Upcoming changes to DeepAffex™ Cloud API - Token binding and token lifetime

Introduction

This article describes upcoming **mandatory security changes** to the DeepAffex™ Cloud API that will prevent client apps from copying a validated DeepAffex™ token onto another (non-validated) physical device and will expire tokens after a fixed duration.

These changes may **impact existing client user experience and possibly *break your working app***. We therefore strongly encourage you to modify your app to account for this update.

1. Token lifetime: DeepAffex™ tokens will expire within 24 hours after they are issued

After this change is deployed, DeepAffex™ tokens will expire 24 hours after they are issued.

You can use a *Refresh Token* to obtain a new pair of tokens after a token has expired.

Token lifetime will go live on **November 28, 2023**.

2. Token binding: DeepAffex™ tokens will be bound to caller IP, user-agent and device ID

After this change is deployed, the DeepAffex™ Cloud will associate *caller IP address, caller user-agent and device ID* with the issued DeepAffex™ token. If a valid token is subsequently used to call the DeepAffex™ Cloud API from a new IP address or with a new user-agent, then the call will fail with an HTTP 406 error code.

To ensure that your devices retain the ability to "roam" across multiple networks, you can use a Refresh Token to obtain a new pair of tokens bound to the new IP and user-agent.

Token binding will go live in **2024 (Exact date TBD)**

Both token lifetime and token binding changes should be handled in the same exact code in your app which should verify, and refresh tokens as needed.

Impact

Product	Affected	Comments
DeepAffex™ Dashboard	No	See Questions at the end
Web Measurement Service	No **unless you are not including a *Refresh Token* in the Call-in URL**	See Questions at the end
Anura Web Enterprise	No	See Questions at the end
Anura Mobile (iOS / Android)	No	
Anura Mobile Enterprise (iOS / Android)	No	See Questions at the end
Anura Core SDK (iOS / Android)	**Yes, upgrade needed**	See Questions at the end
Customer networking code	**Yes, upgrade needed**	See Questions at the end

New and Modified Endpoints

Register License (modified)

The organizations/register-license endpoint has been modified so that:

- The request will contain a *TokenExpiresIn* field.
    - The token will expire after a duration which is the minimum of *TokenExpiresIn*, and license expiration date. By default, the token will expire in 24 hours.
- The response will contain, in addition to the *Device Token*, a *One-Time Refresh Token (OTRT)*.
    - This will be a single-use token and should be saved securely.
- To bind a new IP and new user-agent to the *Device Token*, or to renew it (before or after it has expired,) call the auths/renew endpoint (discussed below) with the *OTRT*.

User Login (modified)

The following endpoints will be **deprecated** and replaced. They will be aliased to the replacements:

Deprecated	Replacement
users/request-phone-login-code	auths/request-login-code

The login endpoints (users/login, users/login-with-phone-code, organizations/login and organizations/login-with-token) will be modified so that:

- The token will expire after 24 hours (or at your license expiration date if it's earlier.)
- The response will contain, in addition to the *User Token*, a *One-Time Refresh Token (OTRT)*.
    - This will be a single-use token and should be saved securely.
- To bind a new IP and new user-agent to the *User Token*, or to renew if after it has expired, call the auths/renew endpoint (discussed below) with the *OTRT*.

Renew Token (new)

The auth/renew endpoint is a new endpoint which will:

- Issue a new *Device Token* or *User Token* that is bound to a new IP and new user-agent (if applicable) and with a fresh expiry duration (calculated the same as above)
- Also issue a new *One-Time Refresh Token (OTRT)*.
- This endpoint will additionally invalidate the old access token.

Create Child Token (new)

The auths/generateToken endpoint is a new endpoint which will:

- Create a child token from a valid *Device Token or User Token* and *One-Time Refresh Token (OTRT)*.
    - The child token obtained will be valid for a minimum of the parent Token's expiry, the request parameter *expiryInSec* or 30 minutes.
- This endpoint will **not** invalidate the input access token.
- This endpoint is primarily used in the Web Measurement Service(WMS). In WMS, the Device Token Pair is obtained by your server and immediately exchanged with a new pair once it reaches the WMS using this endpoint.
- The child token inherits all the permissions from the parent token.

Code showing how to verify and renew tokens

Old API Client pseudocode	New API Client pseudocode

`# Use previously token to create the headers`
`config = load_config()`
`token = config.device_token`
`headers = {"Authorization": f"Bearer {token}"}`
 	
`# Verify that our token is still valid`
`status, body = dfxapi.General.verify_token(headers=headers)`
`if status >= 400:`
`print("Your token is not valid, please register and login again")`
`clear_config(config)`
`save_config(config)`
`return FAIL # Failed since token is not ACTIVE`
 	
`# Continue with verified headers`
	`# Use previously saved token to create the headers`
	`config = load_config()`
	`token = config.device_token`
	`refresh_token = config.device_refresh_token`
	`headers = {"Authorization": f"Bearer {token}"}`
	
	`# Verify that our token is still valid`
	`status, body = dfxapi.General.verify_token(headers=headers)`
	`if status >= 400:`
	`    # Attempt to renew token`
	`    renew_status, renew_body = dfxapi.Auths.renew_token(token, refresh_token)`
	
	`    # Renew failed`
	`    if renew_status >= 400:`
	`        # Show error from verify_token failure`
	`        print("Your token could not be verified and token refresh failed, please register again!")`
	
	`        return FAIL # Failed since API is not ACTIVE`
	
	`    # Renew worked, so save new tokens`
	`    token = renew_body.token`
	`    refresh_token = renew_body.refresh_token`
	`    update_config(config, token, refresh_token)`
	`    save_config(config)`
	
	`    # Adjust headers`
	`    headers = {"Authorization": f"Bearer {token}"}`
	
	# Continue with verified / refreshed headers

Important Dates

2022-03-22: Refresh tokens and related API endpoints available on the DeepAffex™ API

2023-05-11: WMS updates to handle token expiry and token binding

2023-08-01: Android Anura Core SDK updates to handle token expiry and token binding

2023-08-15: iOS Anura Core SDK updates to handle token expiry and token binding

⚠**2023-11-28**: Token expiry enabled on the DeepAffex™ API

⚠**2024-XX-YY**: Token binding enabled on the DeepAffex™ API

Questions

We use DeepAffex™ Dashboard. How will we be affected?

DeepAffex™ Dashboard will be updated to handle this and should continue to work.

We use the Web Measurement Service (WMS). How will we be affected?

Web Measurement Service has been updated to handle this and should continue to work.

⚠If you implemented WMS before the WMS Sample App was updated to handle Refresh Tokens (2022-05-11) or if you implemented your own backend to register the DeepAffex™ license, you must update your application. The server component or your backend **must obtain and then pass the Refresh Token to the front end. The front end must include it while constructing the Call-in URL.** You can see it as part of the Call-in URL structure at Service Details - NuraLogix™ Web Measurement Service. Please refer to the latest WMS sample for the implementation details.

We use the Anura Web Enterprise (AWE) application. How will we be affected?

Anura Web Enterprise has been updated to handle this and should continue to work.

We use Anura Mobile Enterprise (iOS / Android) app. How will we be affected?

Anura Mobile apps (iOS and Android) will be updated to handle this and should continue to work. Please ensure your users update to the latest versions of the apps when they are released.

Our app uses Anura Core SDK (iOS / Android). How will we be affected?

You will need to upgrade to the latest versions of Anura Core SDK Android v2.4.x (which will call the new endpoints for you via its internal API Client) and to Anura Core SDK iOS v1.9.x (which will call the new endpoints for you via its API Client that is part of the Sample App).

If you don't upgrade, your app may work if it follows the license registration and token validation best practices as documented in the Anura Core SDK Developer Guide and as implemented in the Sample Apps for iOS and Android.

⚠️If you are not using Anonymous Measurement mode (i.e. you are using User Tokens) then your users will get logged out very often - **you must upgrade in this case**.

Our app handles all networking and calls the DeepAffex™ API directly. How will we be affected?

Unless you are using Anonymous Measurements and checking for token validity, then you will likely be affected.

⚠️**You must update** all of your REST and/or WebSocket code using the updated documentation published in our Apiary.
