{ "authenticationURI": "/api/v1/authentications/X XXXXXXXXXXXXXXXX" }	
401	Not Authorized		
404	If the ticket is not found or if there were never any user input prompts associated with this ticket		
410	Gone: returned if the ticket is valid and there was previously a user input prompt available, but it is no longer available		
500	Internal Server Error		

DELETE the authentication operation

DELETE /api/v1/authentications/{ticketId}

Implementation Notes

Use this endpoint to cancel the authentication operation identified by ticketId. The authentication will no longer be retrievable.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticketId	yes		Universal unique identifier associated with this authentication. It is provided as part of the URL in the Location header when the authentication operation is first submitted.	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
204	No Content		
401	Not Authorized		
403	Forbidden		
500	Internal Server Error		

DELETE user input interaction

DELETE /api/v1/authentications/{ticketId}/userinputs

Implementation Notes

Use this endpoint to send the quit command to the user input process. The authentication will proceed without the user input and an error will occur. The user input itself will no longer be retrievable

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
ticketId	yes		Unique identifier associated with this authentication (provided as part of URL in Location header when authentication operation is first submitted)	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
204	No Content		
401	Not Authorized		
404	If the ticket is not found or if there were never any user input prompts associated with this ticket		
410	Gone: returned if the ticket is valid and there was previously a user input prompt available, but it is no longer available		
500	Internal Server Error		

Discovery Operations

POST initiate account discovery for a specific credential

POST /api/v1/credentials/{credentialId}/discover

Implementation Notes

Use this endpoint to initiate the discovery operation for the credential specified by 'credentialId'. This operation does not require any payload nor does it return one. On success (201) the Location header will contain the temporary location to use to poll for status.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
credentialId	yes		The identifier of the credential for which to initiate authentication.	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
201	Created		On success, the Location header will contain the URL of the temporary resource for polling
400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

POST discovered bulk accounts of a specific credential

POST /api/v1/credentials/{id}/discovered-accounts

Implementation Notes

Use this endpoint to submit a new request for bulk addition of accounts discovered using the specific id of a credential. Adds either all or a subset of the accounts discovered during a discovery operation for the credential. On success (201) returns a list of account URIs for the created accounts.

Request Headers

The POST body parameters listed in are to be submitted in JSON format as shown in these examples:

Example 1 – request to add specific accounts from the discovery

```
{
  "discoveryTicket": 8652308551851687000,
  "discoveredAccounts": [
   {
     "id": 12484
   },
    { "id": 12485
   }
  ]
}
```

Example 2 – request to add all discovered accounts

```
POST /api/v1/credentials/{id}/discovered-accounts
{
  "discoveryTicket": 8652308551851687000,
}
```

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
discoveryTicket	yes		The discoveryTicket containing the accounts you want to add.	body	string
id			ID of the discovered account that you want added to the system	body	integer

Response Body

```
{
  "uriList": [
   "https://www.byallaccounts.net/api/v1/accounts/123456",
   "https://www.byallaccounts.net/api/v1/accounts/123455",
   "https://www.byallaccounts.net/api/v1/accounts/123454"
  ]
}
```

Response Messages

HTTP Status Code	Reason	Response Model	Headers

200	OK	{
		  "data": {}
		}	

201	On success, indicates successful creation of the accounts	{
		  "data": {}
		}	

400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

GET discovery result

GET /api/v1/discoveries/{ticket}

Implementation Notes

Use this endpoint to obtain the result of a discovery operation. Account discovery cannot be performed on a credential of type OAUTH. The discovery operation requires authenticating to the Financial Institution. If this authentication fails error information is returned in the response, however, you must use other operations to re-attempt the authentication and work through errors and security challenges. Once the authentication is successful you can retry this operation.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
page		0	Page number.	query	integer
size		25	Number of records per page.	query	integer
ticket	yes		Universal unique identifier associated with this account discovery. It is provided as part of the URL returned in the Location header when an account discovery operation was first submitted.	path	string

Response Body

Once the discovery is complete the response will be as follows:

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 1,
  "totalElements": 5,
  "isFirst": true,
  "isLast": true,
  "summary": {
    "status": "Complete",
    "statusTimestamp": "2021-10-20T12:06:04.345-04:00",
    "accountDiscoveryStatusErrcode": 1005,
    "accountDiscoveryStatusTimestamp": "2020-10-30T22:00:12.000-04:00",
    "credentialId": 52086
  },
  "data": [
    {
      "id": 6266936,
      "name": "Test Account-1 XXXXX6789",
      "accountNumber": "123456789"
    },
    {
      "id": 6266937,
      "name": "Test Account-2 XXXXX4321",
      "accountNumber": "987654321"
    },
```

```
    {
      "id": 6266938,
      "name": "Test Account-3 XXXXX5666",
      "accountNumber": "444555666"
    },
    {
      "id": 6266939,
      "name": "Joe & Jennifer's Individual Retirement Account",
      "accountNumber": "Joe & Jennifer's IRA"
    },
    {
      "id": 6266940,
      "name": "Account with lt and gt symbols in it: x<2,x>0. XXXXXX2653",
      "accountNumber": "3141592653"
    }
  ]
}
```

Here is an example of a failed Account Discovery response:

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 0,
  "totalElements": 0,
  "isFirst": true,
  "isLast": true,
  "summary": {
    "status": "Complete",
    "statusTimestamp": "2021-11-04T15:26:28.183-04:00",
    "accountDiscoveryStatusErrcode": 1007,
    "unifiedStatusInfoType": "cannotConnectBadLoginPwSqa",
    "unifiedStatusInfoMsg": "We cannot connect to this institution. The Login, Password, or answer to a
security question is incorrect. Re-authenticate.",
    "accountDiscoveryStatusTimestamp": "2021-11-04T15:26:23.000-04:00",
    "credentialId": 53627
  },
  "data": []
}
```

Response Model

The response structure is as follows.

Label	Req'd?	Type	Description
{			A page of data records
pageSize		integer	Number of records per page
pageNumber		integer	Page number of this page
totalPages		integer	Total number of pages in result set
totalElements		integer	Total number of elements in result set
isFirst		Boolean	True if and only if this is the first page of data in the result set
isLast		Boolean	True if and only if this is the last page of data in the result set
summary {			
status	yes	string	Account Credential ID associated with this authentication
statusTimestamp	yes	string	Status timestamp. For example: 2023-05-24T01:23:45.67 -0400
accountDiscoveryStatusErrcode	yes	integer	Status code for the account discovery operation; will be null (absent) if account discovery not performed
unifiedStatusInfoType		string	Type of status information from the latest authentication attempt. For example: cannotConnectMissingLoginPW
unifiedStatusInfoMsg		string	Status information from the latest authentication attempt (simplified). Example: Cannot connect. Missing Login or Password.
accountDiscoveryStatusTimestamp			Status info for the account discovery operation; will be null (absent) if account discovery not performed. For example: 2023-05-24T01:23:45.67 -0400
credentialId		integer	ID of the Account Credential
}			
data [{			
id	yes	integer	Unique ID of this Account
name	yes	string	The name of this Account
accountNumber		string	The Account Number for this Account
accountNumber2		string	The second Account Number for this Account
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See [Response Model, page 77](#)	
400	Bad Request		
401	Not Authorized		
403	Forbidden		
404	Not Found		
500	Internal Server Error		

Financial Institution Operations

GET Financial Institution

GET /api/v1/fis

Implementation Notes

This operation retrieves the collection of Financial Institutions (FIs).

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
name			Financial institution name search. Search criteria is a contains-type match, meaning the search string is somewhere in the FI name.	query	string
nameUserLoginURL			Financial institution name plus the user login URL search. Search criteria is a contains-type match, meaning the search string is somewhere in the FI name.	query	string
page		0	Page number.	query	integer
size		25	Number of records per page.	query	integer

Response Body

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 1,
  "totalElements": 1,
  "isFirst": true,
  "isLast": true,
  "summary": {},
  "data": [
{
  "id": 43154,
  "name": "Data Test 1 - 401(k)",
```

```
  "userLoginURL": http://localhost/,
  "popularity": 0,
  "popularityConsumer": 0,
  "loginTerm": "Login",
  "pwTerm": "Password",
  "accountNumberTerm": "Account Number",
  "loginTermDetails": "Enter any value",
  "pwTermDetails": "Enter any value",
  "accountNumberTermDetails": "This must be a non-blank value.",
  "accessInstructions": " This is a Test FI that contains sample 401(k) data for one account. ",
  "supportsAccountDiscovery": true,
  "supportsOAuth": false,
  "supportsTestCredential": true,
  "requiresInSessionActivation": false,
  "requiresSQA": false,
  "requiresSecondPW": false,
  "logo": https://localhost/WPDemo/vendorResources/Default/assets/fi/logos/DataTest1401k_logo.svg,
  "icon": https://localhost/WPDemo/vendorResources/Default/assets/fi/icons/DataTest1401k_icon.png,
  "licensed": true
}
    ]
    }
```

Response Model

Label	Req'd?	Type	Description
{			
pageSize		integer	Number of records per page.
pageNumber		integer	Page number of this page.
totalPages		integer	Total number of pages in result set.
totalElements		integer	Total number of elements in result set.
isFirst		Boolean	True or false. True if and only if this is the first page of data in the result set.
isLast		Boolean	True or false. True if and only if this is the last page of data in the result set.
summary			
data [{			Financial Institution list
id	yes	integer	ID of the Financial Institution
name	yes	string	Name of the Financial Institution
userLoginURL	yes	string	User login URL of the Financial Institution
websiteURL		string	Home page of the Financial Institution

Label	Req'd?	Type	Description
popularity	yes	integer	Popularity of the Financial Institution, with larger values indicating higher popularity level (currently always either 0 or 1, but other values possible in the future)
popularityConsumer	yes	integer	Popularity of the Financial Institution at Consumer UI, with larger values indicating higher popularity level (currently always either 0 or 1, but other values possible in the future)
loginTerm	yes	string	The term used for login at the Financial Institution
login2Term		string	The term used for second login at the Financial Institution
pwTerm	yes	string	The term used for PIN at the Financial Institution
pw2Term		string	The term used for second PIN at the Financial Institution
accountNumberTerm	yes	string	The term used for Account Number at the Financial Institution
accountNumber2Term		string	The term used for second Account Number at the Financial Institution
loginTermDetails	yes	string	Detailed instructions for the login field at this Financial Institution
login2TermDetails		string	Detailed instructions for the second login field at this Financial Institution
pwTermDetails	yes	string	Detailed instructions for the PIN field at this Financial Institution
pw2TermDetails		string	Detailed instructions for the second PIN field at this Financial Institution
accountNumberTermDetails	yes	string	Detailed instructions for the Account Number field at this Financial Institution
accountNumber2TermDetails		string	Detailed instructions for the second Account Number at this Financial Institution
accessInstructions	yes	string	Detailed general access instructions for this Financial Institution
supportsAccountDiscovery	yes	Boolean	Indicates whether the Financial Institution supports automatic discovery of accounts at the Financial Institution.
supportsOAuth	yes	Boolean	Indicates whether the Financial Institution supports OAuth authentication.
supportsTestCredential	yes	Boolean	Indicates whether the Financial Institution supports testing access to the Financial Institution with only credential (and not account) data
requiresInSessionActivation	yes	Boolean	Indicates whether the Financial Institution whether the Financial Institution may potentially prompt for In-Session Activation Codes during Test Credential or Test Account operations

Label	Req'd?	Type	Description
requiresSQA	yes	Boolean	Indicates whether the Financial Institution may require security questions and answer input from the user in order to access the site
requiresSecondPW	yes	Boolean	Indicates whether the Financial Institution requires the second PIN term
setupInstructions		string	The financial institution instructions for setting up accounts at the FI for aggregation
knownConnectionIssue		string	Known connectivity issue for the FI or third party
configuredOAuth		Boolean	Indicates whether the OAuth Credential has been configured for the Financial Institution.
logo		string	The name used for logo at the respective Financial Institution
icon		string	The name used for icon at the respective Financial Institution
knownConnectionIssueLongTerm		string	Known connectivity issue long term for the FI or third party
licensed		Boolean	Indicates whether the Financial Institution is licensed for the user's firm
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See [Response Model](#) on page 81	
400	Bad Request		
401	Not Authorized		
500	Internal Server Error		

GET Financial Institution by ID

GET /api/v1/fis/{id}

Implementation Notes

This operation retrieves a financial institution by ID.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id			The ID of the Financial institution requested	query	integer

Response Body

```
{
  "id": 43154,
  "name": "Data Test 1 - 401(k)",
  "userLoginURL": http://localhost/,
  "popularity": 0,
  "popularityConsumer": 0,
  "loginTerm": "Login",
  "pwTerm": "Password",
  "accountNumberTerm": "Account Number",
  "loginTermDetails": "Enter any value",
  "pwTermDetails": "Enter any value",
  "accountNumberTermDetails": "This must be a non-blank value.",
  "accessInstructions": " This is a Test FI that contains sample 401(k) data for one account. ",
  "supportsAccountDiscovery": true,
  "supportsOAuth": false,
  "supportsTestCredential": true,
  "requiresInSessionActivation": false,
  "requiresSQA": false,
  "requiresSecondPW": false,
  "logo": https://localhost/WPDemo/vendorResources/Default/assets/fi/logos/DataTest1401k_logo.svg,
  "icon": https://localhost/WPDemo/vendorResources/Default/assets/fi/icons/DataTest1401k_icon.png,
  "licensed": true
}
```

Response Model

Label	Req'd?	Type	Description
{			
id	yes	integer	ID of the Financial Institution
name	yes	string	Name of the Financial Institution
userLoginURL	yes	string	User login URL of the Financial Institution
websiteURL		string	Home page of the Financial Institution
popularity	yes	integer	Popularity of the Financial Institution, with larger values indicating higher popularity level (currently always either 0 or 1, but other values possible in the future)
popularityConsumer	yes	integer	Popularity of the Financial Institution at Consumer UI, with larger values indicating higher popularity level (currently always either 0 or 1, but other values possible in the future)
loginTerm	yes	string	The term used for login at the Financial Institution
login2Term		string	The term used for second login at the Financial Institution
pwTerm	yes	string	The term used for PIN at the Financial Institution
pw2Term		string	The term used for second PIN at the Financial Institution
accountNumberTerm	yes	string	The term used for Account Number at the Financial Institution
accountNumber2Term		string	The term used for second Account Number at the Financial Institution
loginTermDetails	yes	string	Detailed instructions for the login field at this Financial Institution
login2TermDetails		string	Detailed instructions for the second login field at this Financial Institution
pwTermDetails	yes	string	Detailed instructions for the PIN field at this Financial Institution
pw2TermDetails		string	Detailed instructions for the second PIN field at this Financial Institution
accountNumberTermDetails	yes	string	Detailed instructions for the Account Number field at this Financial Institution
accountNumber2TermDetails		string	Detailed instructions for the second Account Number at this Financial Institution
accessInstructions	yes	string	Detailed general access instructions for this Financial Institution
supportsAccountDiscovery	yes	Boolean	Indicates whether the Financial Institution supports automatic discovery of accounts at the Financial Institution.
supportsOAuth	yes	Boolean	Indicates whether the Financial Institution supports OAuth authentication.

Label	Req'd?	Type	Description
supportsTestCredential	yes	Boolean	Indicates whether the Financial Institution supports testing access to the Financial Institution with only credential (and not account) data
requiresInSessionActivation	yes	Boolean	Indicates whether the Financial Institution whether the Financial Institution may potentially prompt for In-Session Activation Codes during Test Credential or Test Account operations
requiresSQA	yes	Boolean	Indicates whether the Financial Institution may require security questions and answer input from the user in order to access the site
requiresSecondPW	yes	Boolean	Indicates whether the Financial Institution requires the second PIN term
setupInstructions		string	The financial institution instructions for setting up accounts at the FI for aggregation
knownConnectionIssue		string	Known connectivity issue for the FI or third party
configuredOAuth		Boolean	Indicates whether the OAuth Credential has been configured for the Financial Institution.
logo		string	The name used for logo at the respective Financial Institution
icon		string	The name used for icon at the respective Financial Institution
knownConnectionIssueLongTerm		string	Known connectivity issue long term for the FI or third party
licensed		Boolean	Indicates whether the Financial Institution is licensed for the user's firm
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See [Response Model](#) on page 85	
400	Bad Request		
401	Not Authorized		

HTTP Status Code	Reason	Response Model	Headers
404	Not Found		
500	Internal Server Error		

Person Operations

POST new Person

POST /api/v1/persons

Implementation Notes

Add an Investor Person to the system and associate it to a Firm and optionally to an Advisor. Registering a new Person does not require prior authentication.

Notes:

- The Firm to which the Person is to be added must have the 'Investor self-signup" feature enabled.
- The user is created as SSO or non-SSO as determined by the Firm's configuration for creating new "clients".

Request Headers

Registering a new Person does not require prior authentication, so JSESSIONID or CSRF-TOKEN are not required.

A UIM Admin JWT can optionally be submitted to this endpoint using the Authorization header with the header value "Bearer <token-value>". The UIM Admin JWT holds a Service Administrator level authentication context and the uimGuid for the user to be created must be provided in the post body. The endpoint will validate the JWT, extract the UIM Guid, and store the UIM Guid on the Person. The UIM Guid must be unique across the ByAllAccounts system (across all Persons). If not, then the Person is not created and HTTP 409 Conflict is returned with the person URI.

The POST body parameters listed in [Parameters](#), page 89 are to be submitted in in JSON format as shown in this example:

```
POST /api/v1/persons
{
        "firstName" : "Chris",
         "middleName" : "Pat",
         "lastName" : "Smith",
         "role" : "investor",
         "emailAddress" : "ChisSmith@email.com",
         "phoneNumber" : "6035551212",
         "taxId" : "111111111",
         "firmCode" : "ABC-12345",
         "advisorId" : 123
}
```

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
firstName	yes		First name of the Person.	body	string
middleName	no		Middle name of the Person.	body	string
lastName	yes		Last name of the Person.	body	string
Role	yes		Role of the Person. Currently must be value "".	body	string
emailAddress	yes		Email address of the Person. Must be in the form xx@yy.zzz.	body	string
phoneNumber	no		Phone number of the Person. There are no format requirements.	body	string
taxId	yes*		Social Security Number or Tax ID of the Person	body	string
firmTag1	yes*		Firm tag 1. If specified, the value must be unique within the Firm to which the new Person is to be added. If not, HTTP 409 Conflict is returned.	body	string
firmTag2	yes*		Firm tag 2.	body	string
firmTag3	yes*		Firm tag 3.	body	string
firmCode	yes**		Vendor name value for the Firm to which this Investor should be added. The Firm must already exist.	body	string
advisorId	yes**		BAA Person Id for the Advisor to whom this Investor should be assigned after the Investor is created. The Advisor must already exist and be part of the Firm identified in firmCode (if firmCode is specified).	body	integer
uimGuid	yes***		Used in conjunction with Service Admin JWT. The uimGuid for the user to be created. Must be unique across all Persons in the ByAllAccounts system. If not, HTTP 409 Conflict is returned with the person URI. Ignored if a valid Service Admin JWT is not provided.	body	string

*   Only required if the Firm configuration requires a value for this field

**   At least one of these must be specified in order identify to which firm to add the Person. If firmCode is specified and advisorId is not, then the Person is created without any association to an advisor. If both are specified, then they must not conflict, meaning the Advisor identified by advisorId must exist within the Firm identified by the firmCode. Otherwise, an HTTP 400 Bad Request is returned.

*** Required when a Service Admin JWT is submitted to the endpoint.

Response Body

Location header: URI to new resource. For example:

```
{
  "uri": "https://www.byallaccounts.net/api/v1/persons/12345"
}
```
Where 12345 is the BAA Person Id for the new Person.

Response Messages

HTTP Status Code	Reason	Response Model	Headers

201	Created	{
		 "data": {}
		 }	

400	Bad Request
	 Possible causes:
	 ▪ The <field name> field is missing
	 ▪ Missing required value
	 ▪ The <field name> cannot exceed <max>
	 ▪ Invalid Role value
	 ▪ Email addresses must be in the form x@x.x and cannot contain spaces
	 ▪ Firm <firm> not found
	 ▪ Advisor not found. [See Cases where advisor is not found below]
	 ▪ One of these is set on the Firm to be required but is not found
	      o taxId
	      o firmTag1
	      o firmTag2
	      o firmTag3		

401	Not Authorized Possible causes: ▪ Investor self-signup not allowed. ▪ UIM JWT not valid.		
409	Conflict Possible causes: ▪ UIM Guid must be unique (from UIM JWT). ▪ firmTag1 must be unique.		
500	Internal Server Error		

Cases where advisor is not found

Case 1: Response when "Advisor advisorId does not exist at Firm firmCode"

```
{
  "type": "invalid-advisorid",
  "title": "Advisor not found",
  "detail": "Person validation error",
  "additionalInfo": {
    "firmCode": "ABC-12345",
    "advisorId": 65376
  }
}
```

Case 2: Response when "advisorId does not exist." OR "advisorId is valid, but is not an advisor"

```
{
  "type": "invalid-advisorid",
  "title": "Advisor not found",
  "detail": "Person validation error",
  "additionalInfo": {
    "advisorId": 65376
  }
}
```

GET persons ID

GET /api/v1/persons/{id}

Implementation Notes

Use this endpoint to fetch the profile data of a Person specified by the *id* parameter.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id	yes		ID of the Person requested.	path	integer

Response Body

```
{
  "id": 778899,
  "firstName": "Rosalind",
  "middleName": "Elsie",
  "lastName": "Franklin",
  "emailAddress": "RosalindFranklin@email.com",
  "phoneNumber": 5085551212,
  "taxId": 101896403,
  "isSSOUser": true,
  "advisorId": true,
  "firmTag1": "xxx",
  "firmTag2": "yyy",
  "firmTag3": "ZZZ",
  "userAgreementAccepted": true,
  "uimGuid": "C5E883D3-8B92-438C-A43B-E70455FA1F06"
}
```

Response Model

Label	Req'd?	Type	Description
{			
id	yes	integer	ID of the Person
firstName	yes	string	First name of the Person
middleName		string	Middle name of the Person
lastName	yes	string	Last name of the Person
emailAddress		string	Email address of the Person
phoneNumber		string	Phone number of the Person

Label	Req'd?	Type	Description
taxID		string	Social Security Number or Tax ID of the Person
isSSOUser		Boolean	True if Person is an SSO-enabled user
advisorID		integer	ID of the Person's advisor
firmTag1		string	Firm Tag 1
firmTag2		string	Firm Tag 2
firmTag3		string	Firm Tag 3
userAgreementAccepted	yes	Boolean	Indicates whether or not the user agreement has been accepted
uimGuid		string	UIM Guid for the Person if one was assigned at creation
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok		
401	Not Authorized Possible reasons: Invalid JSESSIONID and/or CSRF-TOKEN, expired UIM JWT		
404	Not Found		
500	Internal Server Error		

GET person networth

GET /api/v1/persons/me/networth

Implementation Notes

Use this endpoint to get a person's net worth, net and percentage change in net worth, and the net worth trend data for the specified period. These details are computed using the history of a user's accounts currently available in the system.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
dateFrom	*		Start date for the net worth data (inclusive). Specify the date in yyyy-mm-dd format. When set, *dateTo* must be set.	query	string
dateTo	*		End date for the net worth data (exclusive). Specify the date in yyyy-mm-dd format. When set, *dateFrom* must be set.	query	string
period	*		Period to specify the date range for the net worth data. Possible values are: ▪ **1M** - to get the details for a 1-month period ▪ **3M** - to get the details for a 3-month period ▪ **YTD** - to get the details for a year-to-date period ▪ **1Y** - to get the details for a 1-year period ▪ **ALL** - to get the details using all available data The latest data point is computed using the closing values from yesterday. The retrospective period date is based on the date for the day before yesterday.	query	string

* Either the *period* parameter or the combination of the *dateFrom* and *dateTo* parameters must be used to define the time frame for which the net worth is requested. When used, parameters *dateFrom* and *dateTo* must be used in combination. If one is specified, the other is required. If values are given for all parameters, the *period* takes precedence.

Response Body

```json
{
  "netWorth": {  "amount": 150000.00,  "currencyCode": "USD" },
  "netChange": {   "amount": 50000.00, "currencyCode": "USD" },
  "percentageChange": 50.0,
  "summary": {
    "startDate": "2022-01-15",
    "endDate": "2023-01-16"
  },
  "data": [
    {
      "date": "2022-01-15",
      "marketValue": {  "amount": 100000.00,  "currencyCode": "USD" }
    },
    {
      "date": "2022-01-16",
      "marketValue": { "amount": 100000.00,    "currencyCode": "USD" }
    },
    ......
    {
      "date": "2023-01-14",
      "marketValue": {  "amount": 100000.00,  "currencyCode": "USD" }
    },
    {
      "date": "2023-01-16",
      "marketValue": {   "amount": 150000.00,  "currencyCode": "USD" }
    }
  ]
}
```

Response Model

Label	Req'd?	Type	Description
{			
netWorth {			
amount		number	Net worth based on the closing position values from day before yesterday.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
netChange			
amount		number	Net change in calculated net worth for the specified period.

currencyCode	string	ISO 4217 currency code for the position, such as USD.	
percentageChange	number	Percentage change in Net Worth of the investor for the specified period.	
Summary {			
startDate	string	Beginning of the time period for which the time series data is provided. For predefined trailing periods such as 1M, the startDate is calculated for you based on the requested time period. For time periods requested using *dateFrom* and *dateTo*, the startDate will be *dateFrom* as long as *dateFrom* is in the past.	
endDate	string	End of the time period for which the time series data is provided. Note that there may not be a time series data item for every day in the period. For predefined trailing periods such as 1M, the endDate will be yesterday. For time periods requested using *dateFrom* and *dateTo*, the endDate will be one day prior to *dateTo* if *dateTo* is in the past. If *dateTo* is in the future, endDate will be yesterday.	
}			
data		Net Worth trend of an investor for the specified period.	
PesonNetWorth			
date	string	Historical date to represent previous net worth details.	
marketValue			
amount	number	Net worth based on the closing position values for the specific date.	
currencyCode	string	ISO 4217 currency code for the position, such as USD.	
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok	See Response Model above.	
400	Bad Request		
401	Not Authorized		

404	Not Found	Response body:
		{
		  "type": "networth-data-not-found",
		  "title": "Net worth data not found",
		  "detail": "Net worth data not found for the specified period",
		  "additionalInfo": {}	

HTTP Status Code	Reason	Response Model	Headers
		}	
500	Internal Server Error		

GET person summary

GET /api/v1/persons/me/summary

Implementation Notes

Use this endpoint to get the total market value of the investor's accounts.

Parameters

None.

Response Body

```
{
  "marketValue": {
    "amount": 2078.34,
    "currencyCode": "USD"
  },
  "hasFinancialData": true
}
```

Response Model

Label	Req'd?	Type	Description
{			
marketValue {			Currency value.
amount		number	Total market value of the investor's accounts.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
hasFinancialData		Boolean	True if the investor has at least one account credential, otherwise false.
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok	See [Response Model](#) above.	
401	Not Authorized		
500	Internal Server Error		

Delete person

DELETE /api/v1/persons

Implementation Notes

Delete the data for the investor authenticated for this session. This endpoint enables the authenticated user to delete all of their own data from the ByAllAccounts system.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
notifyPerson		false	Indicates if the deleted investor and associated users, such as advisors and assistants, should be notified of the delete operation.	query	Boolean

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok		
204	No contents		
400	Bad Request		
401	Not Authorized		
403	Bad Request		
404	Not Found		
500	Internal Server Error		

Position Operations

GET positions

GET /api/v1/positions

Implementation Notes

Use this endpoint to get the collection of all positions.

You can specify the number of the page to return and the number of records per page.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
page		0	Page number	query	integer
size		25	Number of records per page	query	integer
incExtraSecInfo		false	If the firm is licensed for extra Morningstar security data and this parameter is set to *true*, the response will append additional security fields as applicable.	query	Boolean

Response Body

This section shows two response body examples. The first is the default example, and the second includes the licensed Morningstar security data.

Default Example

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 1,
  "totalElements": 1,
  "isFirst": true,
  "isLast": true,
  "data": [
   {
     "ticker": "SIEGY",
     "cusip": 826197501,
     "name": "Siemens AG",
     "morningstarSecId": "E0DEU00CVS",
     "morningstarPerfId": "0P000004XO",
     "units": 12,
```

```
          "unitPrice": {
            "amount": 2078.34,
            "currencyCode": "USD"
          },
          "marketValue": {
            "amount": 2078.34,
            "currencyCode": "USD"
          },
          "lastUpdated": "2021-08-19T09:08:10.000-04:00",
          "assetLiabilityIndicator": "Asset",
          "secType": "Bond",
          "costBasis": {
            "amount": 2078.34,
            "currencyCode": "USD"
          },
          "couponRate": 24,
          "maturityDate": "2021-08-19",
          "originalFace": 12484,
          "paydownFactor": 12484,
          "fiSuppliedSecType": 5566,
          "id": 778899,
          "accountId": 778899,
          "securityId": 778899
        }
      ]
    }
```

Example with licensed Morningstar security data fields

This example has one Mutual Fund and one Stock with the licensed Morningstar security data fields.

```
    {
      "pageSize": 25,
      "pageNumber": 0,
      "totalPages": 1,
      "totalElements": 2,
      "isFirst": true,
      "isLast": true,
      "data": [
        {
          "ticker": "CBFAX",
          "name": "AMERICAN FUNDS GLOBAL BALANCED 529-A",
          "morningstarSecId": "F00000LIUD",
```

```json
"units": 2.0000,
"unitPrice": {
 "amount": 2,
 "currencyCode": "USD"
},
"marketValue": {
 "amount": 200.00,
 "currencyCode": "USD"
},
"lastUpdated": "2023-02-06T20:58:38.000-05:00",
"assetLiabilityIndicator": "Asset",
"secType": "Mutualfund",
"costBasis": {
 "amount": 400,
 "currencyCode": "USD"
},
"fiSuppliedSecType": "MUTUALFUND",
"id": 828887,
"accountId": 790641,
"securityId": 5,
"bondStyleBoxLong": 2,
"bondStyleBoxLongName": "Moderate Sensitivity High Quality",
"assetAllocationUSStock": 27.27,
"assetAllocationNonUSStock": 31.79,
"assetAllocationUSBond": 17.42,
"assetAllocationNonUSBond": 15.99,
"assetAllocationPreferred": 0.49,
"assetAllocationConvertible": 0,
"assetAllocationCash": 5.44,
"assetAllocationOther": 1.59,
"regionUnitedStates": 46.18,
"regionCanada": 5.23,
"regionLatinAmerica": 2.87,
"regionUnitedKingdom": 7.97,
"regionEurozone": 14.23,
"regionEuropeExEuro": 7.93,
"regionEuropeEmerging": 0,
"regionAfrica": 0,
"regionMiddleEast": 0,
"regionJapan": 2.19,
"regionAustralasia": 1.94,
"regionAsiaDeveloped": 4.27,
"regionAsiaEmerging": 7.19,
```

```json
    "stockSectorBasicMaterials": 7.47,
    "stockSectorConsumerCyclical": 3.87,
    "stockSectorFinancialServices": 18.09,
    "stockSectorRealEstate": 2.39,
    "stockSectorConsumerDefensive": 9.09,
    "stockSectorHealthcare": 13.25,
    "stockSectorUtilities": 8.33,
    "stockSectorCommunicationServices": 5.93,
    "stockSectorEnergy": 6.85,
    "stockSectorIndustrials": 13.72,
    "stockSectorTechnology": 11.02,
    "bondSuperSectorGovernment": 63.42,
    "bondSuperSectorMunicipal": 0.08,
    "bondSuperSectorCorporate": 14.77,
    "bondSuperSectorSecuritized": 6.5,
    "bondSuperSectorCashAndEquivalents": 15.24,
    "bondSuperSectorDerivative": 0,
    "styleBoxLargeValue": 26.09,
    "styleBoxLargeBlend": 47.05,
    "styleBoxLargeGrowth": 17.45,
    "styleBoxMidValue": 2.79,
    "styleBoxMidBlend": 5.3,
    "styleBoxMidGrowth": 1.06,
    "styleBoxSmallValue": 0,
    "styleBoxSmallBlend": 0.26,
    "styleBoxSmallGrowth": 0
  },

  {
  "ticker": "T",
  "name": "AT&T INC",
  "morningstarSecId": "E0USA00D7T",
  "morningstarPerfId": "0P00000031",
  "units": 333.9320,
  "unitPrice": {
   "amount": 35.1,
   "currencyCode": "USD"
  },
  "marketValue": {
   "amount": 11721.01,
   "currencyCode": "USD"
  },
  "lastUpdated": "2023-02-03T01:10:38.000-05:00",
```

```
      "assetLiabilityIndicator": "Asset",
      "secType": "Stock",
      "fiSuppliedSecType": "STOCK",
      "id": 775066,
      "accountId": 781076,
      "securityId": 24,
      "businessCountryId": "USA",
      "styleBoxCode": 1,
      "styleBoxName": "Large Value",
      "sectorCode": 308,
      "sectorCodeName": "Communication Services"
     }
   ]
 }
```

Response Model

Label	Req'd?	Type	Description
pageSize		integer	Number of records per page.
pageNumber		integer	Page number of this page.
totalPages		integer	Total number of pages in the result set.
totalElements		integer	Total number of elements in the result set.
isFirst		Boolean	True if and only if this is the first page of data in the result set.
isLast		Boolean	True if and only if this is the last page of data in the result set.
data		array	Position.
[{			
ticker		string	Ticker symbol of the position.
cusip		string	Committee on Uniform Security Identification Procedures (CUSIP) for this position. Will only be present if the firm is licensed for CUSIP data and CUSIP delivery is enabled for the firm.
name	yes	string	Name of the position.
morningstarSecId		string	Morningstar security identifier of the position.
morningstarPerfId		string	Morningstar performance identifier of the position.
units		number	Units of the position.
unitPrice {			Currency value.
amount		number	Numeric value for the position.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
marketValue {			Currency value.

Label	Req'd?	Type	Description
amount		number	Total market value of this Position as retrieved from the Financial Institution.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
lastUpdated		string	Last updated date of the position.
assetLiabilityIndicator	yes	string	Valid values are: Asset or Liability.
secType		string	Security type of the position. Can be BOND, CASH, MUTUALFUND, OPTION, OTHER, or STOCK.
costBasis {			Currency value.
amount		number	Financial Service-supplied cost basis for the Holding. If the cost basis is not available, this field may be populated with a calculated value, derived by multiplying the average Financial Service-supplied per-share cost by the total units of the Holding.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
couponRate		number	The interest payment rate of a debt instrument.
maturityDate		string	Maturity date of the position.
originalFace		number	The original face or par value for a security that amortizes or accretes (e.g., a mortgage).
paydownFactor		number	The paydown factor value for bond if provided by the financial institution.
fiSuppliedSecType		string	The security type as supplied by the financial institution.
id	yes	integer	Unique identifier of the position.
accountId	yes	integer	Identifier for the Account that contains this Position.
securityId		integer	Identifier for Security owned by this Position.
businessCountryId		string	ISO code of the business country of the security. For example: USA. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
styleBoxCode		integer	Number representation of Morningstar investment style of stocks and portfolios. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
styleBoxName		string	String representation of Morningstar investment style of stocks and portfolios. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
sectorCode		integer	Number representation of Morningstar sector code. (Industry groups are consolidated into 11 sectors.) Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
sectorCodeName		string	String representation of Morningstar Sector code. (Industry groups are consolidated into 11 sectors.) Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondStyleBoxLong		integer	This model is based on the two pillars of fixed-income performance: interest-rate sensitivity and credit quality. The three duration groups are short, intermediate, and long-term, and the three credit quality groups are high, medium, and low quality. These groupings display a portfolio's effective duration and credit quality to provide an overall representation of the fund's risk, given the length and quality of bonds in its portfolio. As with equity funds, nine possible combinations exist, ranging from short duration/high quality for the safest funds to long duration/low quality for the riskiest. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondStyleBoxLongName		string	This model is based on the two pillars of fixed-income performance: interest-rate sensitivity and credit quality. The three duration groups are short, intermediate, and long-term, and the three credit quality groups are high, medium, and low quality. These groupings display a portfolio's effective duration and credit quality to provide an overall representation of the fund's risk, given the length and quality of bonds in its portfolio. As with equity funds, nine possible combinations exist, ranging from short duration/high quality for the safest funds to long duration/low quality for the riskiest. For example: Limited Sensitivity Low Quality. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
assetAllocationUSStock		number	The percentage of the fund's assets in US Stocks (net). This figure is calculated separately for the short and long positions of the portfolio, and the sum of the asset allocation of each will not necessarily equal 100%. The net value is derived by subtracting the short positions from the long. The long and short positions can be rescaled as well. Rescaling ensures that the sum of the asset allocation breakdown will sum to 100%. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationNonUSStock		number	The percentage of the fund's assets in Non US stocks (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationUSBond		number	The percentage of the fund's assets in US bonds (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationNonUSBond		number	The percentage of the fund's assets in Non US Bonds (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationPreferred		number	The percentage of the fund's assets in preferred stocks (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationConvertible		number	The percentage of the fund's assets in convertibles (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationCash		number	The percentage of the fund's assets in cash (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
assetAllocationOther		number	The percentage of the fund's assets in other instruments (net). Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
regionUnitedStates		number	This data set provides a broad breakdown of an investment's geographical exposure in the United States. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionCanada		number	This data set provides a broad breakdown of an investment's geographical exposure in Canada. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionLatinAmerica		number	This data set provides a broad breakdown of an investment's geographical exposure in Latin America. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionUnitedKingdom		number	This data set provides a broad breakdown of an investment's geographical exposure in the United Kingdom. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionEurozone		number	This data set provides a broad breakdown of an investment's geographical exposure in the Eurozone region. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
regionEuropeExEuro		number	This data set provides a broad breakdown of an investment's geographical exposure in the Europe Ex Euro region. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionEuropeEmerging		number	This data set provides a broad breakdown of an investment's geographical exposure in the Europe Emerging region. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionAfrica		number	This data set provides a broad breakdown of an investment's geographical exposure in Africa. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionMiddleEast		number	This data set provides a broad breakdown of an investment's geographical exposure in the Middle East. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionJapan		number	This data set provides a broad breakdown of an investment's geographical exposure in Japan. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
regionAustralasia		number	This data set provides a broad breakdown of an investment's geographical exposure in the Australasia region. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionAsiaDeveloped		number	This data set provides a broad breakdown of an investment's geographical exposure in the Asia Developed region. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
regionAsiaEmerging		number	This data set provides a broad breakdown of an investment's geographical exposure in the Asia Emerging region. Each region's exposure is presented as a percentage of non-cash equity assets held by the fund. Regional exposure information summarizes a portfolio's exposure to geopolitical risk. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorBasicMaterials		number	The percentage of the fund's assets that are invested in Basic Materials (rescaled long positions). The Basic Materials sector includes companies that manufacture chemicals, building materials, and paper products. This sector also includes companies engaged in commodities exploration and processing. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorConsumerCyclical		number	The percentage of the fund's assets that are invested in the Consumer Cyclical sector (rescaled long positions). The Consumer Cyclical sector includes retail stores, auto and auto parts manufacturers, companies engaged in residential construction, lodging facilities, restaurants, and entertainment companies.

Label	Req'd?	Type	Description
stockSectorFinancialServices		number	The percentage of the fund's assets that are invested in the Financial Services sector (rescaled long positions). The Financial Services sector includes companies that provide financial services (banks, savings and loans, asset management companies, credit services, investment brokerage firms, and insurance companies).
stockSectorRealEstate		number	The percentage of the fund's assets that are invested in the Real Estate sector (rescaled long positions). The Real Estate sector includes mortgage companies, property management companies, and REITs. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorConsumerDefensive		number	The percentage of the fund's assets that are invested in the Consumer Defensive sector (rescaled long positions). The Consumer Defensive sector includes companies engaged in the manufacturing of food, beverages, household and personal products, packaging, or tobacco. Also includes companies that provide services such as education and training services. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorHealthcare		number	The percentage of the fund's assets that are invested in the Healthcare sector (rescaled long positions). The Healthcare sector includes biotechnology, pharmaceuticals, research services, home healthcare, hospitals, long-term care facilities, and medical equipment and supplies. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorUtilities		number	The percentage of the fund's assets that are invested in the Utilities sector (rescaled long positions). The Utilities sector includes electric, gas, and water utilities. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
stockSectorCommunicationServices		number	The percentage of the fund's assets that are invested in the Communication Services sector (rescaled long positions). The Communication Services sector includes companies that provide communication services using fixed-line networks or those that provide wireless access and services. This sector also includes companies that provide internet services such as access, navigation, and internet related software and services. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorEnergy		number	The percentage of the fund's assets that are invested in the Energy sector (rescaled long positions). The Energy sector includes companies that produce or refine oil and gas, oil field services and equipment companies, and pipeline operators. This sector also includes companies engaged in the mining of coal. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorIndustrials		number	The percentage of the fund's assets that are invested in the Industrials sector (rescaled long positions). The Industrials sector includes companies that manufacture machinery, hand-held tools, and industrial products. This sector also includes aerospace and defense firms as well as companied engaged in transportations and logistic services. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
stockSectorTechnology		number	The percentage of the fund's assets that are invested in the Technology sector (rescaled long positions). The Technology sector includes companies engaged in the design, development, and support of computer operating systems and applications. This sector also includes companies that provide computer technology consulting services. Also includes companies engaged in the manufacturing of computer equipment, data storage products, networking products, semiconductors, and components. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
bondSuperSectorGovernment		number	The government Super Sector includes all conventional debt issued by governments other than those which are included in the Municipal sector, including bonds issued by a Central Bank or Treasury, and bonds issued by local governments, cantons, regions, and provinces. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondSuperSectorMunicipal		number	The municipal Super Sector includes taxable and tax-exempt debt obligations issued under the auspices of states, cities, counties, provinces, and other nonfederal government entities. This sector includes issues of private entities which are considered to municipal issues from a regulatory perspective. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondSuperSectorCorporate		number	The corporate Super Sector includes bank loans, convertible bonds, conventional debt securities issued by corporations, and preferred stock. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondSuperSectorSecuritized		number	The securitized Super Sector includes all types of mortgage-backed securities, covered bonds, and asset-backed securities. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondSuperSectorCashAndEquivalents		number	The cash and equivalents Super Sector includes cash in the bank, certificates of deposit, currency, and money market holdings. Cash can also be any fixed-income securities that mature in fewer than 92 days. This Super Sector also includes commercial paper, and any repurchase agreements held by the fund. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
bondSuperSectorDerivative		number	The derivative Super Sector includes the common types of fixed-income derivative contracts: futures and forwards, options, and swaps. For display purposes, products may elect to identify this sector as Other. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
styleBoxLargeValue		number	Top row, left corner quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
styleBoxLargeBlend		number	Top row, middle column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
styleBoxLargeGrowth		number	Top row, right corner quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
styleBoxMidValue		number	Middle row, left column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
styleBoxMidBlend		number	Middle row, middle column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
styleBoxMidGrowth		number	Middle row, right column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
styleBoxSmallValue		number	Bottom row, left column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
styleBoxSmallBlend		number	Bottom row, middle column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.

Label	Req'd?	Type	Description
styleBoxSmallGrowth		number	Bottom row, right column quadrant of the Morningstar Style Box™. The Morningstar Style Box™ is a nine-square grid – three stock investment styles for each of three size categories: small, mid, and large. Two of the three style categories are "value" and "growth." However, the third, central column definition differs: for funds, the central column represents "blend" funds, which include value, core, and growth stocks; for stocks, it represents "core" stocks, those for which neither growth characteristics nor value characteristics are dominant. A stock is classified as large, mid, or small based on its position in the cumulative market capitalization of its style zone. Large-cap stocks are those that together account for the top 70% of the capitalization of each style zone; mid-cap stocks represent the next 20%; and small-cap stocks represent the balance. The market caps that correspond to these breakpoints are flexible and may shift from month to month as the market changes. Can only be present if the firm is licensed for extra Morningstar security data and the *incExtraSecInfo* parameter is set to true.
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok	See [Response Model](#) above.	
400	Bad Request		
401	Not Authorized		
404	Not Found		
500	Internal Server Error		

Security Question and Answer (SQA) Operations

GET all SQA entries for a credential

GET /api/v1/sqas

Implementation Notes

Use this endpoint to get the collection of all Security Question and Answer (SQA) entries for the credential specified by credentialId.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
credentialId	yes		The unique identifier of the credential.	query	integer
incorrectOnly		false	Specify a value of true to only return incorrect security questions in the response.	query	Boolean
page		0	Page number.	query	integer
size		25	Number of records per page.	query	integer

Response Body

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 1,
  "totalElements": 1,
  "isFirst": true,
  "isLast": true,
  "summary": {},
  "data": [
    {
      "id": 778899,
      "question": "In what city did you meet your spouse for the first time?",
      "answerPresent": true
    }
  ]
}
```

Response Model

The response structure is as follows.

Label	Req'd?	Type	Description
{			
pageSize		integer	A page of data records
pageNumber		integer	Number of records per page
totalPages		integer	Total number of pages in result set
totalElements		integer	Total number of elements in result set
isFirst		Boolean	True if and only if this is the first page of data in the result set
isLast		Boolean	True if and only if this is the last page of data in the result set
summary { }			
data [{			
id	yes	integer	ID of the Credential SQA
question	yes	string	The security question
answerPresent		Boolean	Whether or not the security answer is present
}]			
}			

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK	See [Response Model](#), page 119	
400	Bad Request		
401	Not Authorized		
404	Not Found		
500	Internal Server Error		

PATCH a Security Question and Answer (SQA)

PATCH /api/v1/sqas/{id}

Implementation Notes

Use this endpoint to update the answer to an existing Security Question and Answer (SQA) specified by id.

Request Headers

The PATCH body parameter listed in Parameters, page 121 is to be submitted in JSON format as shown in this example:

```
PATCH /api/v1/sqas/{id}
{
  "answer": "Boston"
}
```

The body parameter forms the Security Question and Answer (SQA) definition for PATCH requests.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
id	yes		Id of the Security Question and Answer (SQA).	path	integer
answer			The answer to the security question. minLength: 0 maxLength: 128. For example: Boston.	body	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
400	Bad Request		
401	Not Authorized		
403	Forbidden		

HTTP Status Code	Reason	Response Model	Headers
404	Not Found		
500	Internal Server Error		

Transaction Operations

GET transactions

GET /api/v1/transactions

Implementation Notes

Use this endpoint to get a collection of all transactions.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
accountIds			Limits the result set to transactions associated with the given accountIds. When not specified, parameter is ignored. Specify using a comma-separated list of accountIds.	query	string
sort			By default, results are sorted by *executionDate* in descending order, and then by *totalAmount* in ascending order. Use the *sort* parameter to change the sort order for *executionDate.* Valid values for this parameter are *executionDate.asc* and *executionDate.desc*. The following setting changes to sorting by *executionDate* in ascending order: GET /api/v1/transactions?sort=executionDate.asc	query	string
page		0	Page number	query	integer
size		25	Number of records per page	query	integer

Response Body

```
{
"pageSize": 25,
"pageNumber": 0,
"totalPages": 1,
"totalElements": 2,
"isFirst": true,
"isLast": true,
"data": [{
  "id":12345,
  "accountId":34567,
  "txType":"Dividend",
  "ticker":"CADE",
  "cusip":"12740C103",
```

```
    "name":"CADENCE BANK",
    "description":"DIVIDEND",
    "units":200,
    "executionDate":"2023-01-03",
    "totalAmount":{
      "amount":44,
      "currencyCode":"USD"
    },
    "fiSuppliedDescription":"CADENCE BANK 010323 200",
    "flowUnits":200.0000,
    "flowAmount":{
      "amount":44,
      "currencyCode":"USD"
    },
    "morningstarSecId":"E0USA003DE",
    "morningstarPerfId":"0P000000P5",
    "positionId":37890,
    "securityId":15793
},
{
      "id":8811223,
      "accountId":76234,
      "txType":"Sell",
      "ticker":"LFCR",
      "cusip":"514766104",
      "name":"LIFECORE BIOMEDICAL INC",
      "description":"ASSET SOLD",
      "units":-100,
      "price":{
        "amount":6.0214,
        "currencyCode":"USD"
      },
      "executionDate":"2023-01-05",
      "totalAmount":{
        "amount":557.12,
        "currencyCode":"USD"
      },
      "fiSuppliedDescription":"LIFECORE BIOMEDICAL INC",
      "flowUnits":-100.0000,
      "flowAmount":{
        "amount":557.12,
        "currencyCode":"USD"
      },
```

```
      "morningstarSecId":"E0USA00NLZ",
      "morningstarPerfId":"0P0000038H",
      "positionId":98765,
      "securityId":65432
    }
  ]
}
```

Response Model

Label	Req'd?	Type	Description
pageSize		integer	Number of records per page.
pageNumber		integer	Page number of this page.
totalPages		integer	Total number of pages in result set.
totalElements		integer	Total number of elements in result set.
isFirst		Boolean	True or false. True if and only if this is the first page of data in the result set.
isLast		Boolean	True or false. True if and only if this is the last page of data in the result set.
data [{			Transaction data.
id	yes	integer	Unique numeric identifier for the transaction.
accountId	yes	integer	Identifier of the Account on which the transaction represents activity.
txType	yes	string	Type of the transaction. See the table of [Transaction Values for txType and origTxType](#) on page 127.
ticker		string	The ticker identifying the security the transaction executed against.
cusip		string	Committee on Uniform Security Identification Procedures (CUSIP) identifying the security the transaction executed against. Will only be present if the firm is licensed for CUSIP data and CUSIP delivery is enabled for the firm.
name		string	Either the name of the Security or a short description of the Transaction. It will be the first valid value taken from related objects in this order: 1) security name, 2) position name, and 3) transaction name.
description		string	Either the name of the Security and/or a longer description of the Transaction.
units		number	Number of units (of security) involved in the Transaction.
price {			Currency value.
amount		number	Numeric value for the price associated with the transaction.
currencyCode		string	ISO 4217 currency code for the position, such as USD.

Label	Req'd?	Type	Description
}			
executionDate	yes	string	Date on which this Transaction was executed. Also called Trade Date.
totalAmount {			Total currency amount.
amount		number	Numeric value for the total amount associated with the transaction.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
commissions {			Commission amount.
amount		number	Numeric value for the commissions associated with the transactions.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
commissionsFees {			Commission fees.
amount		number	Numeric value for the commission fees for the transactions.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
fees			Fees.
{			
amount		number	Numeric value for the fees
currencyCode		string	ISO 4217 currency code for the position, such as USD
}			
fiSuppliedDescription		string	Description for the transaction as supplied by the financial institution.
spendingCategory		string	The consumer spending category attributed to the transaction.
spendingCategoryInfo		string	For consumer spending transactions, specifies if the transaction was an outgoing payment (expense) or incoming receipt (income).
flowUnits		number	Normalized units for the transaction. Whereas the *units* field contains the value directly from the financial institution and may have variations in sign within a given transaction type, *flowUnits* contains this same units value but is normalized by transaction type (e.g. withdrawal will always have negative *flowUnits*). For more details about sign, refer to Sign used for flowAmount and flowUnits field in transactions on page 129.
flowAmount	yes		Total amount of the cash flow for this transaction relative to the cash balance of the account. For more details about sign, refer to Sign used for flowAmount and flowUnits field in transactions on page 129.
{			

Label	Req'd?	Type	Description
amount		number	Total amount of the cash flow for this transaction relative to the cash balance of the account.
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
origTxType		string	Transactions reported as a reversal or cancellation by the financial institution will have the original transaction type code in this field. See the table of Transaction Values for txType and origTxType on page 127.
morningstarSecId		string	Morningstar security identifier of the transaction.
morningstarPerfId		string	For equities, this field contains the Morningstar performance identifier. This field is empty for anything other than equities.
positionId		integer	Unique internal identifier for the position associated with the transaction.
securityId		integer	ID for the Security for which the Transaction represents activity.
}]			
}			

Transaction Notes

Transaction Values for txType and origTxType

This table lists the possible transaction values for txType and origTxType, which are described in the Response Model table that starts on page 125.

Transaction Type Value	Description
ATM	ATM debit or credit (depends on signage of amount)
Buy	Buy a Security
Check	Check written
Closure	Close a holding for an option
Credit	Generic credit
Debit	Generic debit
Deposit	Deposit
Direct debit	Merchant initiated debit
Direct deposit	Direct deposit
Dividend	Dividend paid
Fee	Financial Institution fee
Income	Investment income is realized as cash into the investment Account
Interest	Interest earned or paid (depends on signage of amount)
Expense	Miscellaneous investment expense that is associated with a specific Security

Journal	Journal cash or Securities between Sub-Accounts within the same investment Account
Margin interest	Margin interest expense
Other	Other
Payment	Electronic payment
Point of sale	Point of sale debit or credit (depends on signage of amount)
Reinvestment	Reinvestment of income
Repeat payment	Repeating payment/standing order
Return of capital	Return of capital
Sell	Sell a Security
Service charge	Service charge
Split	Stock or Mutual Fund split
Transfer	Transfer cash or Holdings in or out (depends on signage of amount)
Withdrawal	Withdraw funds from Account

Sign used for flowAmount and flowUnits field in transactions

This table defines the sign used for the flowAmount and flowUnits fields which are described in the Response Model table that starts on page 125. The sign is based on the transaction type. Signs available are:

▪ Positive

▪ Negative

▪ Neutral – used only by flowAmount; Neutral is a flow of 0

▪ As is – the sign in the original data from the Financial Institution. Using the sign from the original data is usually done to preserve the full meaning of the transaction (e.g. transfer in vs. transfer out are not distinguished by type alone, but by type plus unit sign).

Transaction Type	flowAmount Sign	flowUnits Sign
ATM	As is	As is
Buy	Negative	Positive
Check	Negative	Negative
Closure	Neutral	As is
Credit	Positive	Positive
Debit	Negative	Negative
Deposit	Positive	Positive
Direct debit	Negative	Negative
Direct deposit	Positive	Positive
Dividend	Positive	Positive
Fee	Negative	Negative
Income	Positive	Positive
Interest	As is	As is
Expense	Negative	Negative
Journal	As is	As is
Margin interest	As is	As is
Other	Neutral	As is
Payment	Negative	Negative
Point of sale	Negative	Negative
Reinvestment	Neutral	Positive
Repeat payment	Negative	Negative
Return of capital	Positive	Positive
Sell	Positive	Negative
Service charge	Negative	Negative
Split	Neutral	As is
Transfer	As is	As is
Withdrawal	Negative	Negative

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok	See [Response Model](#) above.	
400	Bad Request		
401	Not Authorized		
404	Not Found		
500	Internal Server Error		

Appendix A. Deprecated Endpoints

This appendix describes any endpoint(s) being deprecated from the REST API that are described in this guide.

- GET /api/v1/credentials/accounts is being replaced by GET /api/v1/credentials/accounts/summary which is described in [GET credentials and accounts](#) on page 37.
This endpoint is still supported as of 3/2/2023.

GET credentials including account info when available

GET /api/v1/credentials/accounts

Implementation Notes

This endpoint retrieves credentials and any associated accounts in a single list. Credentials that have no associated accounts will also be included. This response also includes information about asynchronous activities for the credentials and accounts. Use the *limitToProgressAfter* parameter to request that information for asynchronous activities in the response should be limited to those initiated after the specified point in time.

The applicable scope of this endpoint is always a single authenticated investor. This endpoint can provide information on asynchronous activity for the current session or for all activity in the system. Use the *scope* parameter with value *session* to request information about activity initiated during the current session. Use the *scope* parameter with value *global* to request information for all activity in the system. When *scope* is *global*, asynchronous activity progress will be available for terminated sessions up to 15 minutes after completion of that activity. If the *scope* parameter is not provided then the endpoint will report on activity for the current session if there is one. If there is no current session (Morningstar Authentication) then it will report on all activity for the authenticated investor.

You can specify the number of the page to return and the number of records per page.

Parameters

Parameter	Required?	Default Value	Description	Parameter Type	Data Type
limitToProgressAfter	no		Show only credentials/accounts authenticated/aggregated by the user after the specified date. If not specified will return the full list of credentials/accounts.	query	date-time ISO 8601 JSON format yyyy-mm-ddThh:mm:ss.nnnnnn+|-hh:mm Local time relative to GMT. For example: 2019-08-22T15:16:33.045-04:00
page	no	0	Page number.	query	integer
size	no	25	Number of records per page.	query	integer
scope	no		Scope of activity for the authenticated user. Values can be *session*, to include only session-specific information, or *global* to also include information from other sessions for this user.	query	String. Either *session* or *global*.

Response Body

This example shows part of a response. Also see

```
{
  "pageSize": 25,
  "pageNumber": 0,
  "totalPages": 1,
  "totalElements": 1,
  "isFirst": true,
  "isLast": true,
  "activitySummary": {
   "activityInProgress": false
  },
  "summary": {},
  "data": [
   {
    "account": {
     "accountNumber": "ABCD12345678",
     "accountNumber2": "XYZ12345",
     "accountType": "CREDITCARD",
     "aggregationStatusErrorCode": 1005,
     "id": 11223344,
     "lastUpdated": "2022-05-21 2:52:23 AM",
     "marketValue": {
      "amount": 2078.34,
      "currencyCode": "USD"
     },
     "name": "BofA Checking Account"
    },
    "activityInProgressStatus": "In Progress",
    "alarm": false,
    "authenticationStatusErrorCode": 1006,
    "credentialComplete": true,
    "financialInstitution": {
     "accountNumber2Term": "Other Account Number",
     "accountNumberTerm": "Plan Number",
     "icon":
"https://www.byallaccounts.net/WebPortfolio/vendorResources/Default/assets/fi/icons/icon.svg",
     "id": 254367,
     "login2Term": "Other Login",
     "loginTerm": "Login",
     "name": "Bank of America - Banking",
```

```
      "pw2Term": "Other Password",
      "pwTerm": "Password",
      "supportsAccountDiscovery": true,
      "supportsOauth": true,
      "supportsTestCredential": true,
      "userLoginURL": "https://chaseonline.chase.com/Logon.aspx?LOB=COLLogin",
      "websiteURL": "https://chaseonline.chase.com/Logon.aspx?LOB=COLLogin"
    },
    "id": 778899,
    "unifiedStatusInfoMsg": "Authenticate to connect.",
    "unifiedStatusInfoType": "cannotConnectMissingLoginPW"
  }
 ]
}
```

Response Model

Special Situations for Credentials and Accounts

Credentials and accounts in the aggregation system are complex objects for which the following statements are true:

- Credentials or accounts can be incomplete, meaning they do not contain enough information to access data from the Financial Institution. This situation can occur if the user has not yet provided all necessary information (e.g. has not yet provided their password or completed OAUTH authorization).

- The aggregation system may encounter a variety of errors when attempting to use a credential or an account to access data from a Financial Institution. These errors can occur because the information in the object is incorrect (e.g. a wrong password), problems with the aggregation system's support (e.g. Financial Institution web site has changed and we need to update our support), or problems at the Financial Institution (e.g. site not available).

These conditions are not errors from an application perspective, instead they are "normal" things that can happen in the day-to-day of aggregation activities. It is important to properly represent these conditions to the end user and, whenever possible, help the user to understand when they must take action to resolve the condition or when the solution is not under their control. Due to the complexity of these error conditions, it is not always possible to make the condition clear to the user. ByAllAccounts continues to work to improve the clarity of these error conditions.

In addition to these situations, the system may be asynchronously performing activities that the user requested, directly or indirectly, on credentials and accounts. For example, if a request was made to obtain the latest data for an account then an asynchronous aggregation process is going on in the background and we want the end user to understand that it is in process and when that process completes. This endpoint includes information at the individual object level (credential or account) as well as the summary level (for the collection) to aid in the presentation of this information to the user. Note also that any asynchronous

activity can result in the clearing of an error condition or the encountering of a new condition, so that information should be queried and redisplayed upon completion of the asynchronous activity.

Account and Credential Error Information

Credentials and Accounts can be incomplete (missing required information like a login, or an account number), or they can be complete and have errors as reported by the custodian when the credentials are used to attempt to access a customer's data at the custodian. These errors could include wrong login/password, account number could not be found, etc.

The unifiedStatusInfoType field indicates an error condition that should be relayed to the user. If unifiedStatusInfoType is absent, then no error condition exists at the present time. When unifiedStatusInfoType is present there will always be a unifiedStatusInfoMsg that will contain a suggested text form of the message for presentation to the user.

For more information about unifiedStatusInfoType, refer to Table of Authentication/Aggregation Status Messages on page A-8. Note that some errors listed may not occur frequently, but they are included for completeness.

There are other fields in the response that contain a variety of information about status, but these fields should not be used. They are present for historical reasons and are superseded by unifiedStatusInfoType. These fields will likely be removed in a future version of the REST API. The following fields should NOT be used to determine whether a credential or account is incomplete or has another type of error:

- aggregationStatusErrorCode
- authenticationStatusErrorCode
- alarm
- credentialComplete

Activity in progress information

As described above, this endpoint can return information about server "activity in progress" for objects in the response collection. Activity in progress includes:

- testing that a credential authenticates at a custodian
- discovering accounts available for a credential at a custodian
- aggregating data for accounts from the custodian

These operations are initiated and running in the ByAllAccounts server while the UI or API caller is awaiting the results of those operations. This activity information can be provided for two different scopes: SESSION or GLOBAL. The default is SESSION if you have a session, and GLOBAL if you do not (some forms of authentication do not use a session). If you have a session you can request GLOBAL using the scope query parameter. For session scope, the progress information is reported for the above operations that were initiated during the current session. For global scope, the information will be reported for all activity initiated through the REST API for the target objects (regardless of who initiated that activity).

The activityInProgress field at the top of the response will have a value of "true" if there is activity in progress for any object in the collection, otherwise "false".

For each object, the activityInProgressStatus field:

- is absent if no activity occurred for the scope of the request (as determined by the query parameters: *scope* and *limitToProgressAfter*).

- if present and value is:
  - "In Progress" then authentication or aggregation activity is currently occurring for this object within the ByAllAccounts Server for the scope of the request (as determined by the query parameters: *scope and limitToProgressAfter*).
  - "Complete" then authentication or aggregation activity has completed for this object within the ByAllAccounts Server for the scope of the request (as determined by the query parameters: *scope and limitToProgressAfter*).

While asynchronous activity is occurring for objects in the response, the error status on objects can change multiple times and additional objects can be added to the response. For example, if a new credential was added and account discovery was initiated (e.g. by the BAA ConsumerUI), then as accounts are discovered they will appear in the response, and subsequently data for those accounts will be aggregated and their market value will appear.

Table of Response Model Contents

Label	Req'd?	Type	Description
{			
pageSize		integer	Number of records per page.
pageNumber		integer	Page number of this page.
totalPages		integer	Total number of pages in result set.
totalElements		integer	Total number of elements in result set.
isFirst		Boolean	True or false. True if and only if this is the first page of data in the result set.
isLast		Boolean	True or false. True if and only if this is the last page of data in the result set.
activitySummary {			
activityInProgress		Boolean	If scope=*session* (or not set), then true indicates aggregation or authentication is in-progress for at least one credential in the session. If scope=*global*, then true indicates aggregation or authentication is in-progress for at least one credential in the session or authentication or discover/add/aggregate is in progress for at least one credential outside the current session.
}			
summary {}			
data [{		array	Credential-account pair. Either an account and its related credential or a credential that has no accounts associated with it .
account{			
accountNumber		string	The account number at this financial institution.
accountNumber2		string	The optional account number at this financial institution.
accountType		string	Type of account. See

Label	Req'd?	Type	Description
			Table of Account Types page A-9.
aggregationStatusErrorCode		integer	Error code from the latest aggregation attempt. This field can be ignored. Instead refer to unifiedStatusInfoType and see Account and Credential Error Information page A-5 regarding best practices on understanding the state of the accounts and credentials.
id	yes	integer	An account identifier assigned by the service.
lastUpdated		string	Date and time stamp of last update. For example: 2018-05-21 2:52:23 AM.
marketValue {			Total market value of the account.
amount		number	A read-only value .
currencyCode		string	ISO 4217 currency code for the position, such as USD.
}			
name		string	Name of the account.
}			
activityInProgressStatus		string	Status of authentication or aggregation. "In Progress" or "Complete".
alarm	yes	Boolean	True or false. If true, credential requires attention from user. This field can be ignored. Instead refer to unifiedStatusInfoType and see Account and Credential Error Information page A-5 regarding best practices on understanding the state of the accounts and credentials.
authenticationStatusErrorCode		integer	Error code from the latest authentication attempt. This field can be ignored. Instead refer to unifiedStatusInfoType and see Account and Credential Error Information page A-5 regarding best practices on understanding the state of the accounts and credentials.
credentialComplete	yes	Boolean	True or false. Indicates whether the credential contains enough information to perform authentication. This field can be ignored. Instead refer to unifiedStatusInfoType and see Account and Credential Error Information page A-5 regarding best practices on understanding the state of the accounts and credentials.
financialInstitution {			
accountNumber2Term		string	Term used for the optional account number at this FI.
accountNumberTerm		string	Term used for the account number at this financial institution.
icon		string	The path to the icon for the financial institution. If the financial institution is requested (not supported) it is the path to a default icon.
id	yes	integer	The ID of the financial institution.
login2Term		string	Term used for the account number at this FI.

Label	Req'd?	Type	Description
loginTerm		string	Term used for the login at this financial institution.
name		string	Name of the financial institution.
pw2Term		string	Term used for the optional second password at this FI.
pwTerm		string	Term used for the password at this financial institution.
supportsAccountDiscovery	yes	Boolean	True or false. Indicates whether the FI supports account discovery.
supportsOauth	yes	Boolean	True or false. Indicates whether the FI supports OAuth authorization.
supportsTestCredential	yes	Boolean	True or false. Indicates whether the FI supports test credential (testing authentication).
userLoginURL	yes	string	User login URL of the financial institution.
websiteURL		string	Website URL of the financial institution.
}			
id	yes	integer	ID of the account credential.
unifiedStatusInfoType		string	Type of status information from the combination of the latest authentication and aggregation attempt. See Table of Authentication/Aggregation Status Messages page A-8.
unifiedStatusInfoMsg		string	Status information from the combination of the latest authentication and aggregation attempt. See Table of Authentication/Aggregation Status Messages page A-8.
}]			

Table of Authentication/Aggregation Status Messages

These status types and messages are provided in the response of GET /api/v1/credentials/accounts.

unifiedStatusInfoType	unifiedStatusInfoMsg
accountClosed	This account is closed.
aggCannotLoadDataCheckLater	We are having trouble accessing this institution. Please check back later.
badAccountCheckLater	We are having trouble accessing this institution. Check back later.
badAccountVerifyAccountNum	We are having trouble accessing this institution. Check back later.
cannotConnectBadLoginPw	We cannot connect to this institution. The {{loginTerm}} or {{passwordTerm}} is incorrect. Re-authenticate.
cannotConnectBadLoginPwIsac	We cannot connect to this institution. The {{loginTerm}}, {{passwordTerm}}, or activation code is incorrect. Re-authenticate.
cannotConnectBadLoginPwSqa	We cannot connect to this institution. The {{loginTerm}}, {{passwordTerm}}, or answer to a security question is incorrect. Re-authenticate.
cannotConnectBadLoginPwSqaIsac	We cannot connect to this institution. The {{loginTerm}}, {{passwordTerm}}, answer to a security question, or security code is incorrect. Re-authenticate.
cannotConnectMissingAcctNum	We are having trouble accessing this institution. Check back later.

unifiedStatusInfoType	unifiedStatusInfoMsg
cannotConnectMissingLoginPW	Authenticate to connect.
cannotConnectNotAuthorized	We cannot connect to this institution. Authorize access to connect.
cannotConnectOauthAcctNotAuthorized	Cannot connect. Account is not authorized.
cannotConnectOauthNotConfigured	Further configuration is required to connect to this institution. Contact your aggregation provider for assistance.
cannotConnectUserActionOnetimeCode	To allow the aggregation service to access your accounts, please login on your institution website and turn off the setting that requires identity verification at every login.
cannotConnectUserActionPersonalInfo	This institution requires you to update or verify personal information or preferences on their website and then re-authenticate.
cannotConnectUserActionSecurity	This institution requires you to set up additional security features on their website and then re-authenticate.
cannotConnectUserActionUserAgreement	This institution requires you to accept a user agreement on their website and then re-authenticate.
cannotLoadDataCheckLater	We are having trouble accessing this institution. Check back later.
cannotVerifyFiLimitation	We cannot verify your credentials due to institution limitation. Check back later.
credHasNoAccounts	No accounts have been connected. Connect accounts.
filoginCannotConnectBadLoginPw	Cannot connect. The {{loginTerm}} or {{passwordTerm}} is incorrect.
fiNotYetSupported	This institution is not yet supported.
fiRequestMissingElements	Additional inputs are required before this institution request can be processed.
isacCannotConnectBadIsac	Cannot connect. The information you provided is incorrect.
noAccountsFound	No accounts found at this institution.
noConnectAttemptYet	Authenticate to connect.
noNewAccountsFound	All accounts are already set up.
oauthCannotConnectBadAuthorization	Cannot connect. Authorization failed.
sqaCannotConnectBadSqa	Cannot connect. The answer to a security question is incorrect.

Table of Account Types

Type	Type	Type
UNKNOWN	INSURANCE_LIFEINSURANCE	INVESTMENT_SARSEP
OTHER	INSURANCE_OTHER	INVESTMENT_SAVINGSBOND
INVESTMENT_CASHMANAGEMENT	INVESTMENT_401A	INVESTMENT_SEPIRA
BANKING_CD	INVESTMENT_401K	INVESTMENT_TREASURYBOND
BANKING_CHECKING	INVESTMENT_403B	INVESTMENT_TRUST
INVESTMENT_COVERDELL	INVESTMENT_457B	INVESTMENT_UGMA
BANKING_CREDITLINE	INVESTMENT_529	INVESTMENT_UTMA
BANKING_DEPOSIT	INVESTMENT_BROKERAGE	LOAN_AUTO

Type	Type	Type
BANKING_MONEYMARKET	INVESTMENT_IRA	LOAN_BANK
BANKING_OTHER	INVESTMENT_KEOGH	LOAN_BOAT
BANKING_SAVINGS	INVESTMENT_MUTUALFUND	LOAN_HOMEEQUITY
CREDITCARD	INVESTMENT_OTHER	LOAN_MORTGAGE
HEALTHACCOUNT_FSA	INVESTMENT_PENSION	LOAN_OTHER
HEALTHACCOUNT_HRA	INVESTMENT_PREPAIDTUITION	LOAN_PERSONAL
HEALTHACCOUNT_HSA	INVESTMENT_PROFITSHARE	LOAN_STUDENT
HEALTHACCOUNT_OTHER	INVESTMENT_RETIREMENT	
INSURANCE_ANNUITY	INVESTMENT_ROTHIRA	

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	Ok		
400	Bad Request		
401	Not Authorized		
500	Internal Server Error		

Appendix B. Cumulative Changes

This appendix is a running list of changes to this guide, beginning with changes made on October 13, 2023.

Date	Summary of Changes
October 18, 2023	New document.
October 23, 2023	Document update to add a section that describes available test financial institutions.
November 9, 2023	The response for the GET Financial Institution operation (GET /api/v1/fis) now has a *licensed* field to indicate whether the financial institution is licensed for the user's firm.
December 21, 2023	Added GET /api/v1/persons/me/networth endpoint.
January 18, 2024	Added *dateFrom* and *dateTo* parameters to the GET /api/v1/persons/me/networth endpoint.
February 29, 2024	▪ Added DELETE /api/v1/persons endpoint. ▪ Updated GET /api/v1/persons/me/networth endpoint New summary block was added to the response of the endpoint. It includes a startDate and endDate that define the time period for which data was requested. Also, the description for the period parameter has been updated for clarity. ▪ Updated POST /api/v1/credentials/{credentialId}/authenticate endpoint to add body parameters oauthRedirectURL and oauthRedirectType.
April 11, 2024	▪ Changes in this release were for maintenance purposes.
May 23, 2024	▪ Description for costBasis amount has been updated.