BETTER MESSAGING
campaign registry

Authentication+ 2.0

Feature Overview

Last Updated 11/13/25

Summary

With the introduction of Authentication+ (also referred to as Auth+), TCR added an additional Two-Factor Authentication (2FA) mechanism to verify PUBLIC_PROFIT brands. With Auth+ 2.0, TCR further refines this process so that Auth+ verifications are unbundled from the basic identity check. PUBLIC_PROFIT brands can now request Auth+ verifications separately from the identity status and can appeal the results. Also, additional webhook events allow CSPs to monitor the status of Auth+ verifications, providing more visibility into the workflow.

Auth+ 2.0 is now available as of release 6.15. For information on testing, see the CSP Non-Production Integration Testing guide.

To learn more about the original Auth+ implementation, please see the Auth+ specification document.

Document Changes:

- Added information about a new BRAND_EMAIL_2FA_EXPIRED event introduced in the 6.22 release.

Note: *Changes from the previous version of this document are highlighted in yellow*.

Table of Contents

Document History

Date	Comment	Author
2/20/2025	Initial publication.	Victor Cardoso
3/20/2025	Added August 7, 2025 as the release date for Authentication+ 2.0.	Victor Cardoso
4/3/2025	Added information on endpoints and new events that will be used in the Auth+ 2.0 implementation.	Victor Cardoso
5/1/2025	Added more information to the business rules and noted a change to the `vettingClass` property.	Victor Cardoso
5/29/2025	Updated error descriptions, appeal descriptions, and added an impact to an existing endpoint.	Victor Cardoso
6/12/2025	Updated categories associated with webhook events and modified samples to include the fields `evpName`, `evpId`, and `vettingId`.	Victor Cardoso
7/10/2025	Added screenshots showing changes to the CSP portal and clarified language used in the document.	Victor Cardoso
7/29/2025	Fixed a broken link to the Auth+ 2.0 Testing document.	Victor Cardoso
8/7/2025	Updated the document to reflect Auth+ 2.0 is now available in the 6.15 release.	Victor Cardoso
11/13/2025	Added information about a new BRAND_EMAIL_2FA_EXPIRED event introduced in the 6.22 release.	Victor Cardoso

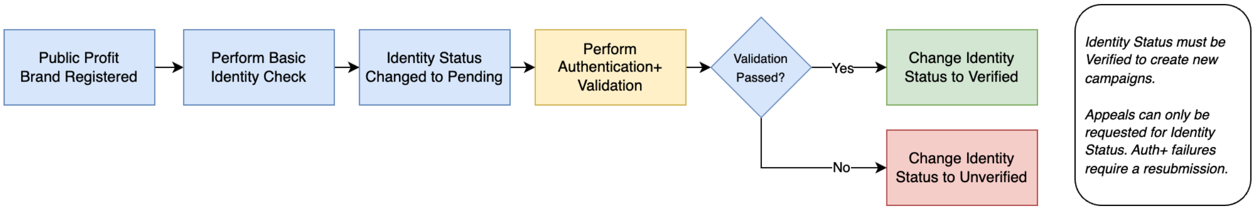
Introduction

The primary objective of Auth+ for PUBLIC_PROFIT brands is to prevent brand impersonation, which can lead to consumer fraud such as disinformation, smishing, and spoofing. This is accomplished through brand personnel attestation via a 2FA email message to a brand's business contact, as specified in the brand's profile.

Process Flows

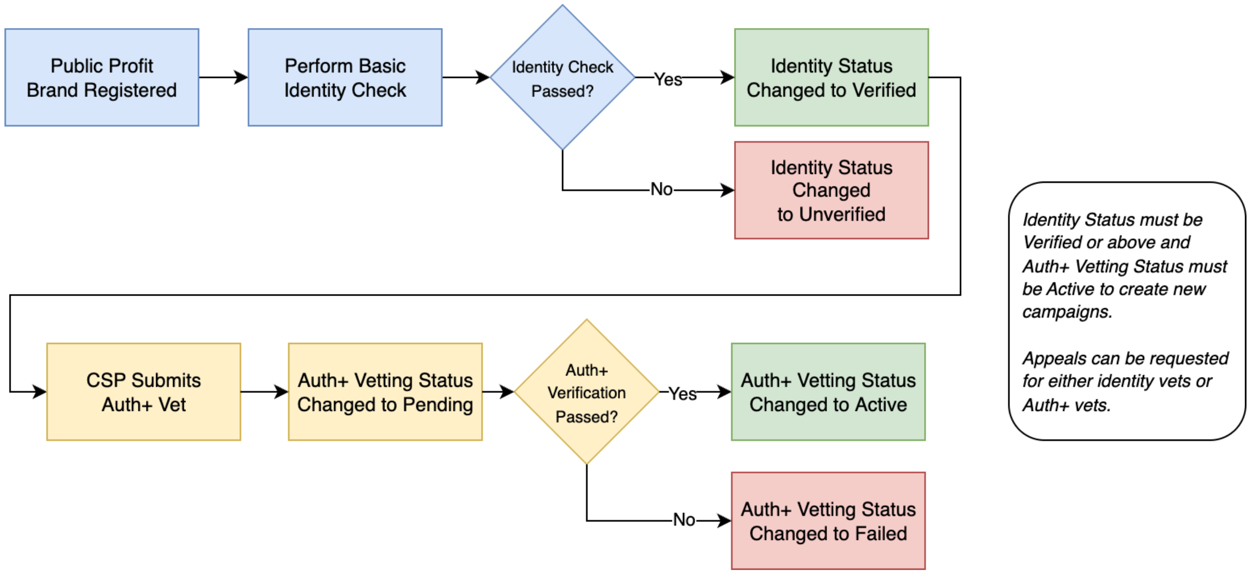
Original Auth+ Process Flow

The original Auth+ process flow combined the basic identity check with an Auth+ verification mechanism for PUBLIC_PROFIT brands.


Public Profit Brand Registered
Perform Basic Identity Check
Identity Status Changed to Pending
Perform Authentication+ Validation
Validation Passed?
Yes
No
Change Identity Status to Verified
Change Identity Status to Unverified
Identity Status must be Verified to create new campaigns.
Appeals can only be requested for Identity Status. Auth+ failures require a resubmission.

While effective, brands could not apply for Standard or Enhanced vets while awaiting the results of an Auth+ vet. Also, if a brand failed Auth+ verification, it had to be resubmitted for an identity check, leading to increased wait times and costs.

New Auth+ 2.0 Process Flow


Public Profit Brand Registered
Perform Basic Identity Check
Identity Check Passed?
Yes
No
Identity Status Changed to Verified
Identity Status Changed to Unverified
CSP Submits Auth+ Vet
Auth+ Vetting Status Changed to Pending
Auth+ Verification Passed?
Yes
No
Auth+ Vetting Status Changed to Active
Auth+ Vetting Status Changed to Failed

Identity Status must be Verified or above and Auth+ Vetting Status must be Active to create new campaigns.

Appeals can be requested for either identity vets or Auth+ vets.

With Auth+ 2.0, the basic identity check is unbundled from Auth+ verification. The basic identity check will happen automatically when a PUBLIC_PROFIT brand is registered, but now CSPs must manually request an Auth+ vet after a brand receives a VERIFIED identity status or above (i.e., VETTED_VERIFIED).

This means that appeals can be submitted independently if either the identity check or the Auth+ verification fails. Plus, CSPs can once again apply for Standard and Enhanced vets while Auth+ verification is still in progress.

❗ **Important:** *CSPs will not be able to create new campaigns for a PUBLIC_PROFIT brand until the identity status is VERIFIED or VETTED_VERIFIED and the Auth+ vetting status is ACTIVE.*

Auth+ 2.0 Vetting Statuses

With Auth+ verification separate from the basic identity check, a new Auth+ vetting status has been introduced. In the CSP portal, this is displayed in the Vetting Details section of the Brand Details page. This status can also be retrieved via the CSP API (see Fetch Auth+ Results for a Brand).

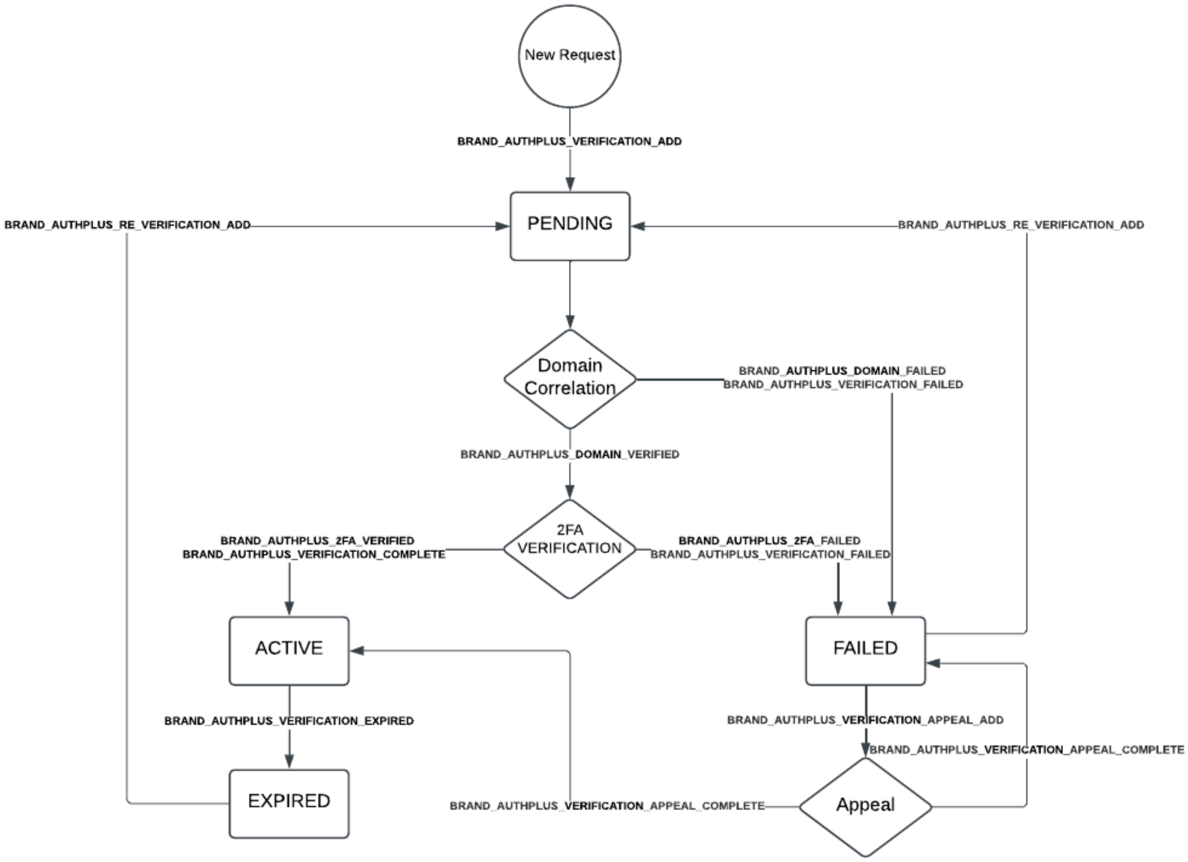
- **PENDING:** Auth+ verification is still in progress. This could mean the brand's domain is being checked or that the 2FA process has not been completed. If a second Auth+ verification is requested, the original verification will expire once the second verification is completed. Campaigns will not be affected by this transition.
- **ACTIVE:** Auth+ verification is complete. The brand's domain has been verified and the 2FA process is complete. As long as the brand's identity status is also VERIFIED, the CSP can register new campaigns for the brand.
- **FAILED:** Auth+ verification was unsuccessful and feedback from the external vetting provider was returned. This could mean that the brand's domain could not be verified or the 2FA process was not completed within 30 days. CSPs can submit an Auth+ appeal with evidence to challenge certain Auth+ results. Appeals for FAILED Auth+ statuses can be submitted within 45 days of the completed Auth+ verification.
- **EXPIRED:** Auth+ verification has reached the expiration date provided by the external vetting provider (or the verification was revoked). While currently active campaigns will not be affected, new campaigns cannot be created until the brand completes a new Auth+ verification. CSPs can request a new Auth+ verification at any time prior to expiration.

❗ **Important**

- *In the CSP portal brand listing pages, the Auth+ Compliant column will show a label of No if the brand is not a PUBLIC_PROFIT entity and is not eligible for Auth+ verification. In the CSP API, attempting to submit a non-PUBLIC_PROFIT entity for Auth+ verification will result in an error. See the Submit a Brand for Auth+ Verification endpoint for more information.*
- *In the CSP API, the `GET /brand/{brandId}/externalVetting` endpoint will return Auth+ verification records, indicating whether a brand has initiated an Auth+ vet. See the Fetch Auth+ Results for a Brand endpoint for more information.*

Auth+ 2.0 Status Transitions and Events

The following diagram shows the new progression of Auth+ vetting statuses (and the events they trigger) when an Auth+ 2.0 vet is submitted. For more information on events, see Appendix B: New and Impacted Webhook Events.


New Request
BRAND_AUTHPLUS_VERIFICATION_ADD
BRAND_AUTHPLUS_RE_VERIFICATION_ADD
PENDING
BRAND_AUTHPLUS_RE_VERIFICATION_ADD
Domain Correlation
BRAND_AUTHPLUS_DOMAIN_FAILED
BRAND_AUTHPLUS_VERIFICATION_FAILED
BRAND_AUTHPLUS_DOMAIN_VERIFIED
BRAND_AUTHPLUS_2FA_VERIFIED
BRAND_AUTHPLUS_VERIFICATION_COMPLETE
2FA VERIFICATION
BRAND_AUTHPLUS_2FA_FAILED
BRAND_AUTHPLUS_VERIFICATION_FAILED
ACTIVE
FAILED
BRAND_AUTHPLUS_VERIFICATION_EXPIRED
BRAND_AUTHPLUS_VERIFICATION_APPEAL_ADD
BRAND_AUTHPLUS_VERIFICATION_APPEAL_COMPLETE
EXPIRED
BRAND_AUTHPLUS_VERIFICATION_APPEAL_COMPLETE
Appeal

Auth+ 2.0 Appeals

CSPs can appeal a FAILED Auth+ vetting status under specific conditions. For example, brands that do not complete their Auth+ 2FA process within 30 days will not be allowed to appeal. They will have to request a new Auth+ vet.

If a brand's submitted business contact email is legitimate but results in a FAILED Auth+ vetting status, the CSP will be able to submit an appeal with evidence.

CSPs can submit an Auth+ vet appeal within 45 days of receiving a FAILED vetting status.

Auth+ 2.0 Business Rules

The following business rules apply to Auth+ 2.0 verification:

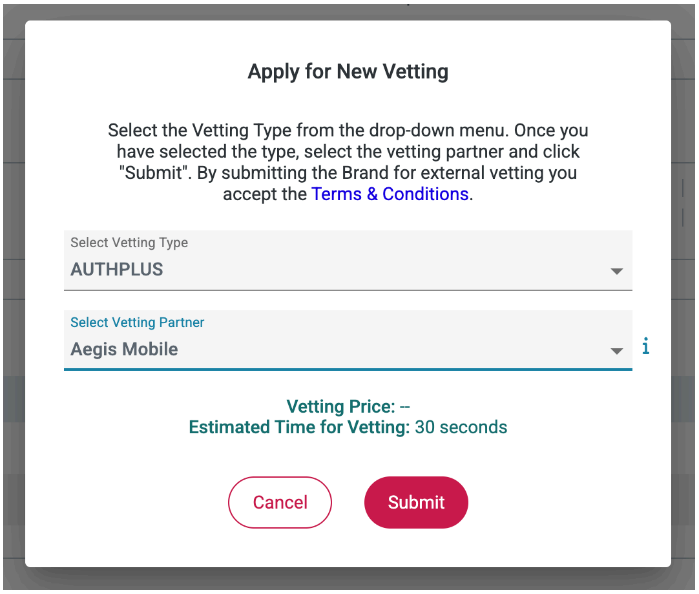
- Auth+ verification remains exclusive to PUBLIC_PROFIT brands.
- Following Auth+ verification:
    - Changing a brand's identity information will not be allowed. In order to change brand identity information, the CSP will need to create a new brand.
    - Changing a brand's business contact email address will be allowed and will only invalidate the Auth+ verification. The brand will need to request an Auth+ vet again in order to create new campaigns.
- CSPs are still required to submit a business contact email address for someone who works at the brand and can complete the Auth+ 2FA process.
    - Email addresses are still subject to validation. Personal and free email addresses will be rejected, as well as common email distribution addresses like sales@company.com or support@company.com.
- Brand business contacts will still receive a 2FA email with a PIN as part of Auth+ verification. Clicking on a link in the email will take them to a web page to enter some basic information and the PIN.
    - Auth+ PINs are only valid for 7 days. CSPs can retrigger a 2FA email with a new PIN to the business contact within 30 days of the original Auth+ verification request.
    - If the Auth+ 2FA process is not completed within 30 days of the original request, the brand's Auth+ vetting status will change to FAILED. The CSP will then need to request a new Auth+ vet.

Portal Changes

CSP Portal

Requesting an Auth+ Vet

Auth+ 2.0 verification is requested by submitting a new type of external vet. CSPs apply for external vetting on the Brand Details page and clicking on **Apply for Vetting**. You can then select **AUTHPLUS** from the vetting type menu and **Aegis Mobile** for the vetting partner. The brand must be a PUBLIC_PROFIT brand and have a VERIFIED or VETTED_VERIFIED identity status to request an Auth+ vet.



Apply for New Vetting

Select the Vetting Type from the drop-down menu. Once you have selected the type, select the vetting partner and click "Submit". By submitting the Brand for external vetting you accept the Terms & Conditions.

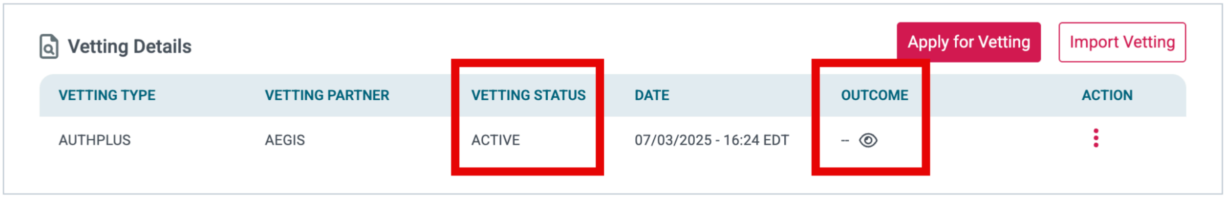
Select Vetting Type: AUTHPLUS

Select Vetting Partner: Aegis Mobile

Vetting Price: --
Estimated Time for Vetting: 30 seconds

Checking the Auth+ Vetting Status

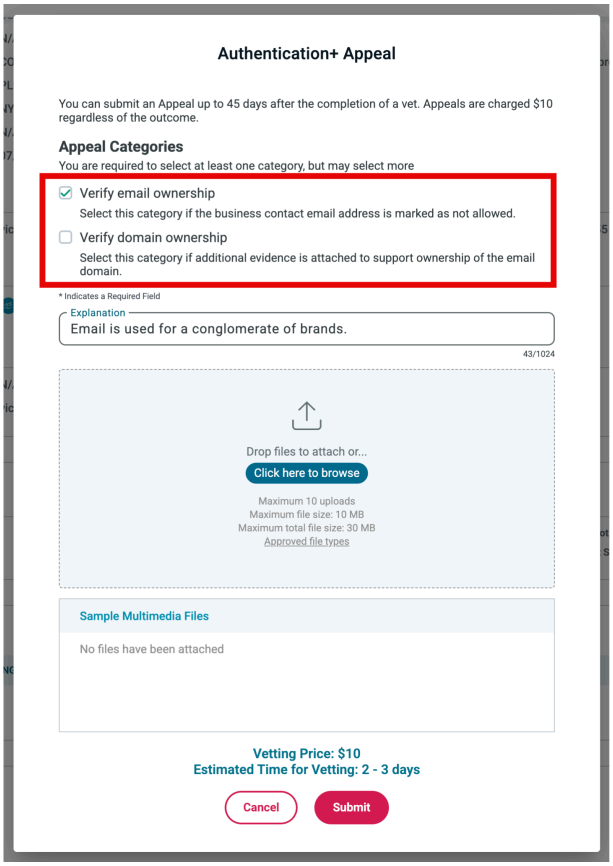
On the Brand Details page, the Vetting Details section now shows a new AUTHPLUS vetting type if an Auth+ vet has been submitted. The Vetting Status column will show the current status of the vet. Should it fail, feedback will be available in the Outcome column.



VETTING TYPE	VETTING PARTNER	VETTING STATUS	DATE	OUTCOME	ACTION
AUTHPLUS	AEGIS	ACTIVE	07/03/2025 - 16:24 EDT	--	⋮

Appealing a Failed Auth+ Vet

If Auth+ verification fails, the Action dropdown menu on the Auth+ vet will show an **Appeal** option. A window will appear that lets CSPs select one or more of the applicable categories to submit an Auth+ appeal. Evidence can also be uploaded to support the appeal.



Authentication+ Appeal

You can submit an Appeal up to 45 days after the completion of a vet. Appeals are charged $10 regardless of the outcome.

Appeal Categories

You are required to select at least one category, but may select more

☑ Verify email ownership

Select this category if the business contact email address is marked as not allowed.

☐ Verify domain ownership

Select this category if additional evidence is attached to support ownership of the email domain.

* Indicates a Required Field

Explanation: Email is used for a conglomerate of brands.

43/1024

Sample Multimedia Files

No files have been attached

Vetting Price: $10

Estimated Time for Vetting: 2 - 3 days

FAQ

Q. If I change a brand's business contact email address, will the identity status change?

No. Only the Auth+ vetting status will change. However, the CSP will need to submit a new Auth+ vet for the brand in order to create new campaigns.

Q. If my Auth+ status changes from ACTIVE to something else, what will happen to my existing campaigns?

Existing campaigns will continue to run. CSPs will only be prevented from registering new campaigns until a new Auth+ vet is completed.

Q. When Auth+ 2.0 is released, what happens to my existing brands that are already Auth+ compliant? What will happen to their campaigns?

Upon release, brands that are already Auth+ compliant will continue to be marked as Auth+ compliant, even though they won't see a specific Auth+ vet in their Brand Details. Existing campaigns will continue to run uninterrupted, and they will be able to create new campaigns.

Q. What if my PUBLIC_PROFIT brand hasn't completed Auth+ compliance yet? What will happen when Auth+ 2.0 is released?

Those legacy brands that have a VETTED or VETTED_VERIFIED identity status will need to update their business contact email address and then request an Auth+ vet. Existing campaigns will be unaffected, but CSPs will not be able to register new campaigns until Auth+ verification is complete.

Q. Are the brand attributes `businessContactTitle`, `businessContactFirstName`, `businessContactLastName`, `businessContactEmail`, and `businessContactEmailVerifiedDate` still be present in Auth+ 2.0?

Yes. Those brand attributes are still present in the Auth+ 2.0 implementation.

Appendix A: New and Impacted Endpoints

New CSP API Endpoints

- There are no new endpoints introduced for Auth+ 2.0.

Impacted CSP API Endpoints

The following endpoints have been modified to support Auth+ 2.0:

Submit a Brand for Auth+ Verification

`POST /brand/{brandId}/externalVetting`

Changes

Submitting a brand for Auth+ 2.0 verification is similar to requesting an external vet. CSPs should use a new combination of `evpId` and `vettingClass` to make a request (see the Sample Request Body below). Also, only brands that meet the following conditions can submit a request for Auth+ verification:

- The brand must be a PUBLIC_PROFIT entity.
- The brand must have the `businessContactEmail` field filled out in its profile.
- The brand must be in a VERIFIED or VETTED_VERIFIED identity status.

Brands are only allowed one Auth+ record in an ACTIVE vetting status.

- Brands with a PENDING Auth+ vet are not allowed to submit another.
- Brands with an Auth+ vetting status of ACTIVE/FAILED/EXPIRED are allowed to make an additional request. CSPs can submit an additional Auth+ vet request prior to an old vet's expiration date. If successful, the newer Auth+ vetting status will show PENDING. When the newer request becomes ACTIVE, the older verification changes to EXPIRED, allowing campaigns to continue uninterrupted.

Path Parameters

- **brandId** `string` The unique alphanumeric identifier for the brand.

Sample Request Body

```
{
  "evpId": "AEGIS",
  "vettingClass": "AUTHPLUS"
}
```

Error Codes

Code	Description
501	Operation declined. Update the brand to include a valid business email address.
525	Operation declined. Brand has already been submitted for Auth+ verification.
525	Operation declined. Submission only allowed for brands in a VERIFIED or VETTED_VERIFIED identity status.
592	Operation declined. Auth+ only supported for PUBLIC_PROFIT entities.

Fetch Auth+ Results for a Brand

`GET /brand/{brandId}/externalVetting`

Changes

- This endpoint fetches Auth+ records by **`brandId`** and **`vettingClass=AUTHPLUS`**.

Resend 2FA Email for a Brand

`POST /brand/{brandId}/2faEmail`

Changes

This endpoint resends a 2FA email to a brand's business contact. The request will only be successful if the following conditions are met:

- The latest Auth+ vet is in a PENDING status.
- The latest Auth+ vet is less than 30 days old.

If the above conditions aren't met, TCR will respond with an error.

Error Codes

Code	Description
592	Operation declined. Auth+ verification status is already ACTIVE.

Updating a Brand

`PUT /brand/{brandId}`

Changes

- PUBLIC_PROFIT brand updates will not be allowed if there's a PENDING Auth+ vet request.
- Updating the `businessContactEmail` will not impact a brand's identity status. In other words, if a VERIFIED brand updates its business contact email, the brand will remain in a VERIFIED identity status. If the brand has an ACTIVE Auth+ vet, it will be marked EXPIRED and the brand will need to undergo another Auth+ verification to create new campaigns.

Appeal Auth+ Verification Result

`POST /brand/{brandId}/externalVetting/appeal`

Changes

This endpoint allows Auth+ vets with a FAILED vetting status to appeal. The request must contain one or more pre-defined appeal categories, any optional attachments, and an optional explanation.

The following conditions must be met to appeal:

- Brand can't be a mock brand.
- Auth+ vetting status must be FAILED.
- Only allowed up to 45 days from an Auth+ vet result.

List Available Auth+ Verification Appeal Categories

`GET /enum/extVettingAppealCategory`

Changes

- This endpoint adds two new categories for use with Auth+ vet appeals:
    - VERIFY_EMAIL_OWNERSHIP: Used to appeal a rejection if the email cannot be delivered due to a bounce, DNS problems, or other scenarios where it could not be delivered.
    - VERIFY_DOMAIN_OWNERSHIP: Used to appeal when domain ownership is not recognized. This allows the CSP to provide additional evidence to support domain ownership for the email address.

List Existing Auth+ Verification Appeals

`GET /brand/{brandId}/externalVetting/appeal`

Changes

- This endpoint fetches the appeal history for a brand (including Auth+ vet appeals). Supports querying by an appeal status.

Upload Auth+ Appeal Evidence Files

`POST /brand/{brandId}/appeal/evidence`

Changes

- This endpoint is used to upload Auth+ appeal evidence files. The returned `attachmentUuid` can be used in an Auth+ vet appeal.

List Auth+ Appeal Evidence Files

`GET /brand/{brandId}/appeal/evidence`

Changes

- This endpoint returns all evidence files for a brand (including those for Auth+).

Appendix B: New and Impacted Webhook Events

New Events

Event Type	Description

BRAND_AUTHPLUS_VERIFICATION_ADD	**Category:** VETTING
	Visible To:
	- CSP who initiated the event
	Triggered When:
	- Brand is initially submitted for Auth+ verification.
	Webhook Sample:
	`{`
	`"cspId": "S123ABC",`
	`"brandName": "BrandA",`
	`"brandReferenceId": "Unique Brand Reference ID",`
	`"brandId": "B123ABC",`
	`"description": "Brand B123ABC (BrandA) submitted for auth+ verification",`
	`"mock": false,`
	`"eventType": "BRAND_AUTHPLUS_VERIFICATION_ADD",`
	`"evpName": "Aegis Mobile",`
	`"evpId": "AEGIS",`
	`"vettingId": "Unique Vetting Id",`
	`"cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_RE_VERIFICATION_ADD	**Category:** VETTING **Visible To:** - CSP who initiated the event **Triggered When:** - Brand is submitted again after the first Auth+ verification. This could be the result of a failed Auth+ vet, or if the brand's identity information is changed (e.g., updating the **`businessContactEmail`**).

Event Type	Description

	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`
	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`
	`    "description": "Brand B123ABC (BrandA) submitted for auth+ re-verification",`
	`    "mock": false,`
	`    "eventType": "BRAND_AUTHPLUS_RE_VERIFICATION_ADD",`
	`    "evpName": "Aegis Mobile",`
	`    "evpId": "AEGIS",`
	`    "vettingId": "Unique Vetting Id",`
	`    "cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_DOMAIN_VERIFIED	**Category:** VETTING
	Visible To:
	● CSP who initiated the event
	Triggered When:
	● The brand's web domain is successfully verified against the brand's **`businessContactEmail`**.
	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`
	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`
	`    "description": "Domain verification for brand B123ABC (BrandA) is successful",`
	`    "mock": false,`
	`    "eventType": "BRAND_AUTHPLUS_DOMAIN_VERIFIED",`
	`    "evpName": "Aegis Mobile",`
	`    "evpId": "AEGIS",`

Event Type	Description

	`    "vettingId": "Unique Vetting Id",`
	`    "cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_DOMAIN_FAILED	**Category:** VETTING
	Visible To:
	- CSP who initiated the event
	Triggered When:
	- The brand's web domain cannot be matched with the brand's **`businessContactEmail`**.
	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`
	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`
	`    "description": "Domain verification for brand B123ABC (BrandA) is failed",`
	`    "mock": false,`
	`    "eventType": "BRAND_AUTHPLUS_DOMAIN_FAILED",`
	`    "evpName": "Aegis Mobile",`
	`    "evpId": "AEGIS",`
	`    "vettingId": "Unique Vetting Id",`
	`    "cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_2FA_VERIFIED	**Category:** VETTING
	Visible To:
	- CSP who initiated the event
	Triggered When:
	- Brand's Auth+ 2FA verification process is successful.
	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`

Event Type	Description

	`"brandReferenceId": "Unique Brand Reference ID",`
	`"brandId": "B123ABC",`
	`"description": "2FA verification for brand B123ABC (BrandA) is successful",`
	`"mock": false,`
	`"eventType": "BRAND_AUTHPLUS_2FA_VERIFIED",`
	`"evpName": "Aegis Mobile",`
	`"evpId": "AEGIS",`
	`"vettingId": "Unique Vetting Id",`
	`"cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_2FA_FAILED	**Category:** VETTING
	Visible To:
	● CSP who manages the brand
	Triggered When:
	● Brand's Auth+ 2FA verification process fails (e.g., the 2FA is never completed).
	Webhook Sample:
	`{`
	`"cspId": "S123ABC",`
	`"brandName": "BrandA",`
	`"brandReferenceId": "Unique Brand Reference ID",`
	`"brandId": "B123ABC",`
	`"description": "2FA verification for brand B123ABC (BrandA) is failed",`
	`"mock": false,`
	`"eventType": "BRAND_AUTHPLUS_2FA_FAILED",`
	`"evpName": "Aegis Mobile",`
	`"evpId": "AEGIS",`
	`"vettingId": "Unique Vetting Id",`
	`"cspName": "CSPA"`
	`}`

<table>
<tr><th>Event Type</th><th>Description</th></tr>
<tr><td>BRAND_AUTHPLUS_
VERIFICATION_
COMPLETE</td><td>

Category: VETTING
Visible To:

- CSP who manages the brand

Triggered When:

- Auth+ verification completed successfully. The Auth+ vetting status will change to ACTIVE.

Webhook Sample:

```
{
    "cspId": "S123ABC",
    "brandName": "BrandA",
    "brandReferenceId": "Unique Brand Reference ID",
    "brandId": "B123ABC",
    "description": "Auth+ verification is successfully completed for brand B123ABC (BrandA)",
    "mock": false,
    "eventType": "BRAND_AUTHPLUS_VERIFICATION_COMPLETE",
    "evpName": "Aegis Mobile",
    "evpId": "AEGIS",
    "vettingId": "Unique Vetting Id",
    "cspName": "CSPA"
}
```

</td></tr>
<tr><td>BRAND_AUTHPLUS_
VERIFICATION_
FAILED</td><td>

Category: VETTING
Visible To:

- CSP who manages the brand

Triggered When:

- The brand's Auth+ verification fails. The Auth+ vetting status will change to FAILED.

Webhook Sample:

```
{
    "cspId": "S123ABC",
    "brandName": "BrandA",
```

</td></tr>
</table>

Event Type	Description

	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`
	`    "description": "Auth+ verification is failed for brand B123ABC (BrandA)",`
	`    "mock": false,`
	`    "eventType": "BRAND_AUTHPLUS_VERIFICATION_FAILED",`
	`    "evpName": "Aegis Mobile",`
	`    "evpId": "AEGIS",`
	`    "vettingId": "Unique Vetting Id",`
	`    "cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_VERIFICATION_EXPIRED	**Category:** VETTING
	Visible To:
	- CSP who manages the brand.
	Triggered When:
	- Brand's Auth+ vet reaches its expired date. The Auth+ vetting status will change to EXPIRED.
	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`
	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`
	`    "description": "Auth+ verification is expired for brand B123ABC (BrandA)",`
	`    "mock": false,`
	`    "eventType": "BRAND_AUTHPLUS_VERIFICATION_EXPIRED",`
	`    "evpName": "Aegis Mobile",`
	`    "evpId": "AEGIS",`
	`    "vettingId": "Unique Vetting Id",`
	`    "cspName": "CSPA"`
	`}`

Event Type	Description

BRAND_AUTHPLUS_VERIFICATION_APPEAL_ADD	**Category:** VETTING
	Visible To:
	- CSP who initiated the event
	Triggered When:
	- A brand's Auth+ vetting status is FAILED and a CSP submits an appeal.
	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`
	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`
	`    "description": "New appeal request raised for auth+ verification for brand B123ABC (BrandA)",`
	`    "mock": false,`
	`    "eventType": "BRAND_AUTHPLUS_VERIFICATION_APPEAL_ADD",`
	`    "evpName": "Aegis Mobile",`
	`    "evpId": "AEGIS",`
	`    "vettingId": "Unique Vetting Id",`
	`    "cspName": "CSPA"`
	`}`

BRAND_AUTHPLUS_VERIFICATION_APPEAL_COMPLETE	**Category:** VETTING
	Visible To:
	- CSP who initiated the event
	Triggered When:
	- A brand's Auth+ appeal is complete.
	Webhook Sample:
	`{`
	`    "cspId": "S123ABC",`
	`    "brandName": "BrandA",`
	`    "brandReferenceId": "Unique Brand Reference ID",`
	`    "brandId": "B123ABC",`

Event Type	Description
	"description": "Appeal request received an update for auth+ verification for brand B123ABC (BrandA)", "mock": false, "eventType": "BRAND_AUTHPLUS_VERIFICATION_APPEAL_COMPLETE", "evpName": "Aegis Mobile", "evpId": "AEGIS", "vettingId": "Unique Vetting Id", "cspName": "CSPA" }

BRAND_EMAIL_2FA_EXPIRED	**Category:** VETTING
	Visible To:
	● CSP who manages the brand
	Triggered When:
	● When the issued 2FA PIN expires.
	Webhook Sample:
	{
	"brandId": "B123ABC",
	"brandName": "BrandA",
	"cspId": "S123ABC",
	"cspName": "CSP_X",
	"description": "The 2FA pin was expired",
	"eventType": "BRAND_EMAIL_2FA_EXPIRED",
	"brandReferenceId": null,
	"mock": false
	}

Impacted Events

Event Type	Description
BRAND_EMAIL_2FA_COMPLETE	This event is now retired with the Auth+ 2.0 release. Instead, the BRAND_AUTHPLUS_VERIFICATION_COMPLETE event will signal when Auth+ verification is complete.

BRAND_EMAIL_2FA_SEND	**Category:** VETTING
	Visible To:
	- CSP who manages the brand
	Triggered When:
	- A 2FA email is sent to the brand's business contact.
	Webhook Sample:
	`{`
	`  "cspId": "S123ABC",`
	`  "brandName": "Brand_X",`
	`  "brandReferenceId": null,`
	`  "brandId": "B123ABC",`
	`  "description": "The 2FA email is sent to brand B123ABC (2FA resend feature)",`
	`  "mock": false,`
	`  "eventType": "BRAND_EMAIL_2FA_SEND",`
	`  "cspName": "CSP_X"`
	`}`

BRAND_EMAIL_2FA_OPEN	**Category:** VETTING
	Visible To:
	- CSP who manages the brand
	Triggered When:
	- The brand's business contact opens the 2FA email.
	Webhook Sample:
	`{`
	`  "cspId": "S123ABC",`
	`  "brandName": "Brand_X",`
	`  "brandReferenceId": null,`
	`  "brandId": "B123ABC",`

<table>
<tr>
<td></td>
<td>

```
  "description": "The 2FA email is opened by brand B123ABC (2FA resend feature)",
  "mock": false,
  "eventType": "BRAND_EMAIL_2FA_OPEN",
  "cspName": "CSP_X"
}
```

</td>
</tr>
<tr>
<td>BRAND_EMAIL_2FA_CLICK</td>
<td>

Category: VETTING
Visible To:

- CSP who initiated the event

Triggered When:

- The brand’s business contact clicks on the link in 2FA the email.

Webhook Sample:

```
{
  "cspId": "S123ABC",
  "brandName": "Brand_X",
  "brandReferenceId": null,
  "brandId": "B123ABC",
  "description": "Brand B123ABC (Brand_X) clicks the 2FA verification link",
  "mock": false,
  "eventType": "BRAND_EMAIL_2FA_CLICK",
  "cspName": "CSP_Z"
}
```

</td>
</tr>
</table>