The bridge to possible

Implementing OAuth 2.0

Authorization for Webex Integrations

Joe Zanini Developer Evangelist + Webex App Hub Reviewer
@joezanini

DEVNET-2675

Cisco Webex App

Questions?

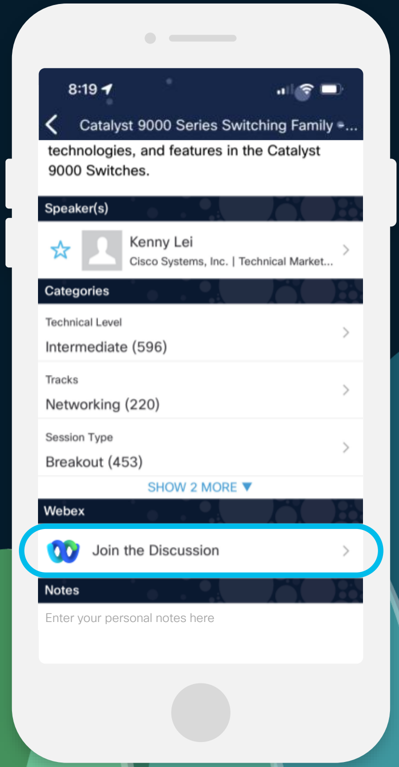
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 7, 2024.

https://ciscolive.ciscoevents.com/
ciscolivebot/#DEVNET-2675



8:19

Catalyst 9000 Series Switching Family -...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

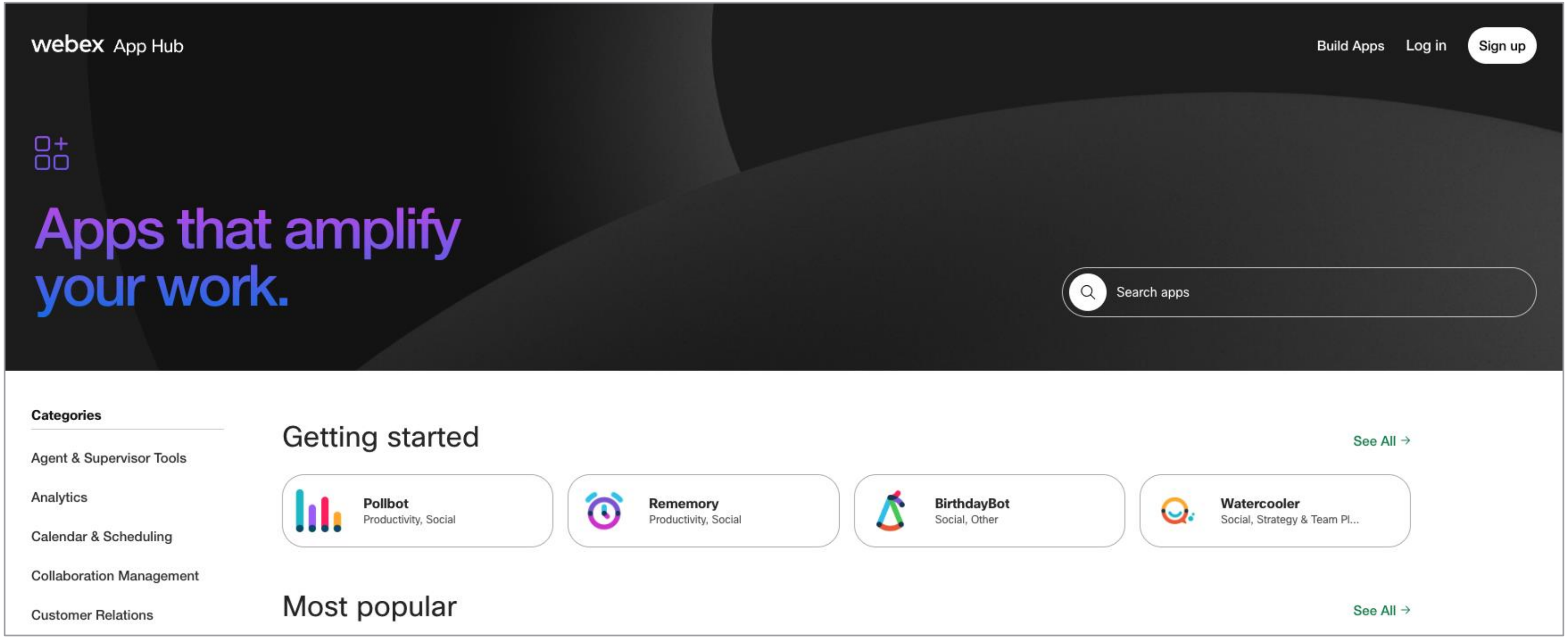
- Introduction
- History of Authorization
- Intro to OAuth 1.0 + 2.0
- How to OAuth 2.0
- Webex and OAuth 2.0

Webex Developer Featured Demos Schedule

Monday, June 3rd	Tuesday, June 4th	Wednesday, June 5th
11:00 AM – Our Vision, Your Voice: “Bring Your Own AI”	12:00 PM – Instant Connect	11:00 AM – Build and Use a Service App
1:00 PM – Build Embedded Apps	2:00 PM – Flow Designer	12:00 PM – Build a Webex Bot
4:00 PM – Webex Contact Center Desktop Widgets	4:00 PM – AI Assistant Preview	3:00 PM – Webex Meetings SDK

Introduction

Webex App Hub : https://apphub.webex.com



webex App Hub

Build Apps Log in Sign up

Apps that amplify your work.

Search apps

Categories

- Agent & Supervisor Tools
- Analytics
- Calendar & Scheduling
- Collaboration Management
- Customer Relations

Getting started

See All →

Pollbot
Productivity, Social

Rememory
Productivity, Social

BirthdayBot
Social, Other

Watercooler
Social, Strategy & Team Pl...

Most popular

See All →

MoYoBi - Analyze & Monitor your Webex platform

What is MoYoBi?

MoYoBi is a cloud-based software solution that provides real-time call queuing monitoring, analytics, and reporting for Webex Calling.

It offers advanced features such as customizable dashboards and reports to help businesses achieve their

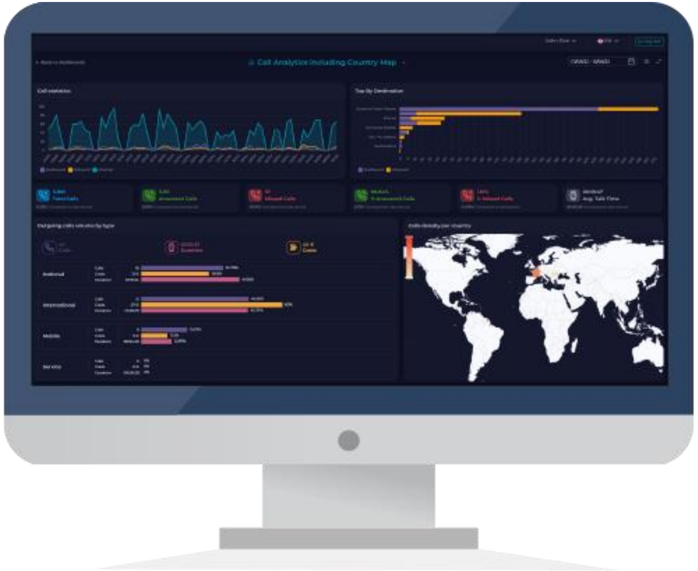
Value to Customer:

Provides insights into collaboration usage, adoption, and performance that can help customers optimize their communication workflows and increase productivity.

Offers customizable dashboards and reporting features, giving customers the flexibility to track the metrics that matter most to their business.

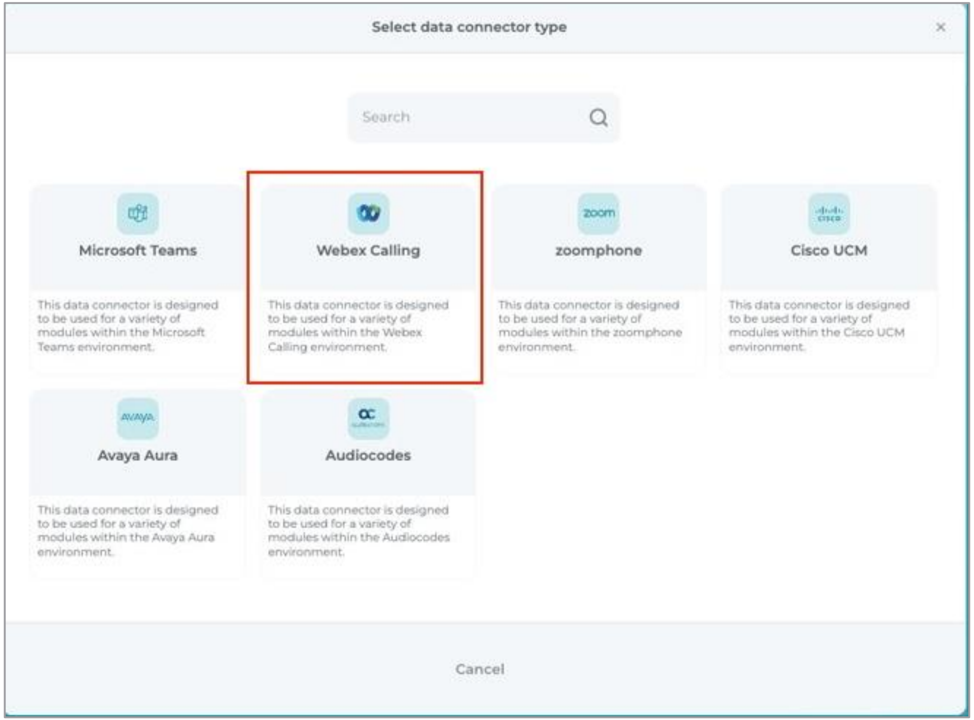
Easy to install and use. It integrates seamlessly with Webex Calling and provides a user-friendly interface that makes it easy to access.

Scalable solution that grows with the need of customers. It can accommodate small teams or large enterprises.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Experience with Webex Integrations



Select data connector type

Search

Microsoft Teams

This data connector is designed to be used for a variety of modules within the Microsoft Teams environment.

Webex Calling

This data connector is designed to be used for a variety of modules within the Webex Calling environment.

zoomphone

This data connector is designed to be used for a variety of modules within the zoomphone environment.

Cisco UCM

This data connector is designed to be used for a variety of modules within the Cisco UCM environment.

Avaya Aura

This data connector is designed to be used for a variety of modules within the Avaya Aura environment.

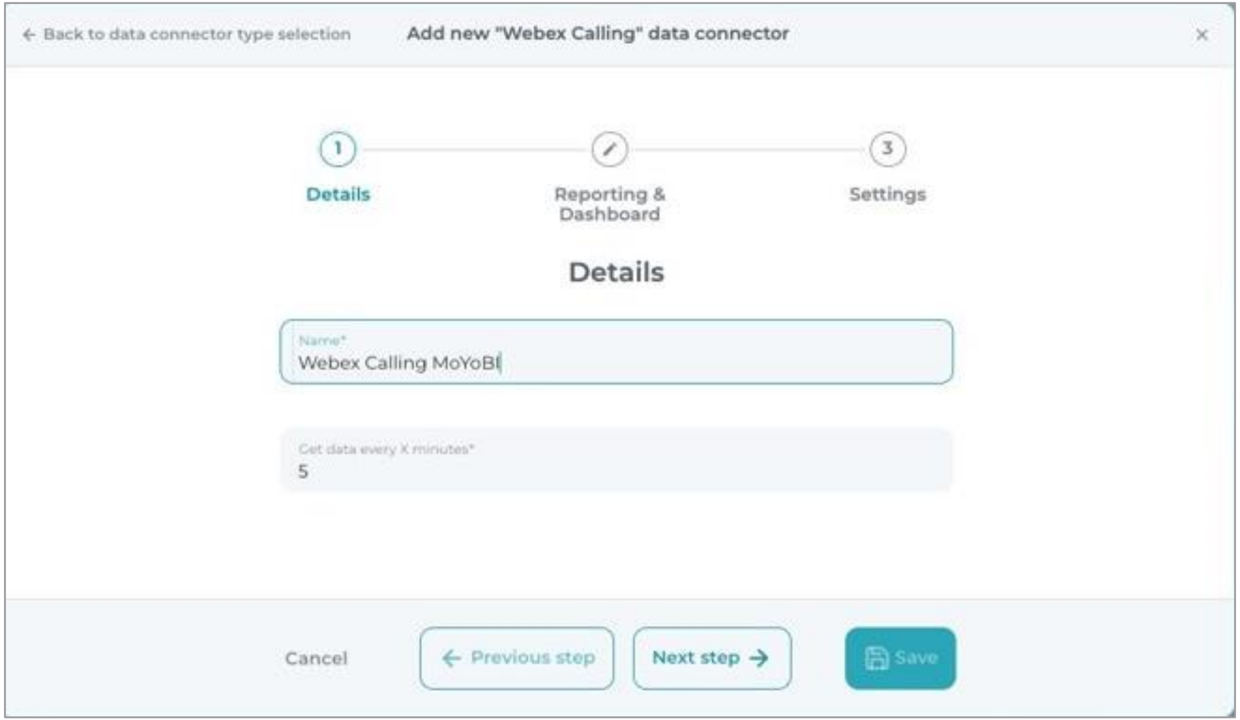
Audiocodes

This data connector is designed to be used for a variety of modules within the Audiocodes environment.

Cancel

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Experience with Webex Integrations



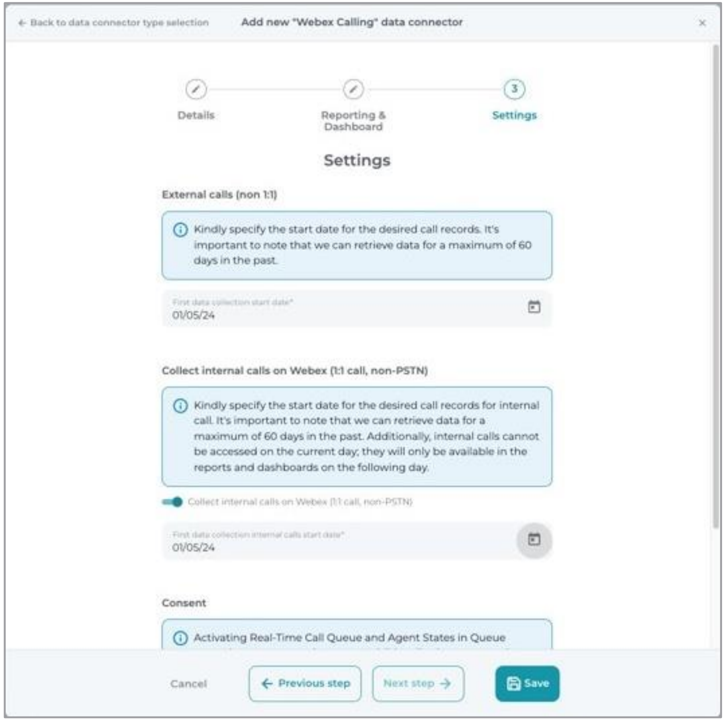
Add new "Webex Calling" data connector

Details

Name*
Webex Calling MoYoBI

Get data every X minutes*
5

User Experience with Webex Integrations



← Back to data connector type selection

Add new "Webex Calling" data connector

Settings

External calls (non 1:1)

ⓘ Kindly specify the start date for the desired call records. It's important to note that we can retrieve data for a maximum of 60 days in the past.

First data collection start date*
01/05/24

Collect internal calls on Webex (1:1 call, non-PSTN)

ⓘ Kindly specify the start date for the desired call records for internal call. It's important to note that we can retrieve data for a maximum of 60 days in the past. Additionally, internal calls cannot be accessed on the current day; they will only be available in the reports and dashboards on the following day.

● Collect internal calls on Webex (1:1 call, non-PSTN)

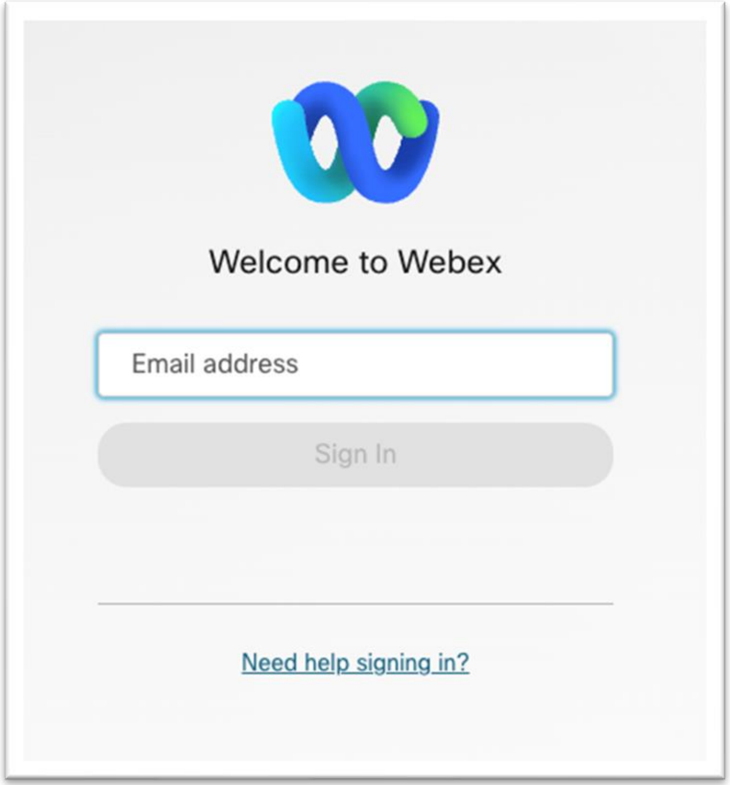
First data collection internal calls start date*
01/05/24

Consent

ⓘ Activating Real-Time Call Queue and Agent States in Queue

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Experience with Webex Integrations

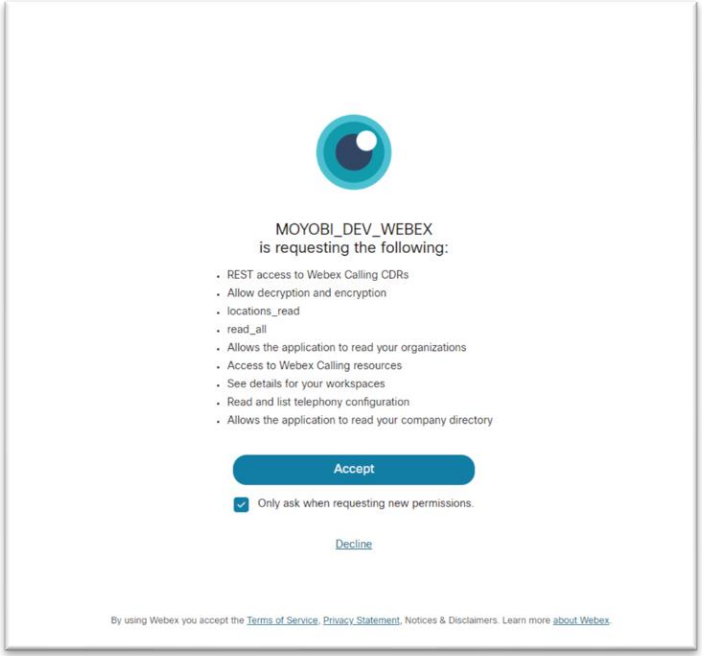


Welcome to Webex

Email address

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

User Experience with Webex Integrations



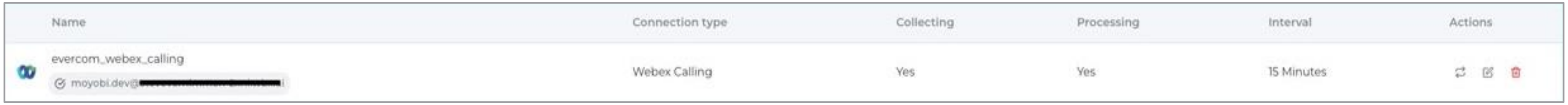
MOYOBI_DEV_WEBEX
is requesting the following:

- REST access to Webex Calling CDRs
- Allow decryption and encryption
- locations_read
- read_all
- Allows the application to read your organizations
- Access to Webex Calling resources
- See details for your workspaces
- Read and list telephony configuration
- Allows the application to read your company directory

☑ Only ask when requesting new permissions.

By using Webex you accept the Terms of Service, Privacy Statement, Notices & Disclaimers. Learn more about Webex.

User Experience with Webex Integrations



Name	Connection type	Collecting	Processing	Interval	Actions
evercom_webex_calling moyobi.dev@[redacted]	Webex Calling	Yes	Yes	15 Minutes	⟳ ✎ 🗑

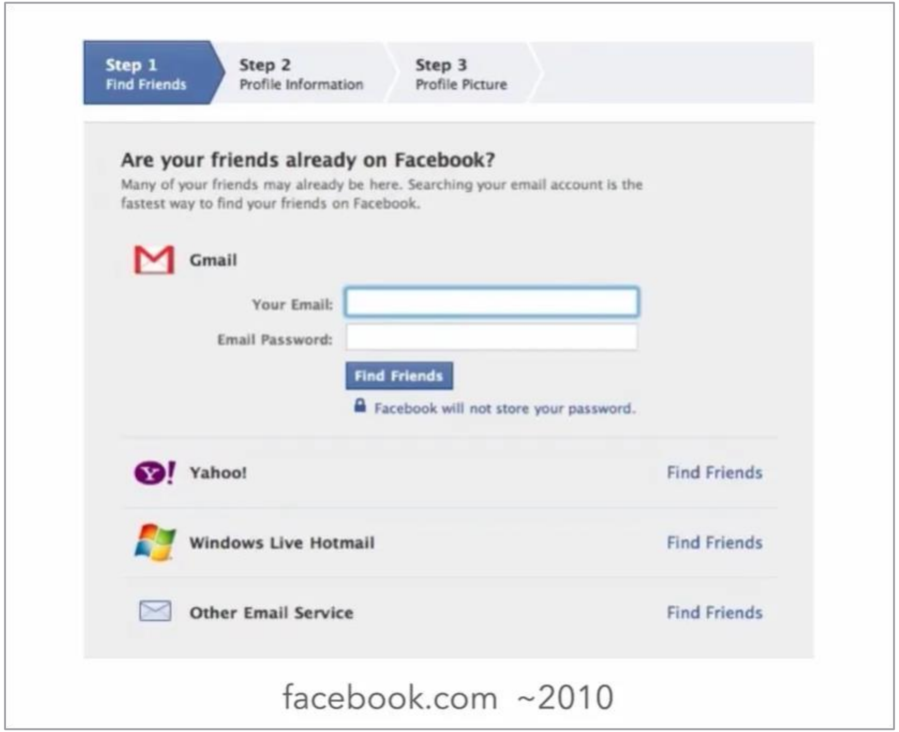
History of Authorization

HTTP Basic Auth

- User gives the application a user id and password
- API request contains a header field in the form of

```
Authorization: Basic <credentials>
```

- <credentials> is a Base64 encoding of ID and password joined by a single colon ":"



Are your friends already on Facebook?

Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

Gmail

Your Email:

Email Password:

Facebook will not store your password.

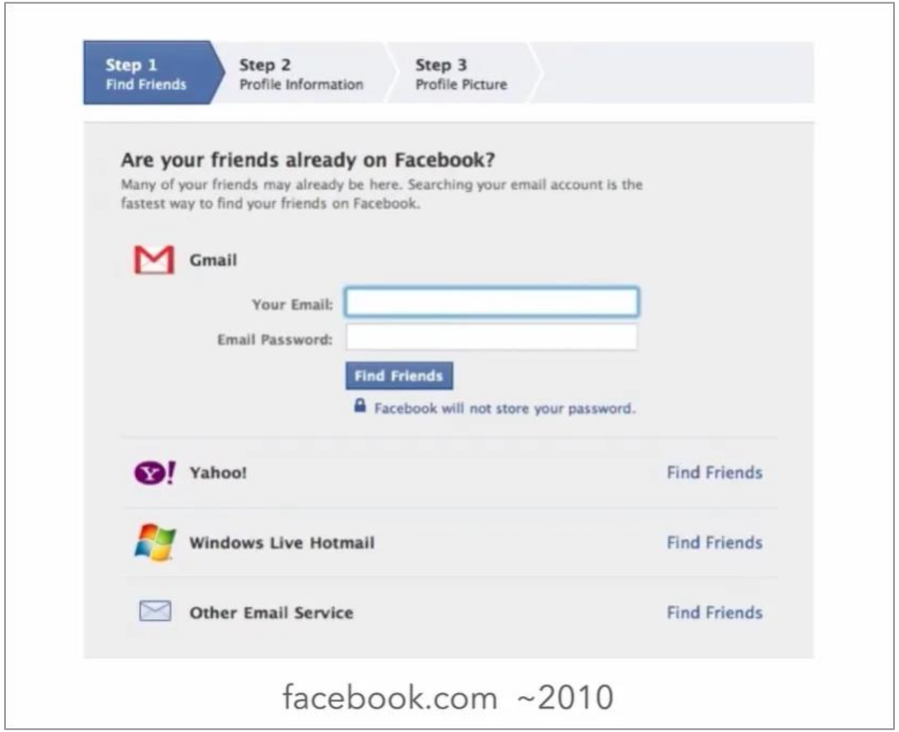
Yahoo!	Find Friends
Windows Live Hotmail	Find Friends
Other Email Service	Find Friends

facebook.com ~2010

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

HTTP Basic Auth

- There is no encryption unless the developer bakes in HTTPS
- Users must either log in all the time or be OK with creds being cached in the browser.



Step 1 Find Friends
Step 2 Profile Information
Step 3 Profile Picture

Are your friends already on Facebook?

Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

Gmail

Your Email:

Email Password:

Facebook will not store your password.

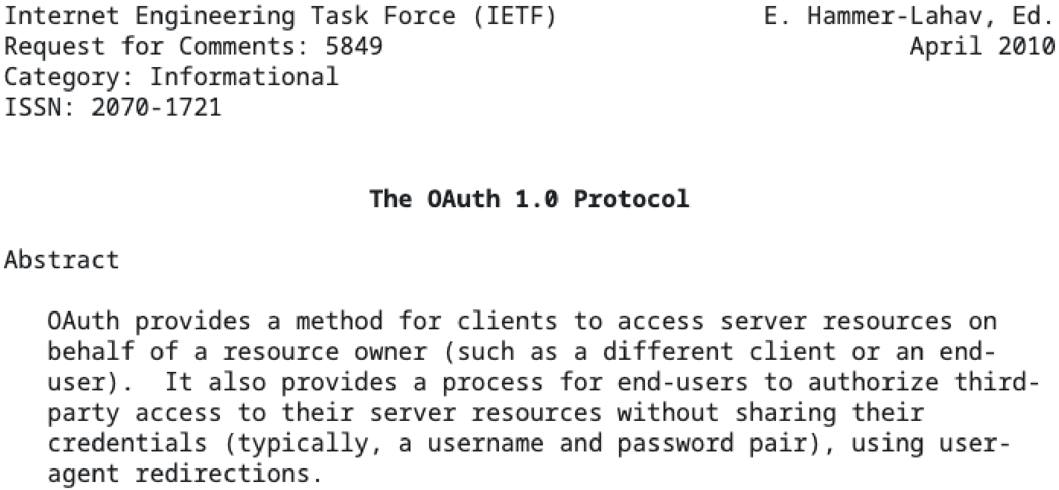
Yahoo! Find Friends
Windows Live Hotmail Find Friends
Other Email Service Find Friends

facebook.com ~2010

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Intro to OAuth

OAuth 1.0



```
Internet Engineering Task Force (IETF)                 E. Hammer-Lahav, Ed.
Request for Comments: 5849                                       April 2010
Category: Informational
ISSN: 2070-1721
```

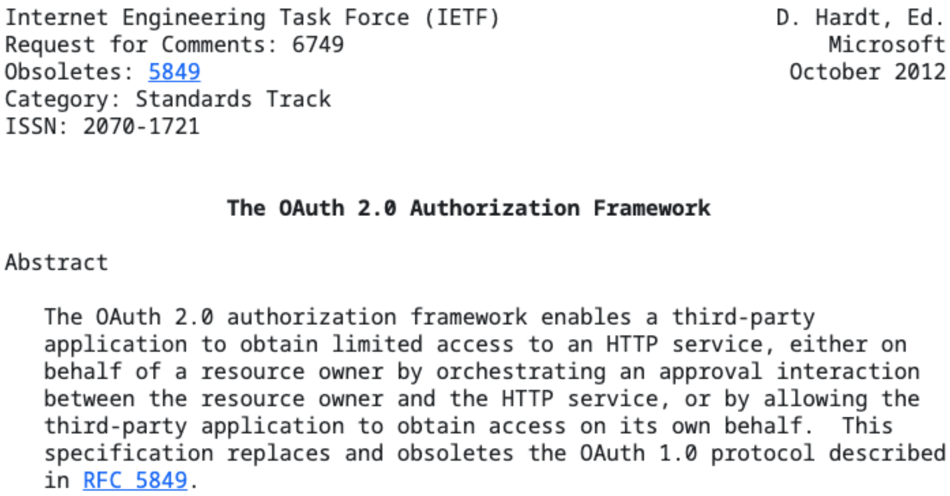
The OAuth 1.0 Protocol

Abstract

OAuth provides a method for clients to access server resources on behalf of a resource owner (such as a different client or an end-user). It also provides a process for end-users to authorize third-party access to their server resources without sharing their credentials (typically, a username and password pair), using user-agent redirections.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0



Internet Engineering Task Force (IETF)　　D. Hardt, Ed.
Request for Comments: 6749　　Microsoft
Obsoletes: 5849　　October 2012
Category: Standards Track
ISSN: 2070-1721

The OAuth 2.0 Authorization Framework

Abstract

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf. This specification replaces and obsoletes the OAuth 1.0 protocol described in RFC 5849.

OAuth 2.0

- Security is delegated to HTTPS/TLS
- Simpler implementation for developers
- Centered in bearer tokens (RFC6750)
- More usable with non-web clients

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to OAuth

OAuth 2.0 Various Flows

- Authorization Code Flow
- Athorization Code Flow w/ PKCE
- Device Code Flow

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Getting Started

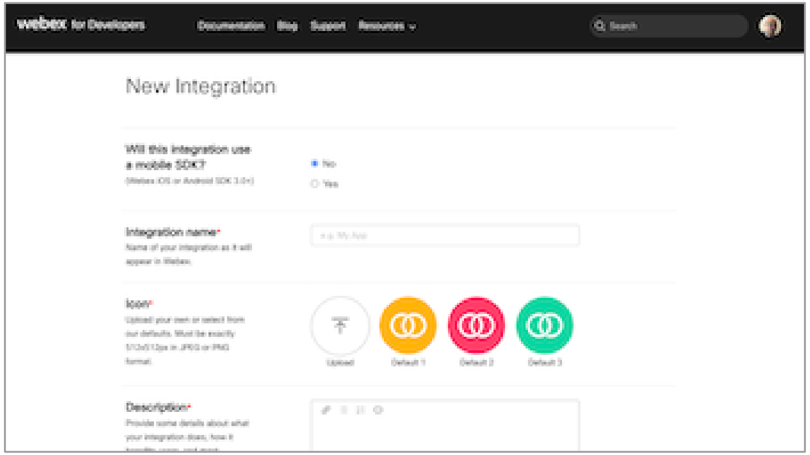
Your Application

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Getting Started

0. Go to https://developer.webex.com/ and register a new integration in exchange for a Client ID and Client Secret.

Your Application



New Integration

Will this integration use a mobile SDK?
(Webex iOS or Android SDK 3.0+)

● No
○ Yes

Integration name*
Name of your integration as it will appear in Webex.

e.g. My App

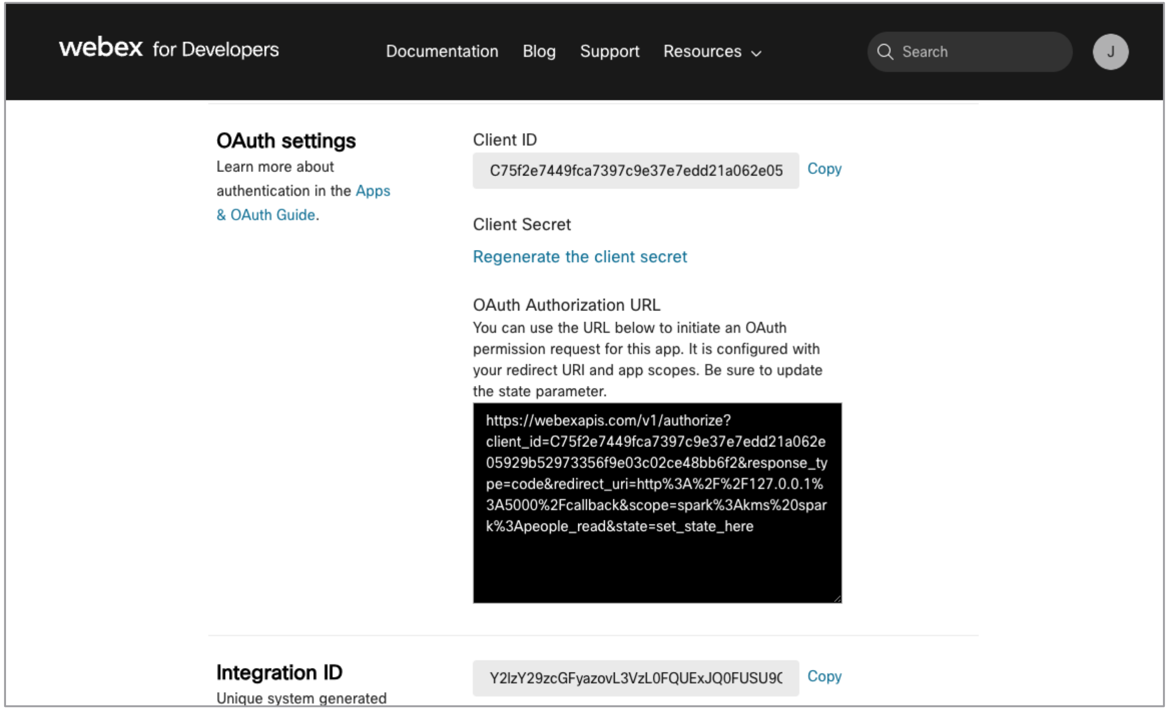
Icon*
Upload your own or select from our defaults. Must be exactly 512x512px in JPEG or PNG format.

Upload Default 1 Default 2 Default 3

Description*
Provide some details about what your integration does, how it

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Getting Started



OAuth settings

Learn more about authentication in the Apps & OAuth Guide.

Client ID

C75f2e7449fca7397c9e37e7edd21a062e05 Copy

Client Secret

Regenerate the client secret

OAuth Authorization URL

You can use the URL below to initiate an OAuth permission request for this app. It is configured with your redirect URI and app scopes. Be sure to update the state parameter.

```
https://webexapis.com/v1/authorize?
client_id=C75f2e7449fca7397c9e37e7edd21a062e
05929b52973356f9e03c02ce48bb6f2&response_ty
pe=code&redirect_uri=http%3A%2F%2F127.0.0.1%
3A5000%2Fcallback&scope=spark%3Akms%20spar
k%3Apeople_read&state=set_state_here
```

Integration ID

Unique system generated

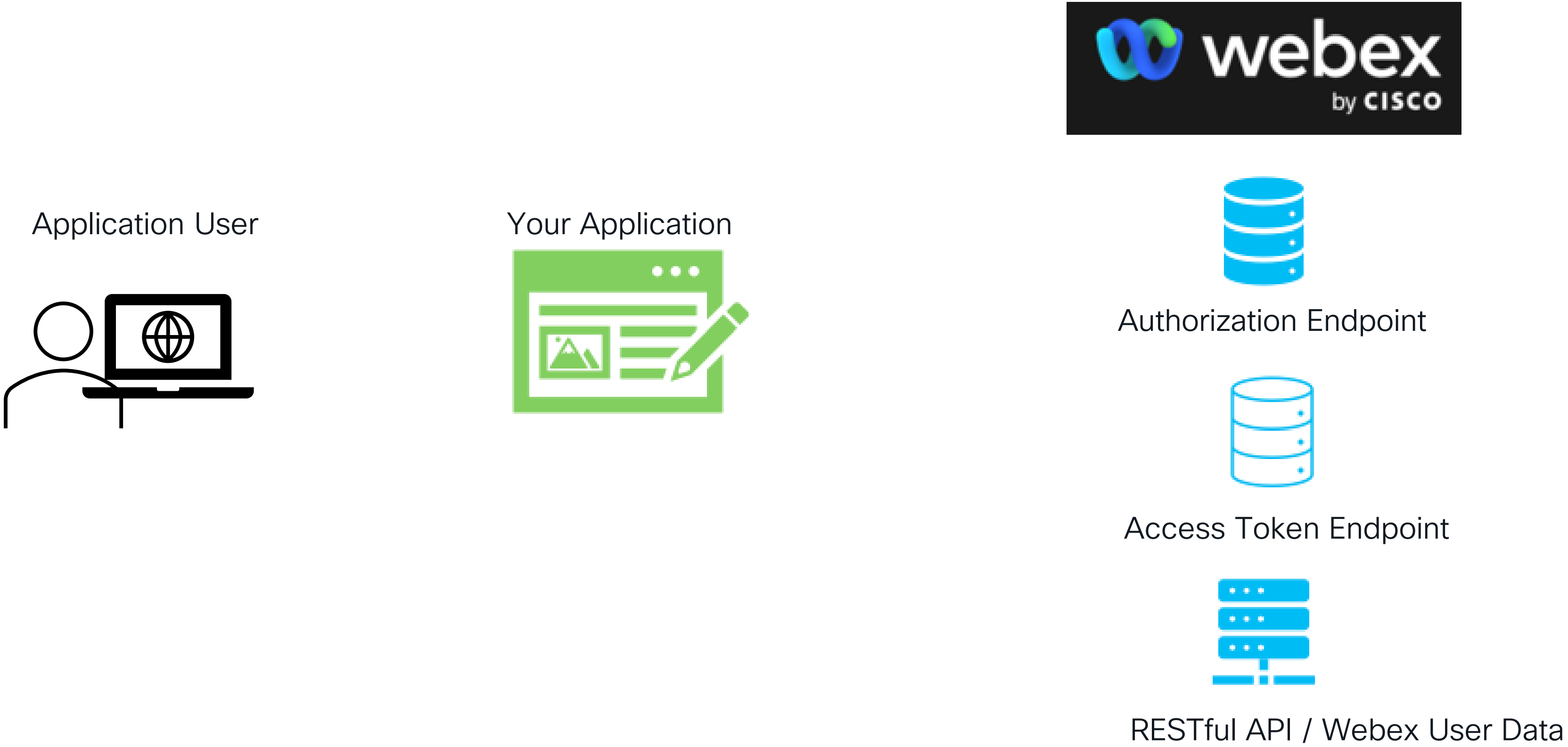
Y2lzY29zcGFyazovL3VzL0FQUExJQ0FUSU9(Copy

Authorization Endpoint

Access Token Endpoint

RESTful API / Webex User Data

OAuth 2.0 : Getting Started



Application User

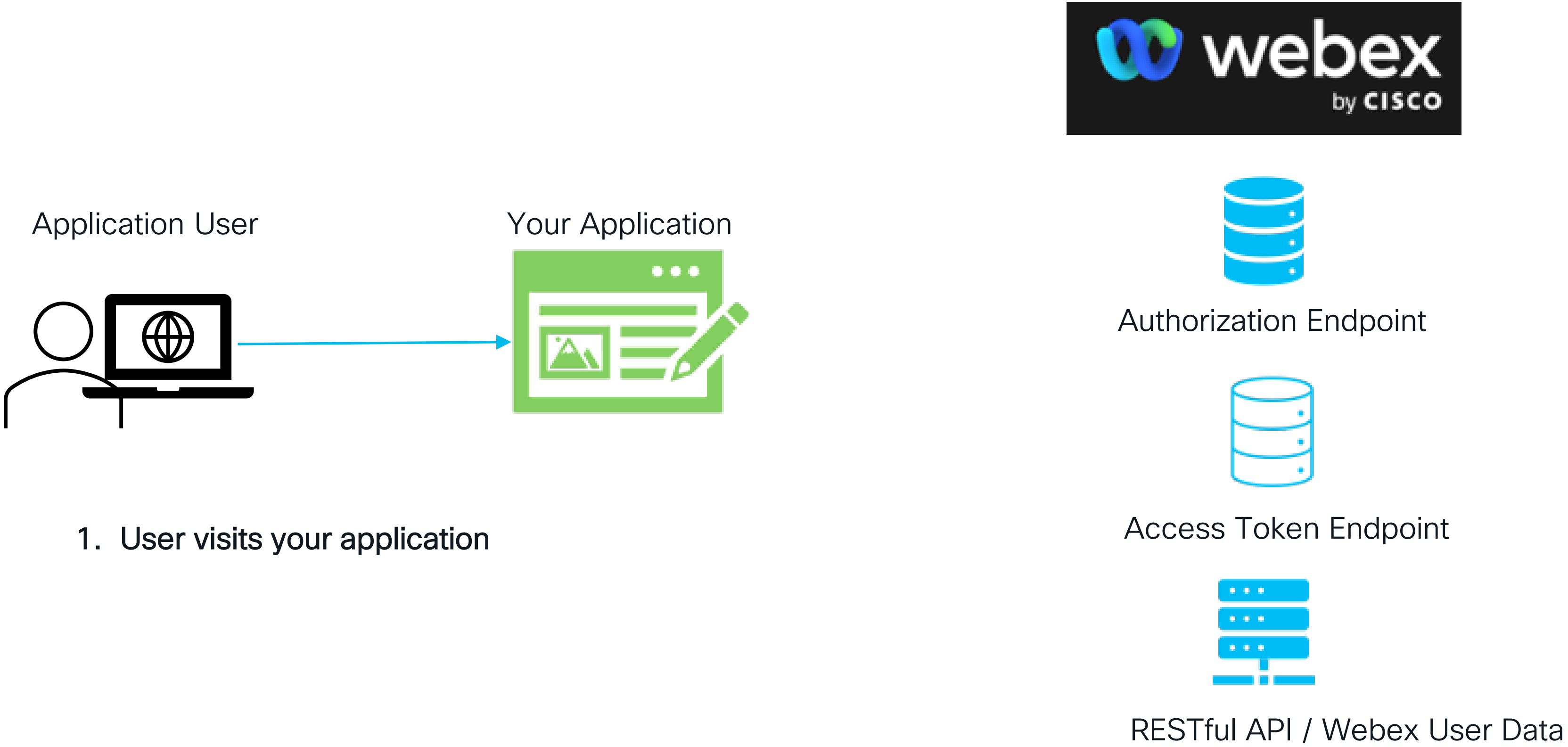
Your Application

Authorization Endpoint

Access Token Endpoint

RESTful API / Webex User Data

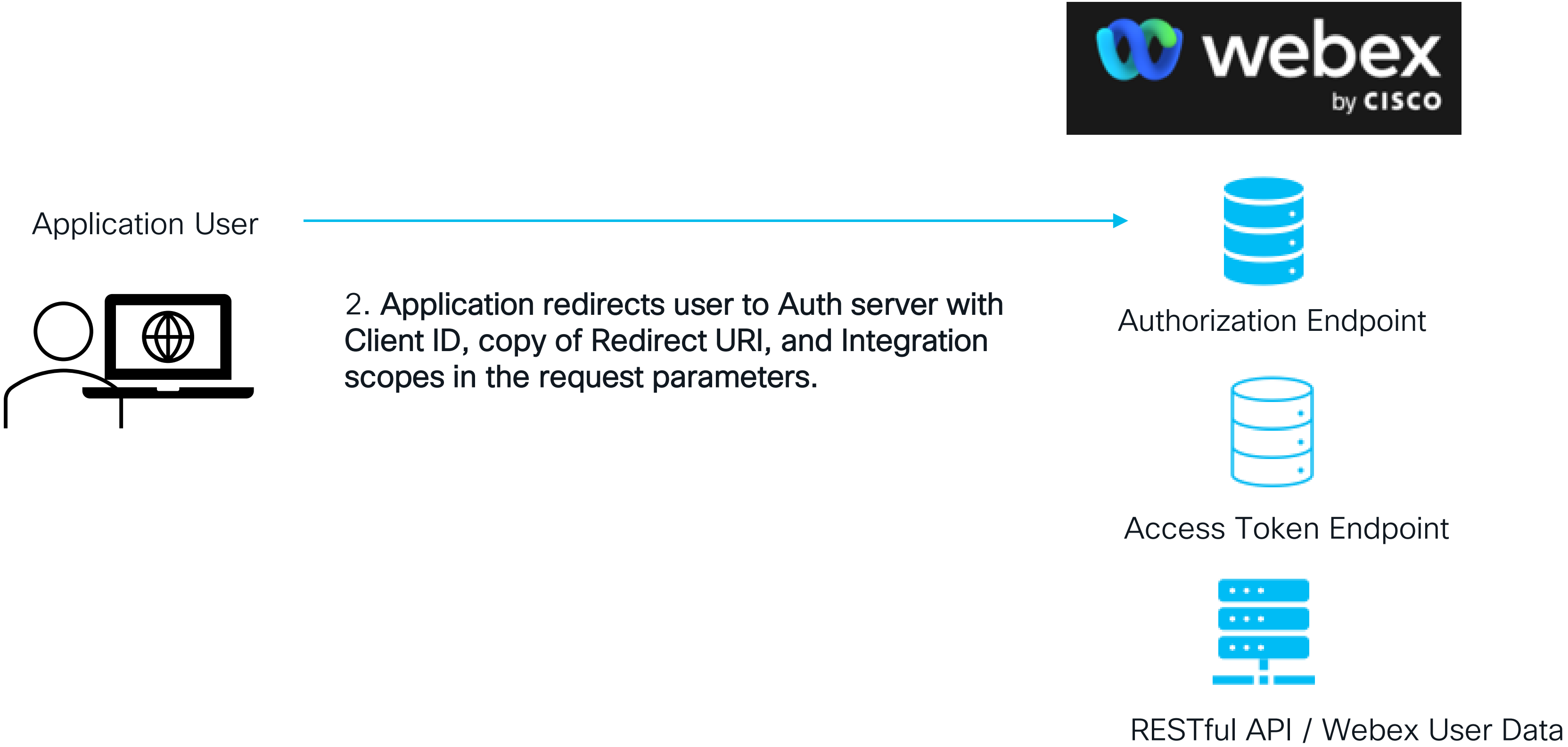
OAuth 2.0 : Authorization Code Flow



1. User visits your application

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow



Application User

2. Application redirects user to Auth server with Client ID, copy of Redirect URI, and Integration scopes in the request parameters.

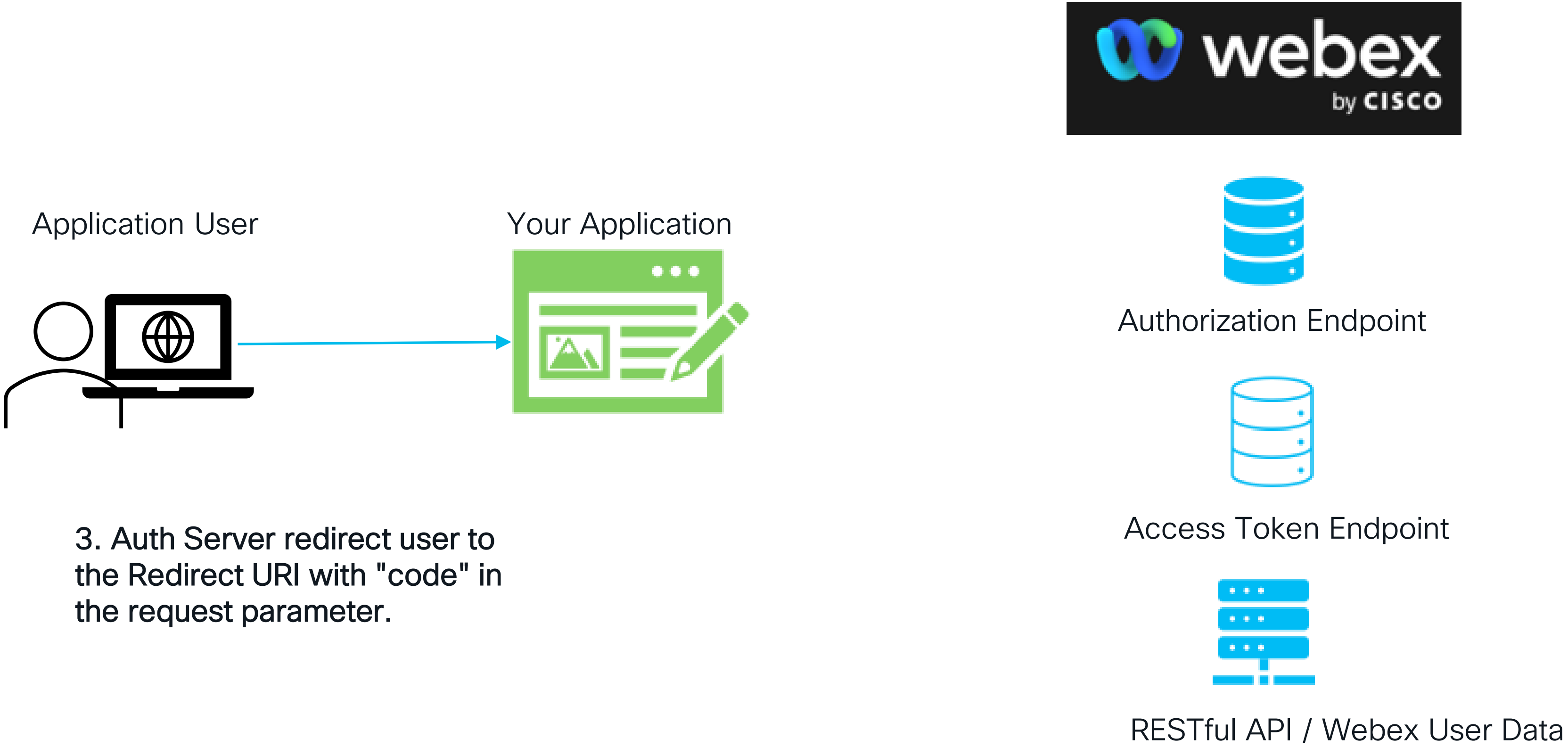
Authorization Endpoint

Access Token Endpoint

RESTful API / Webex User Data

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow



Application User

Your Application

Authorization Endpoint

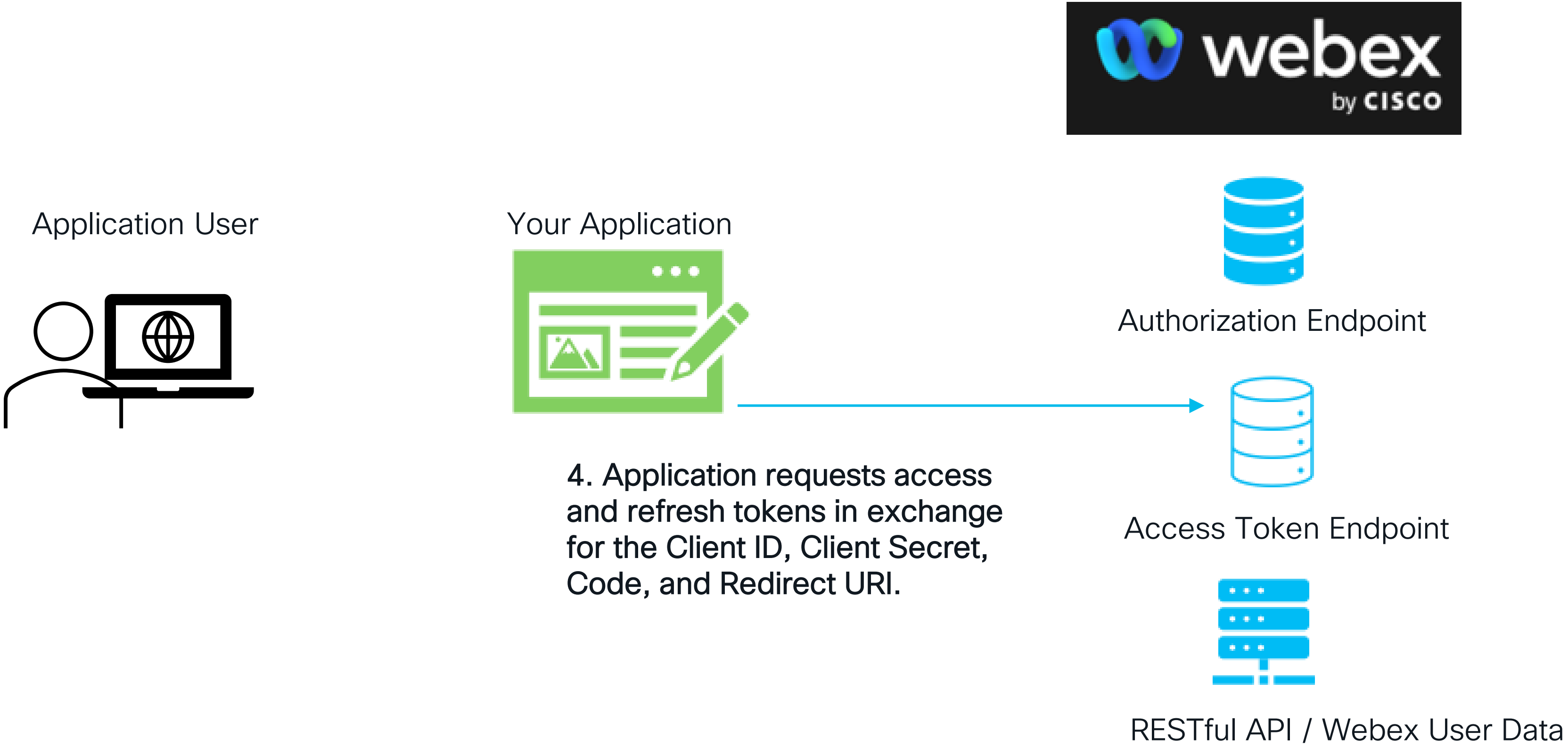
Access Token Endpoint

RESTful API / Webex User Data

3. Auth Server redirect user to the Redirect URI with "code" in the request parameter.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow



Application User

Your Application

Authorization Endpoint

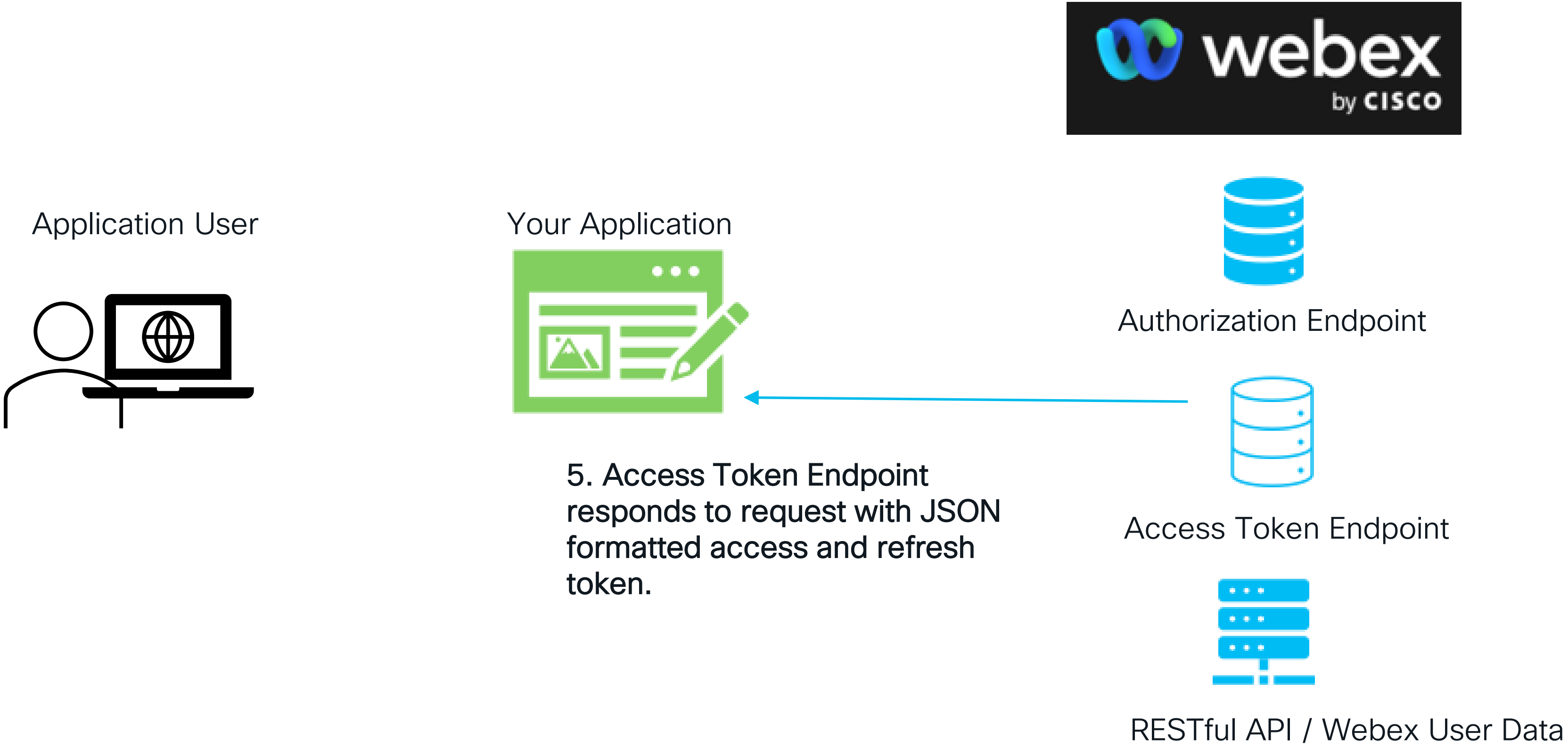
Access Token Endpoint

RESTful API / Webex User Data

4. Application requests access and refresh tokens in exchange for the Client ID, Client Secret, Code, and Redirect URI.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow



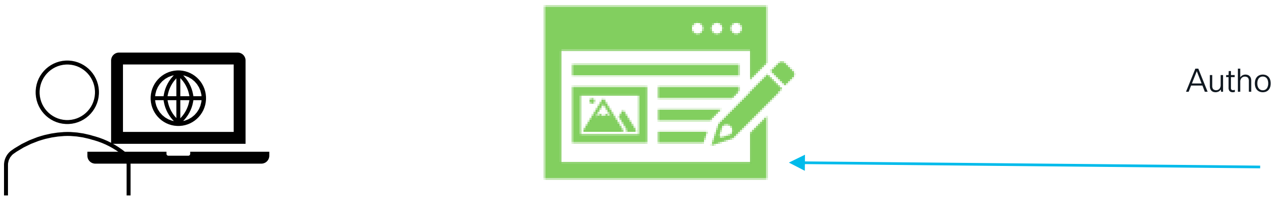
5. Access Token Endpoint responds to request with JSON formatted access and refresh token.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow

Application User

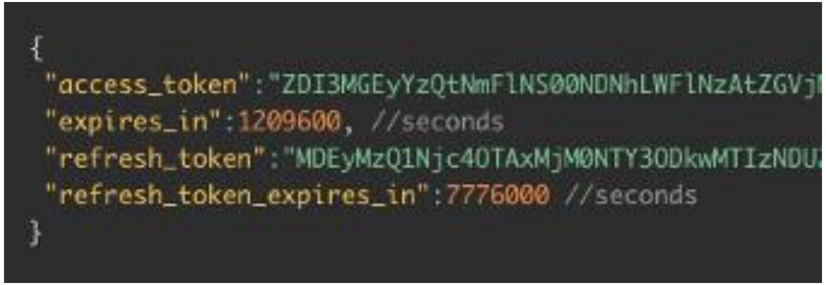
Your Application



Authorization Endpoint

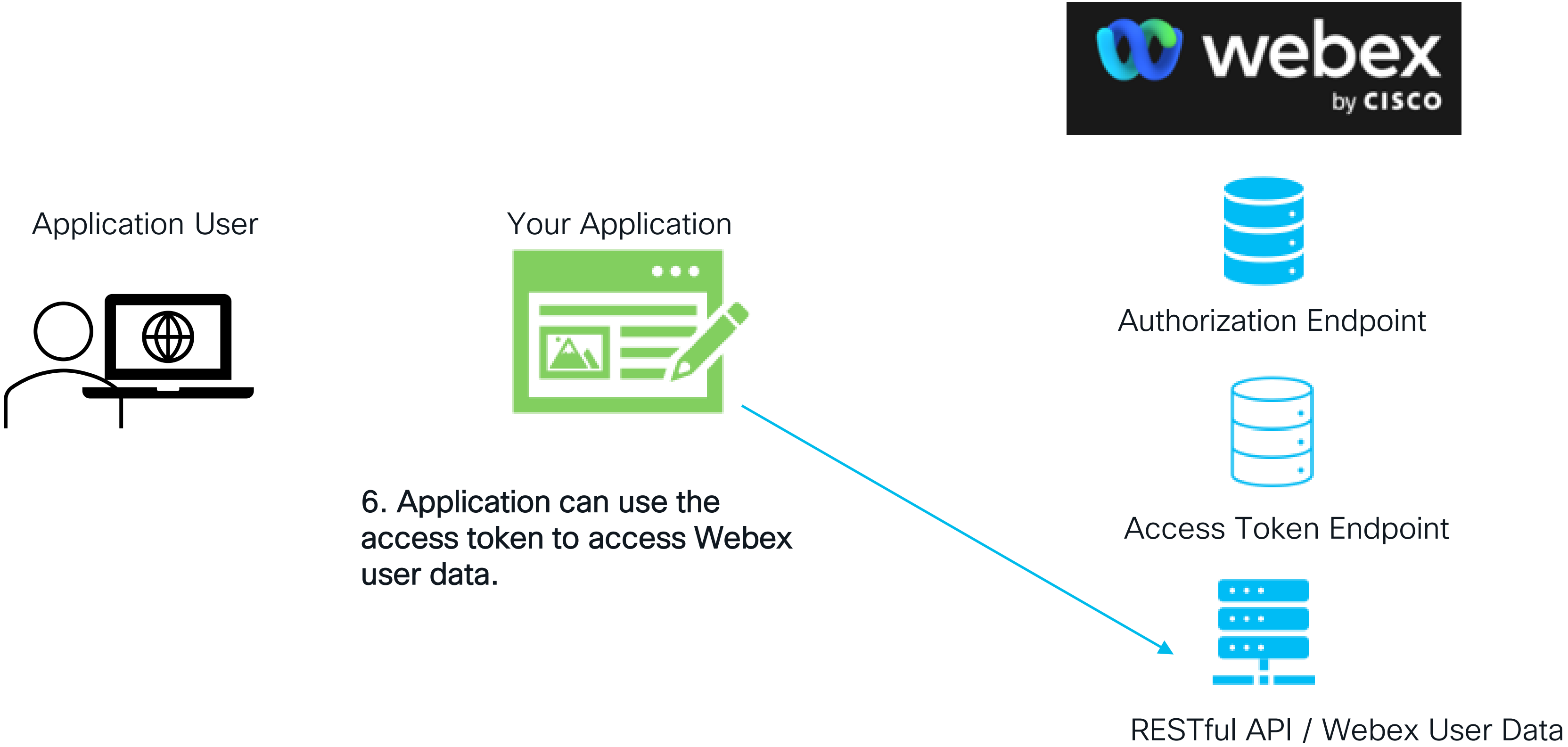
Access Token Endpoint

RESTful API / Webex User Data



```
{
 "access_token":"ZDI3MGEyYzQtNmFlNS00NDNhLWFlNzAtZGVj
 "expires_in":1209600, //seconds
 "refresh_token":"MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU
 "refresh_token_expires_in":7776000 //seconds
}
```

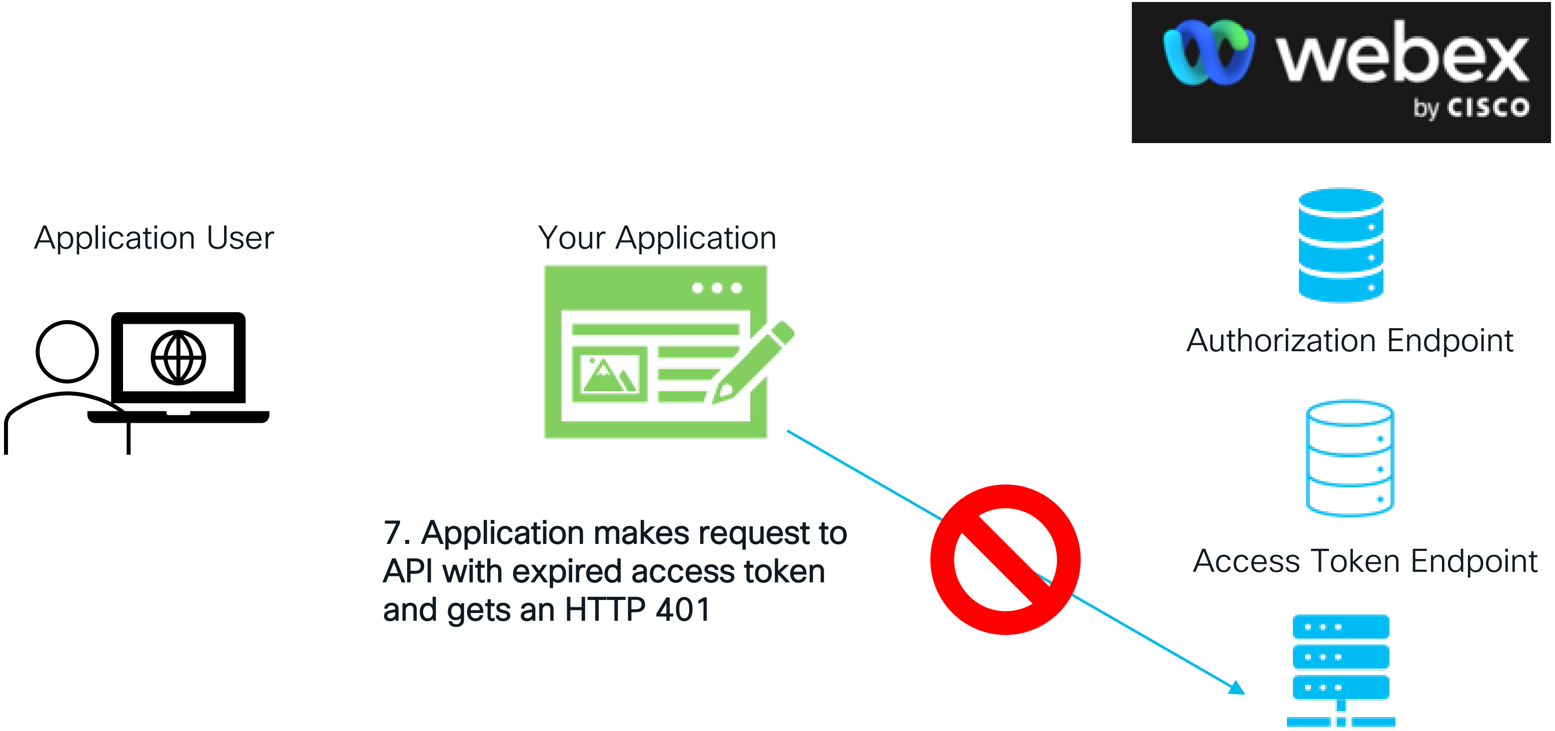
OAuth 2.0 : Authorization Code Flow



6. Application can use the access token to access Webex user data.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow



Application User

Your Application

Authorization Endpoint

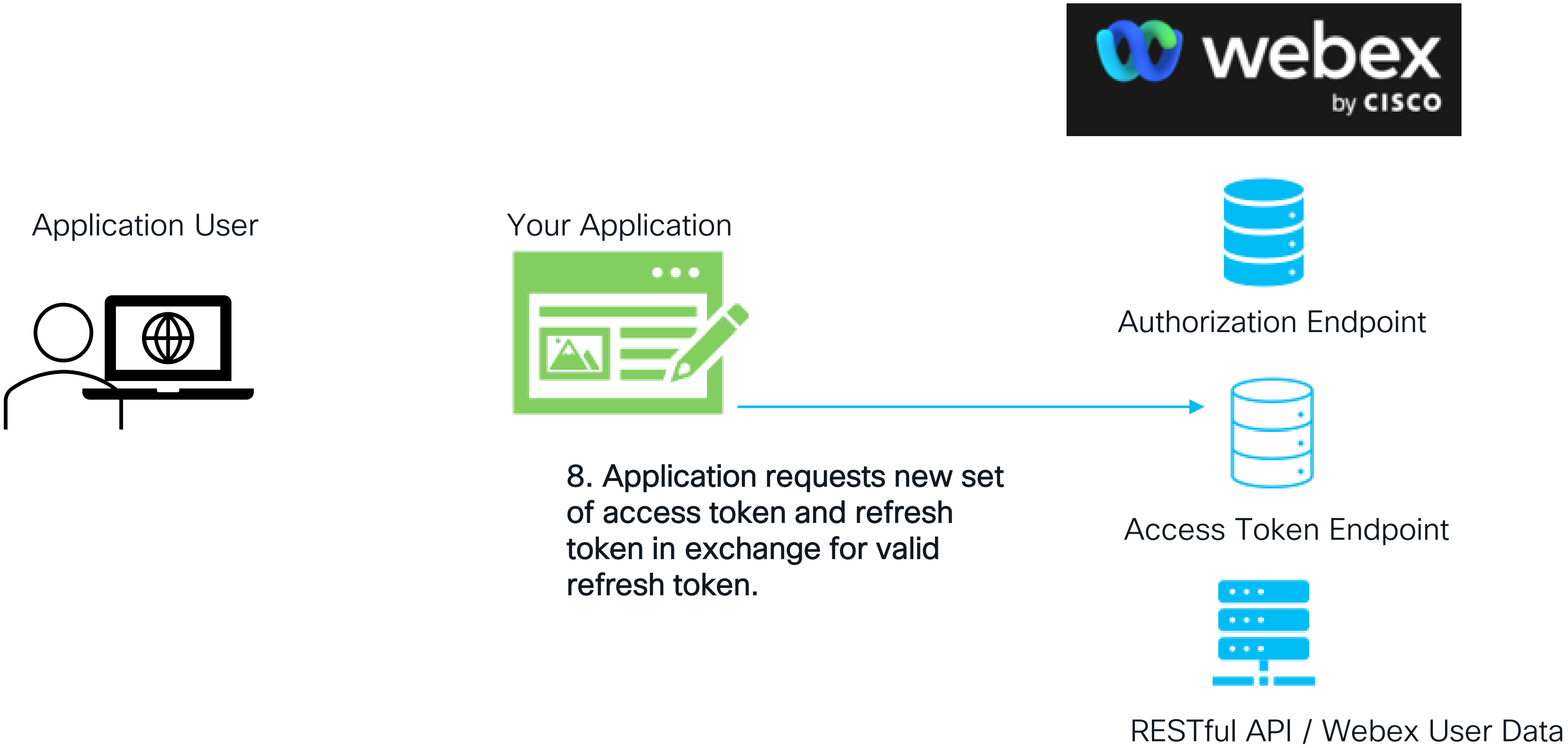
Access Token Endpoint

RESTful API / Webex User Data

7. Application makes request to API with expired access token and gets an HTTP 401

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

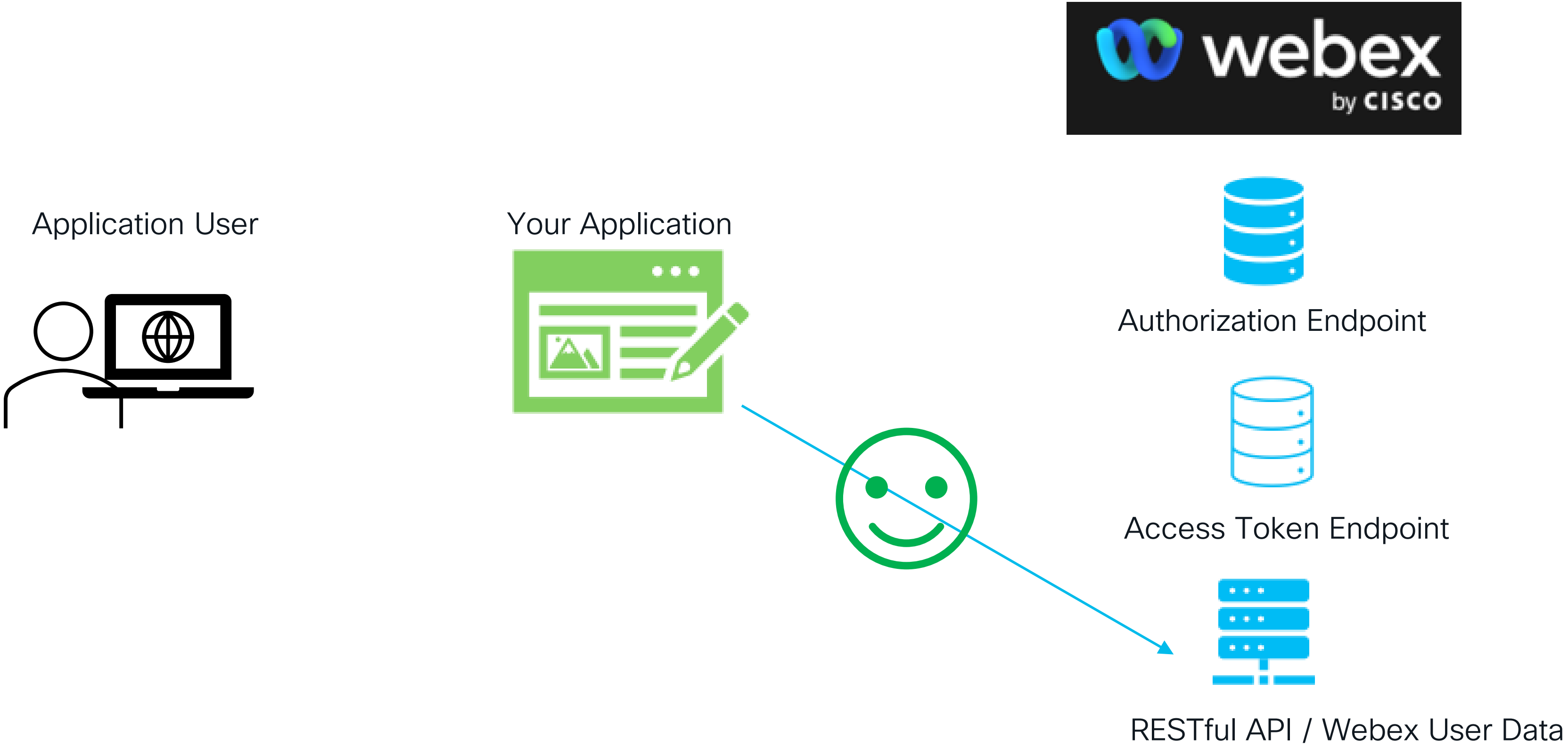
OAuth 2.0 : Getting Refresh Token



8. Application requests new set of access token and refresh token in exchange for valid refresh token.

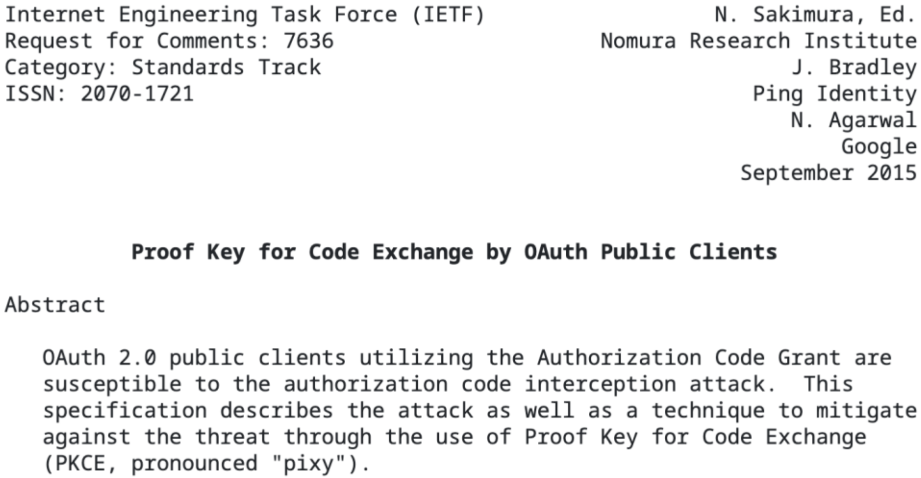
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Using New Access Token



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

PKCE



Internet Engineering Task Force (IETF)
Request for Comments: 7636
Category: Standards Track
ISSN: 2070-1721

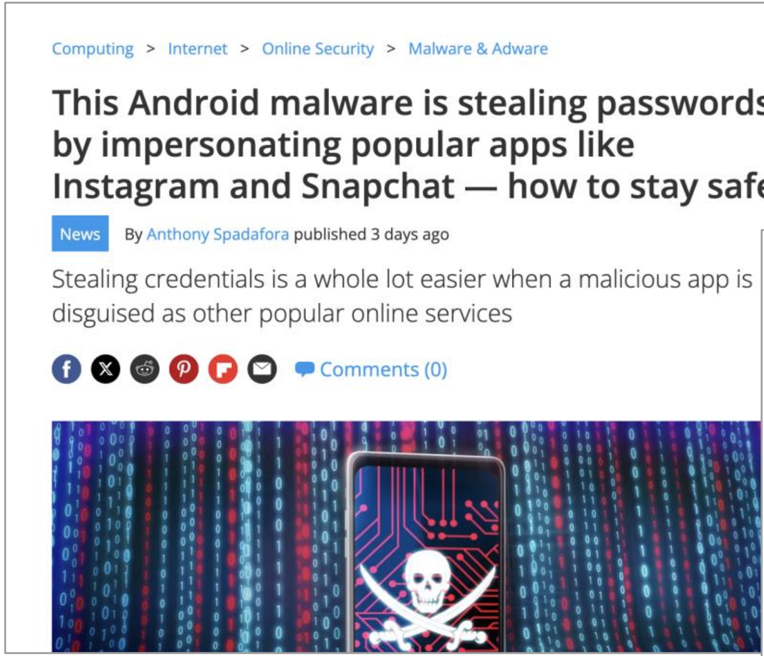
N. Sakimura, Ed.
Nomura Research Institute
J. Bradley
Ping Identity
N. Agarwal
Google
September 2015

Proof Key for Code Exchange by OAuth Public Clients

Abstract

OAuth 2.0 public clients utilizing the Authorization Code Grant are susceptible to the authorization code interception attack. This specification describes the attack as well as a technique to mitigate against the threat through the use of Proof Key for Code Exchange (PKCE, pronounced "pixy").

PKCE



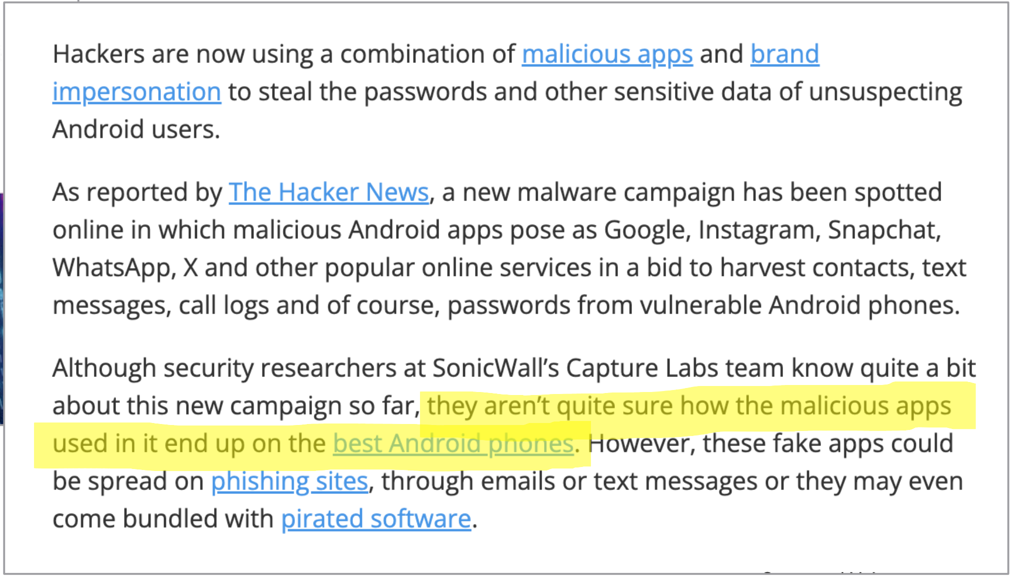
Computing > Internet > Online Security > Malware & Adware

This Android malware is stealing passwords by impersonating popular apps like Instagram and Snapchat — how to stay safe

News By Anthony Spadafora published 3 days ago

Stealing credentials is a whole lot easier when a malicious app is disguised as other popular online services

Comments (0)



Hackers are now using a combination of malicious apps and brand impersonation to steal the passwords and other sensitive data of unsuspecting Android users.

As reported by The Hacker News, a new malware campaign has been spotted online in which malicious Android apps pose as Google, Instagram, Snapchat, WhatsApp, X and other popular online services in a bid to harvest contacts, text messages, call logs and of course, passwords from vulnerable Android phones.

Although security researchers at SonicWall's Capture Labs team know quite a bit about this new campaign so far, they aren't quite sure how the malicious apps used in it end up on the best Android phones. However, these fake apps could be spread on phishing sites, through emails or text messages or they may even come bundled with pirated software.

Authorization Code Flow with PKCE

- Your App creates and records a secret called a "Code Verifier"
- Your App derives a transformed version of the Code Verifier called a "Code Challenge"
- The Code Challenge and transformation method is sent in Authorization request

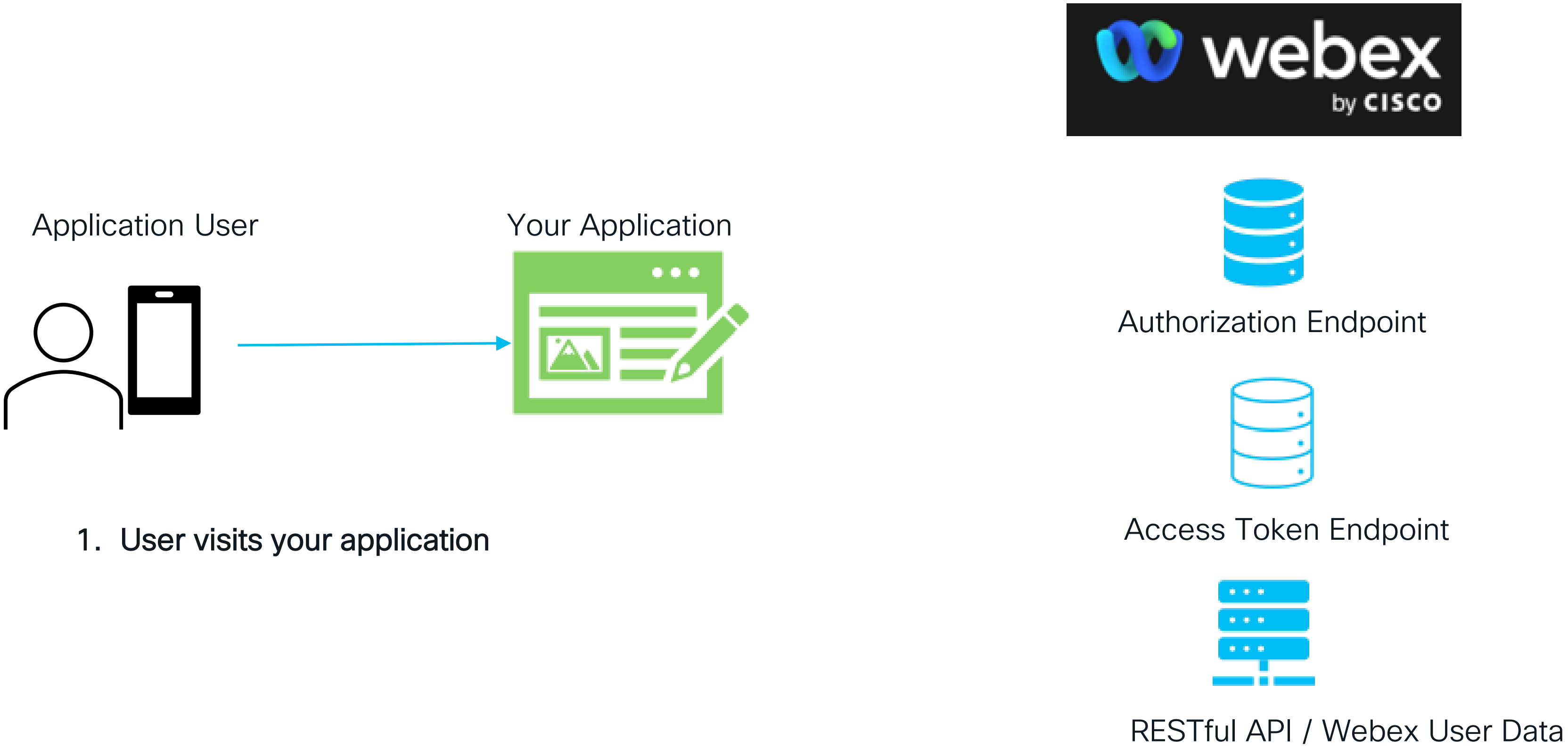
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Authorization Code Flow with PKCE

- The Authorization endpoint responds as usual, but makes note of the code challenge and transformation method
- Your App sends the Access Token request as usual with code, but also sends the Code Verifier.
- The Authorization server decodes the Code Challenge. Access token server responds on match with tokens.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow w/ PKCE



Application User

Your Application

Authorization Endpoint

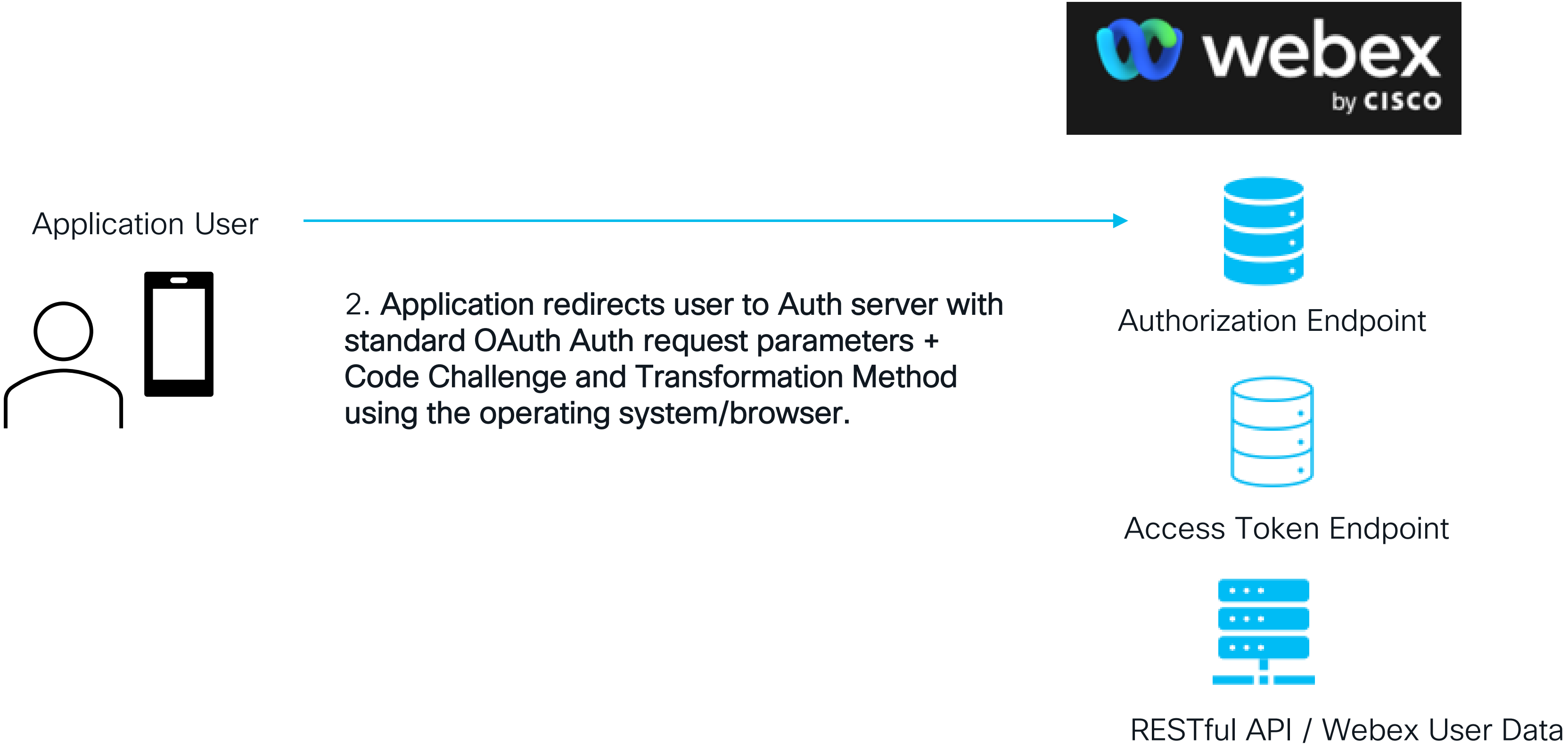
Access Token Endpoint

RESTful API / Webex User Data

1. User visits your application

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow w/ PKCE



Application User

2. Application redirects user to Auth server with standard OAuth Auth request parameters + Code Challenge and Transformation Method using the operating system/browser.

Authorization Endpoint

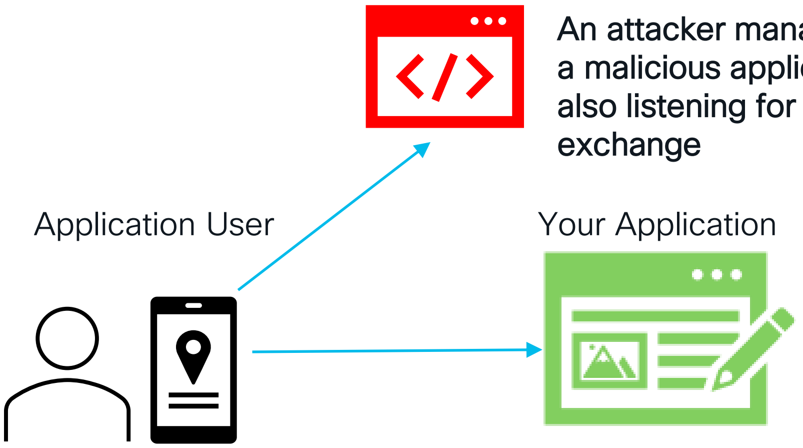
Access Token Endpoint

RESTful API / Webex User Data

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow w/ PKCE

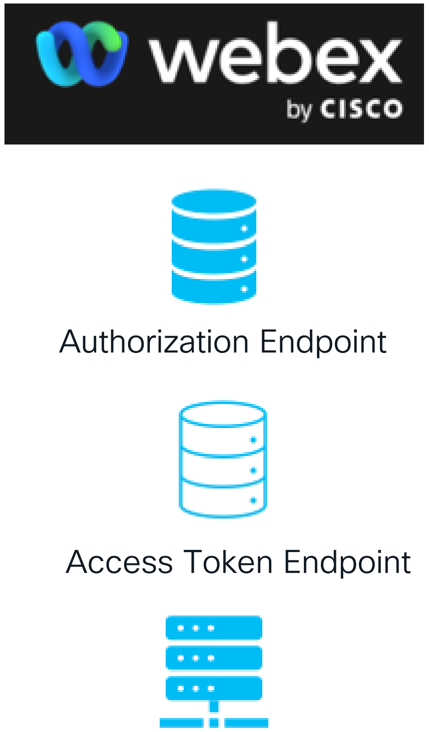
Malicious Application



An attacker manages to register a malicious application that is also listening for this code exchange

Application User

Your Application



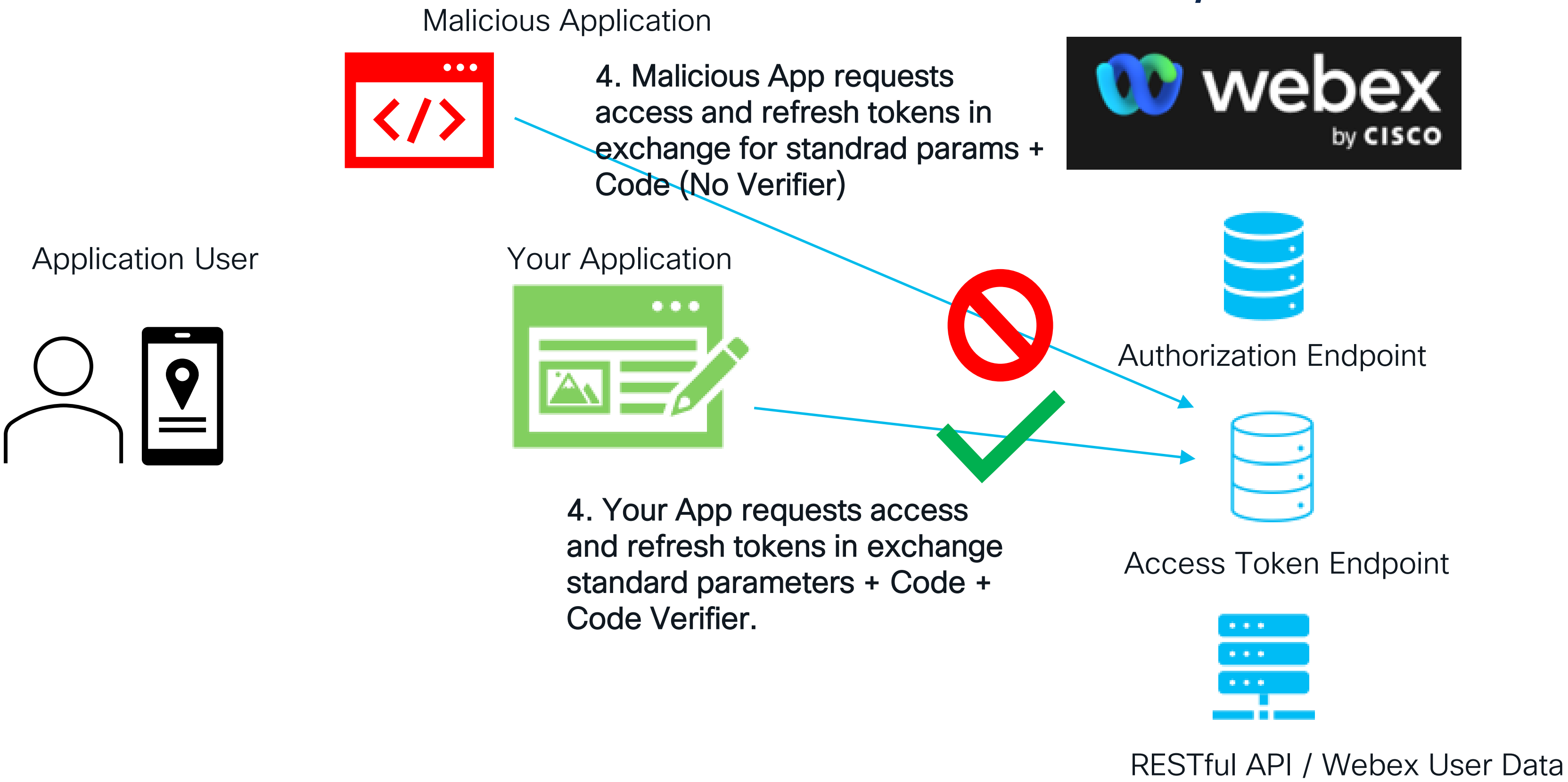
Authorization Endpoint

Access Token Endpoint

RESTful API / Webex User Data

3. Auth Server redirect user to the Redirect URI with "code" in the request parameter.

OAuth 2.0 : Authorization Code Flow w/ PKCE



Malicious Application

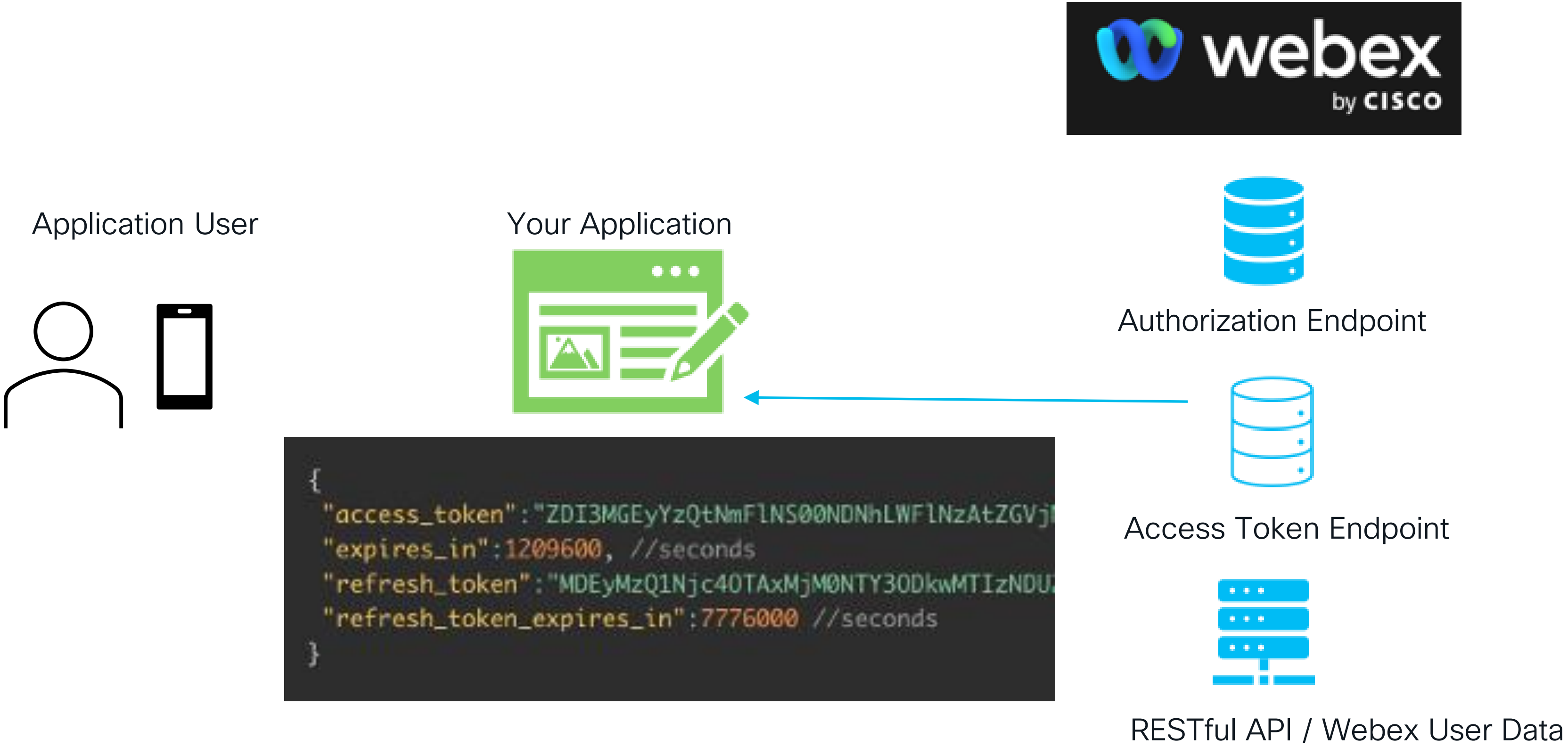
4. Malicious App requests access and refresh tokens in exchange for standrad params + Code (No Verifier)

Application User

Your Application

4. Your App requests access and refresh tokens in exchange standard parameters + Code + Code Verifier.

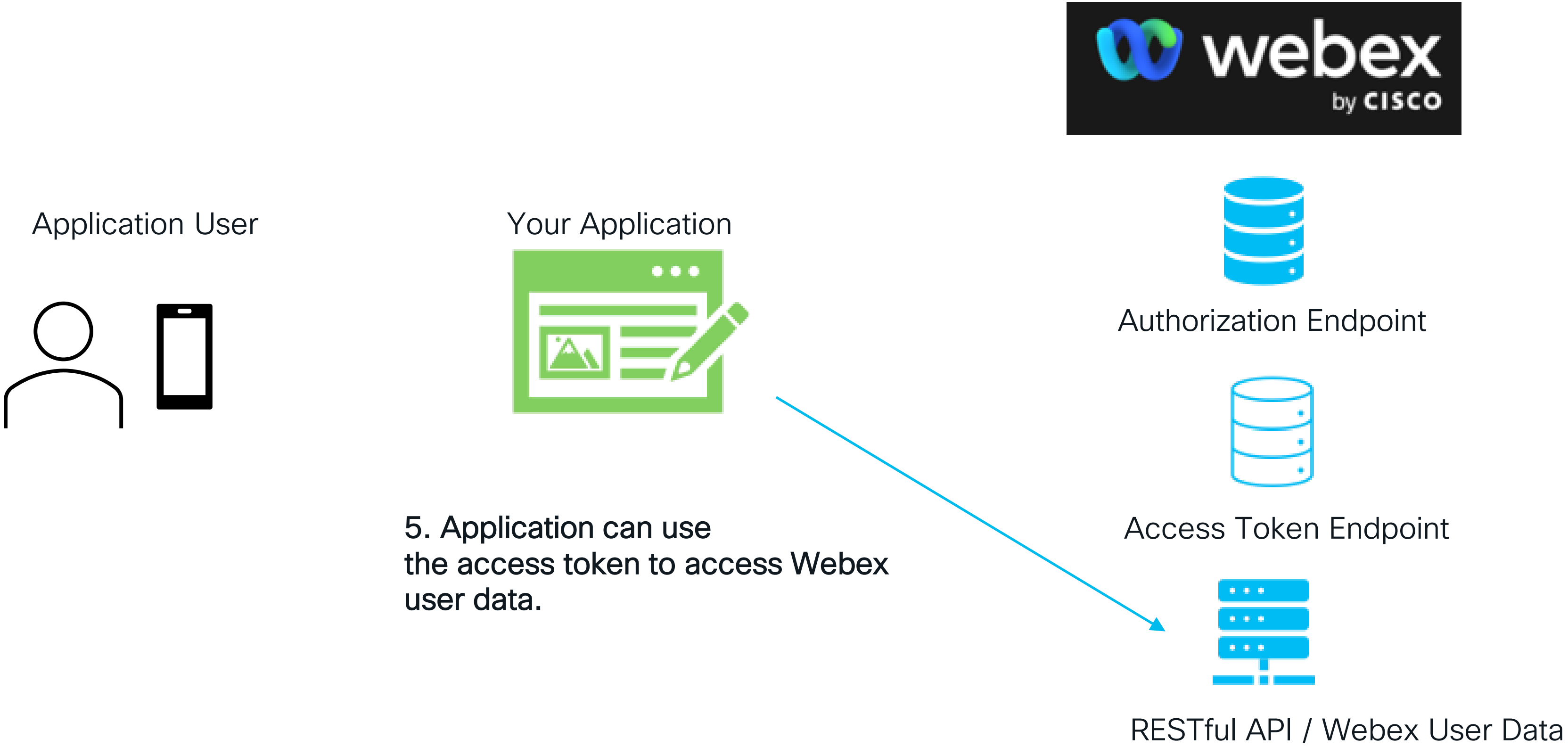
OAuth 2.0 : Authorization Code Flow w/ PKCE



```
{
  "access_token":"ZDI3MGEyYzQtNmFlNS00NDNhLWFlNzAtZGVj
  "expires_in":1209600, //seconds
  "refresh_token":"MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU
  "refresh_token_expires_in":7776000 //seconds
}
```

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

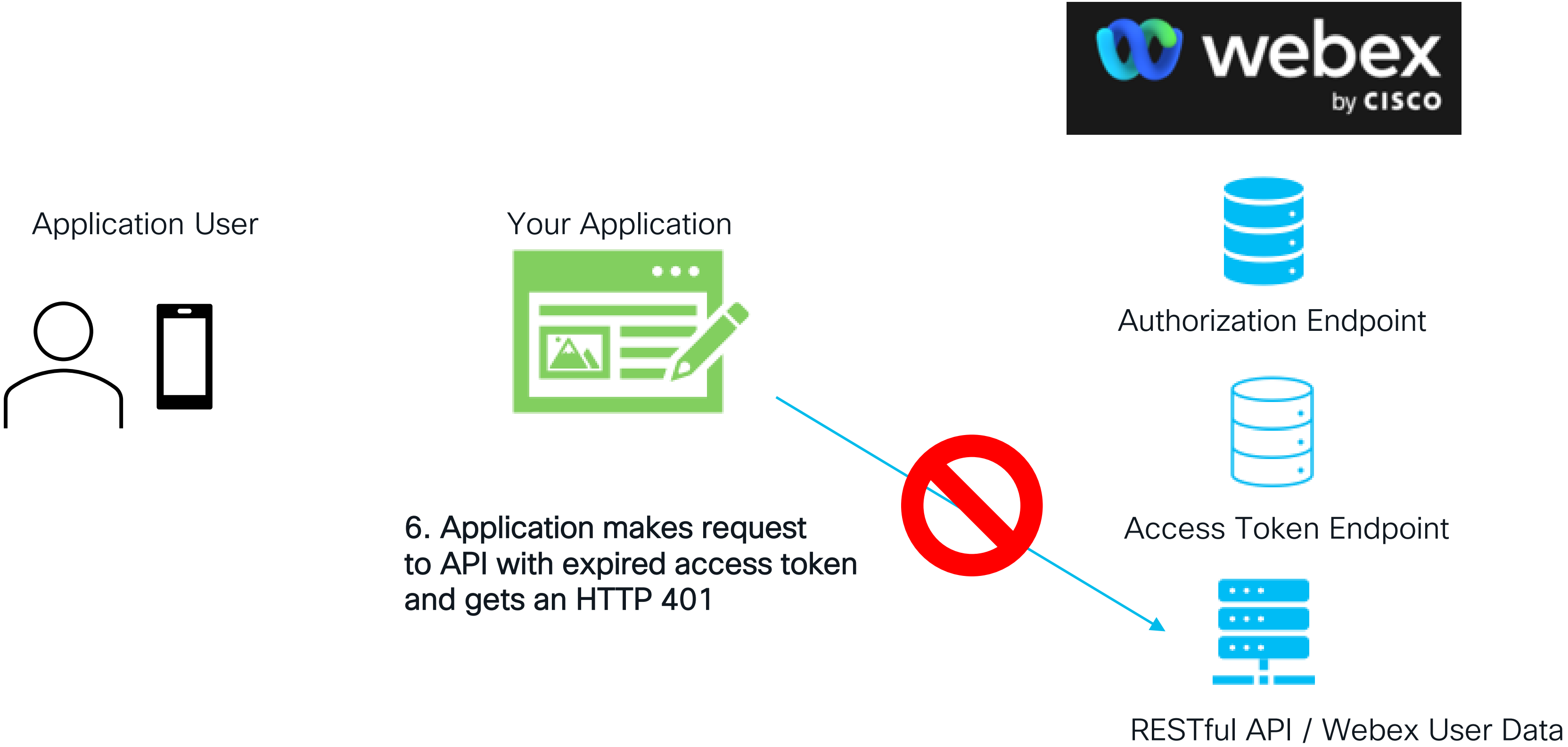
OAuth 2.0 : Authorization Code Flow w/ PKCE



5. Application can use the access token to access Webex user data.

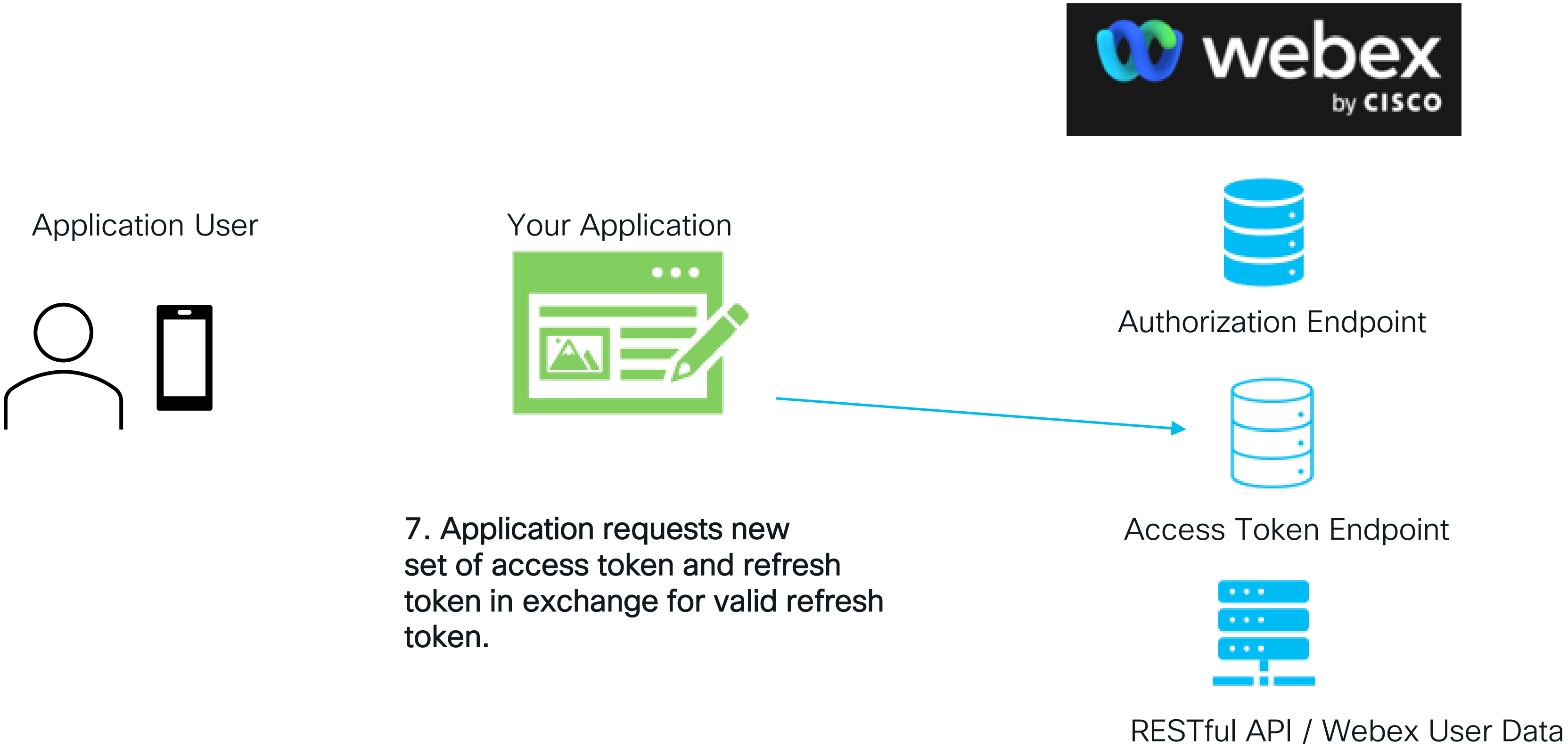
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow w/ PKCE



6. Application makes request to API with expired access token and gets an HTTP 401

OAuth 2.0 : Authorization Code Flow w/ PKCE



Application User

Your Application

Authorization Endpoint

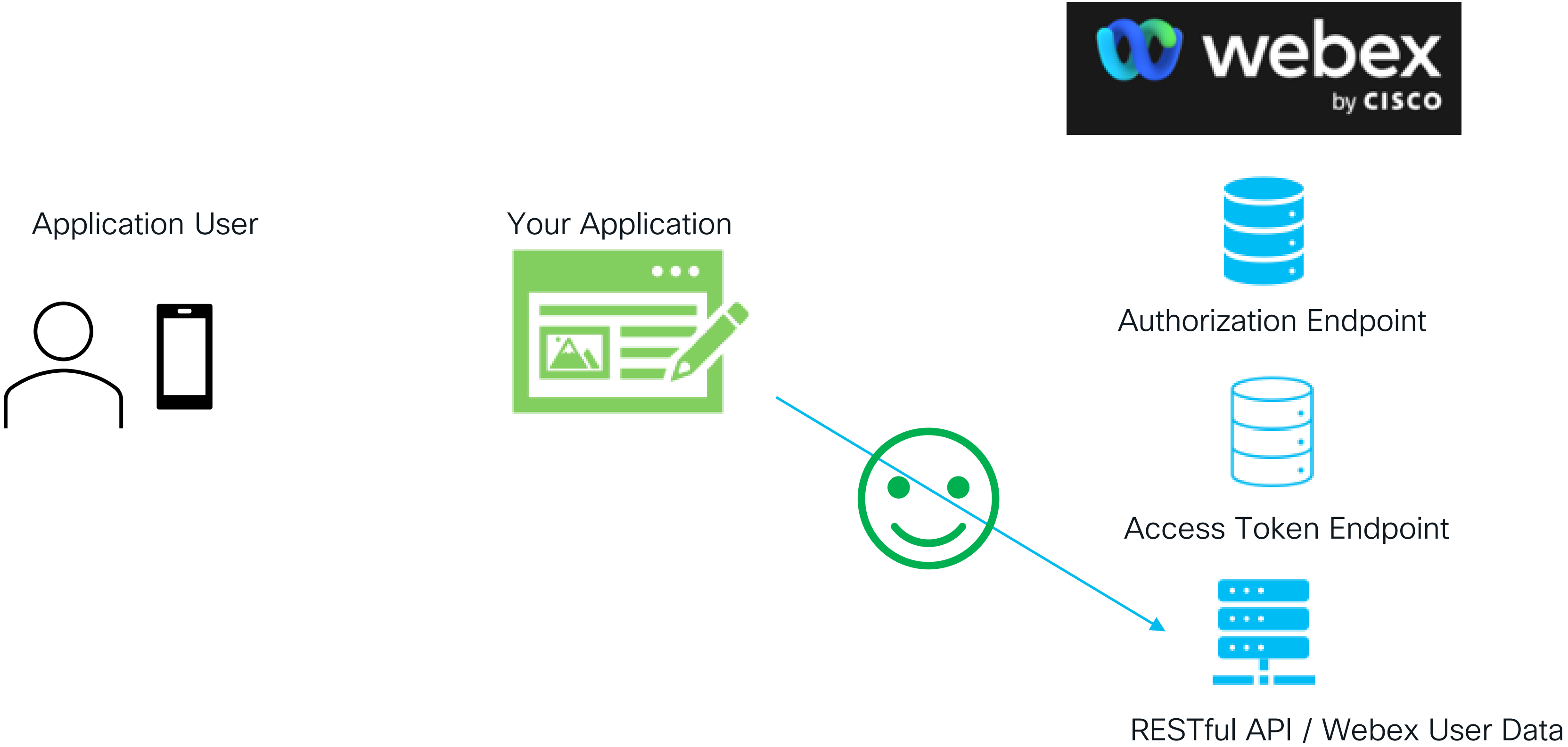
Access Token Endpoint

RESTful API / Webex User Data

7. Application requests new set of access token and refresh token in exchange for valid refresh token.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Authorization Code Flow w/ PKCE



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

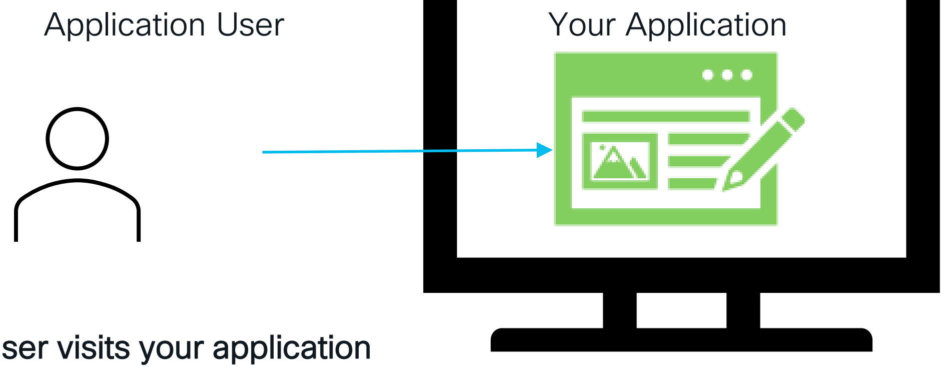
Device Grant Flow

- Request user authorization on devices that have limited input capabilities.
- The app requests "User Code" and "Device Code" from The Device Authorization endpoint.
- User can use QR Code or input User Code on separate Device.

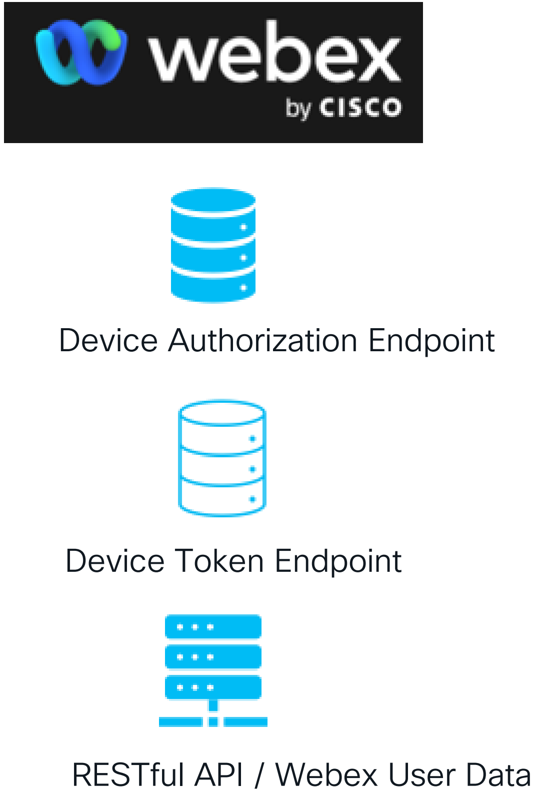
cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Device Grant Flow

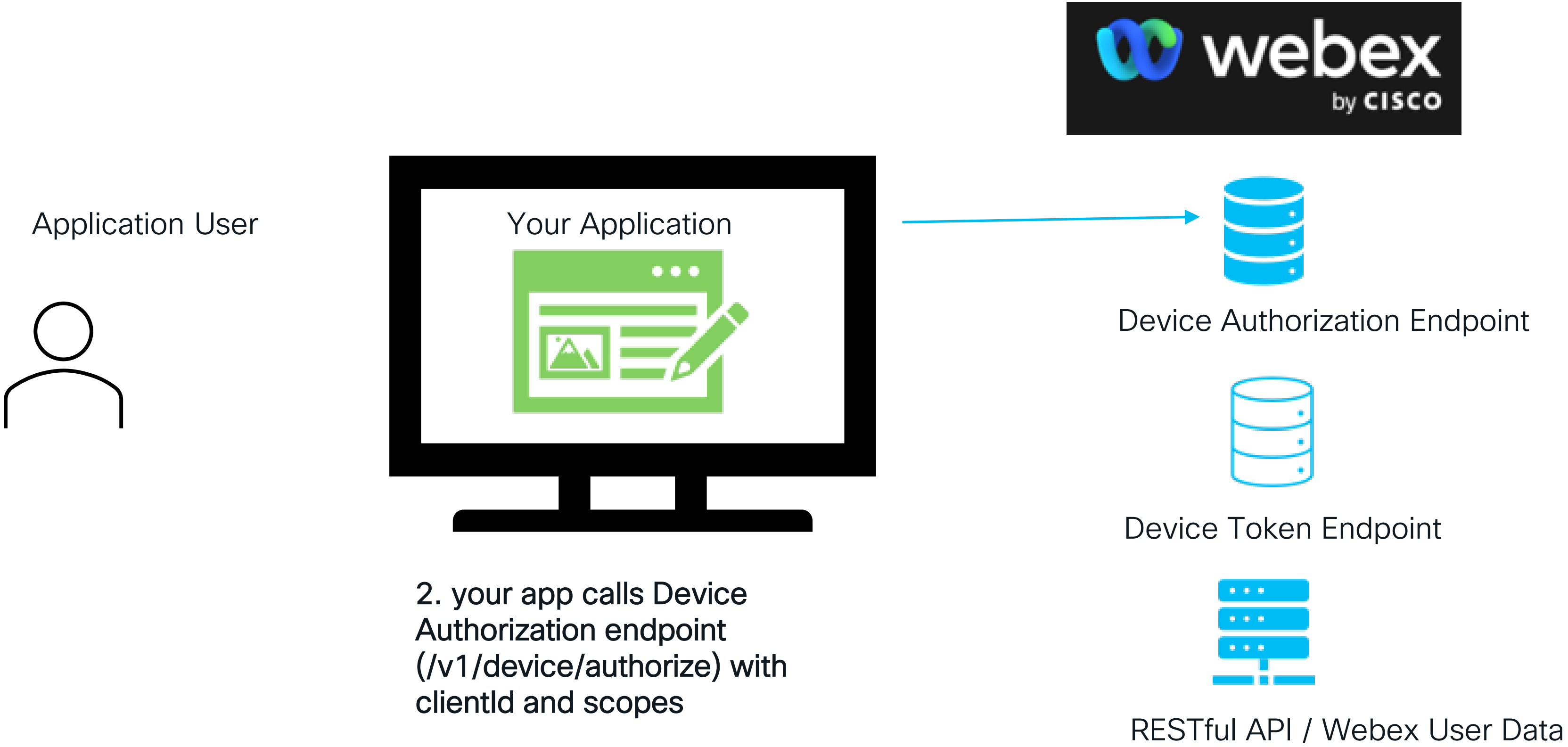


1. User visits your application



© 2024 Cisco and/or its affiliates. All rights reserved.

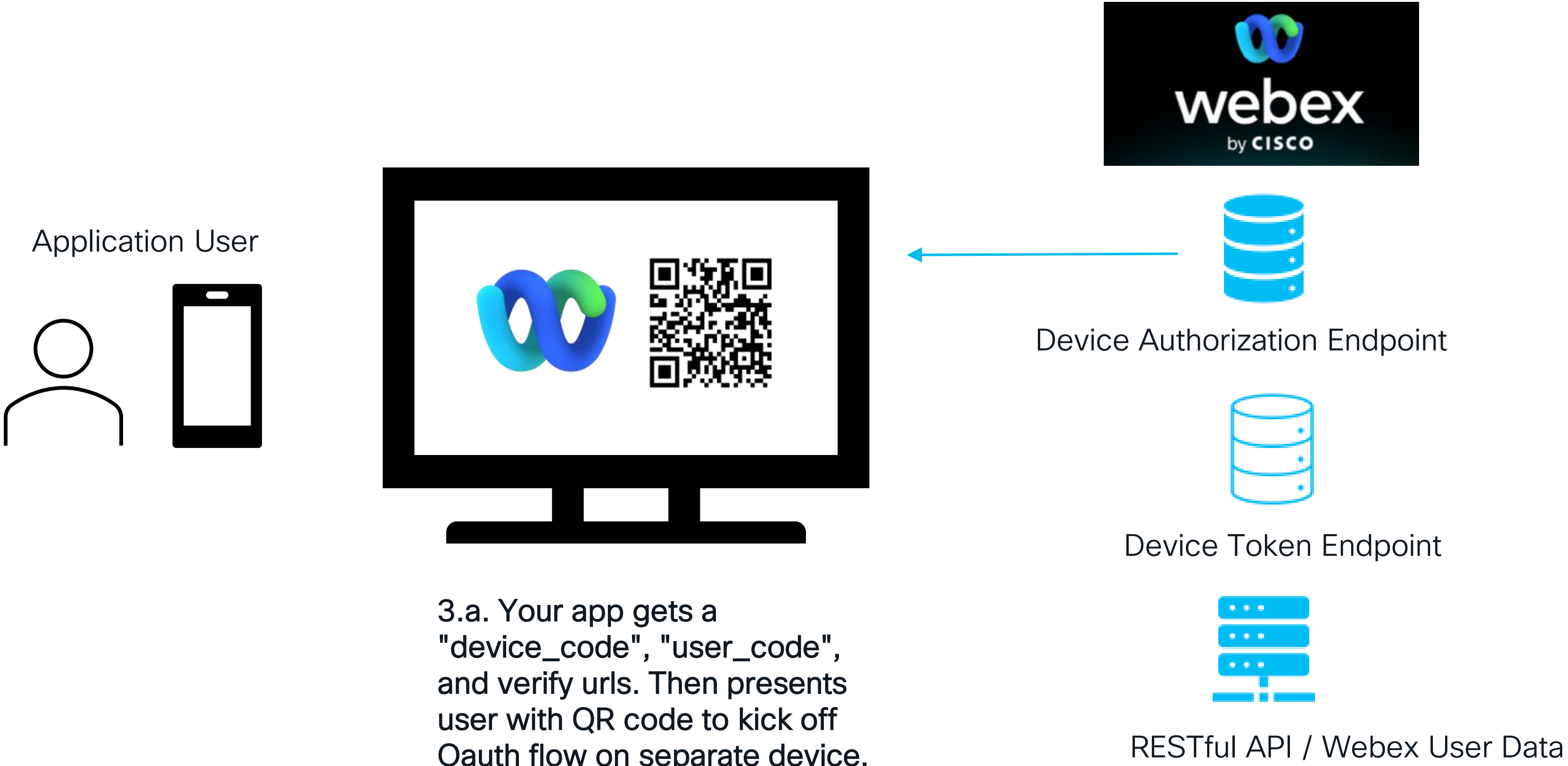
OAuth 2.0 : Device Grant Flow



2. your app calls Device Authorization endpoint (/v1/device/authorize) with clientId and scopes

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Device Grant Flow



Application User

Device Authorization Endpoint

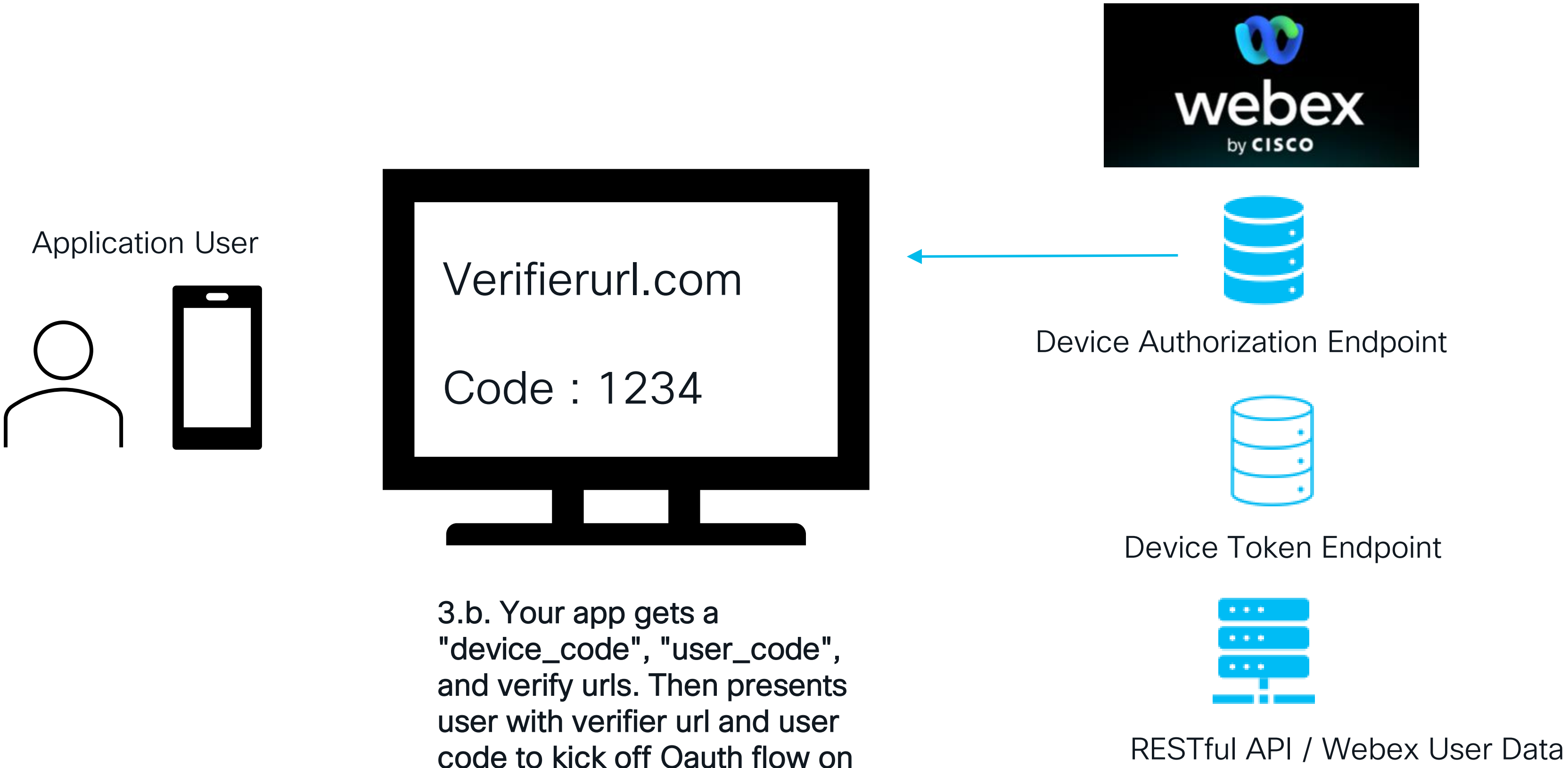
Device Token Endpoint

RESTful API / Webex User Data

3.a. Your app gets a "device_code", "user_code", and verify urls. Then presents user with QR code to kick off Oauth flow on separate device.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Device Grant Flow



Application User

Verifierurl.com

Code : 1234

Device Authorization Endpoint

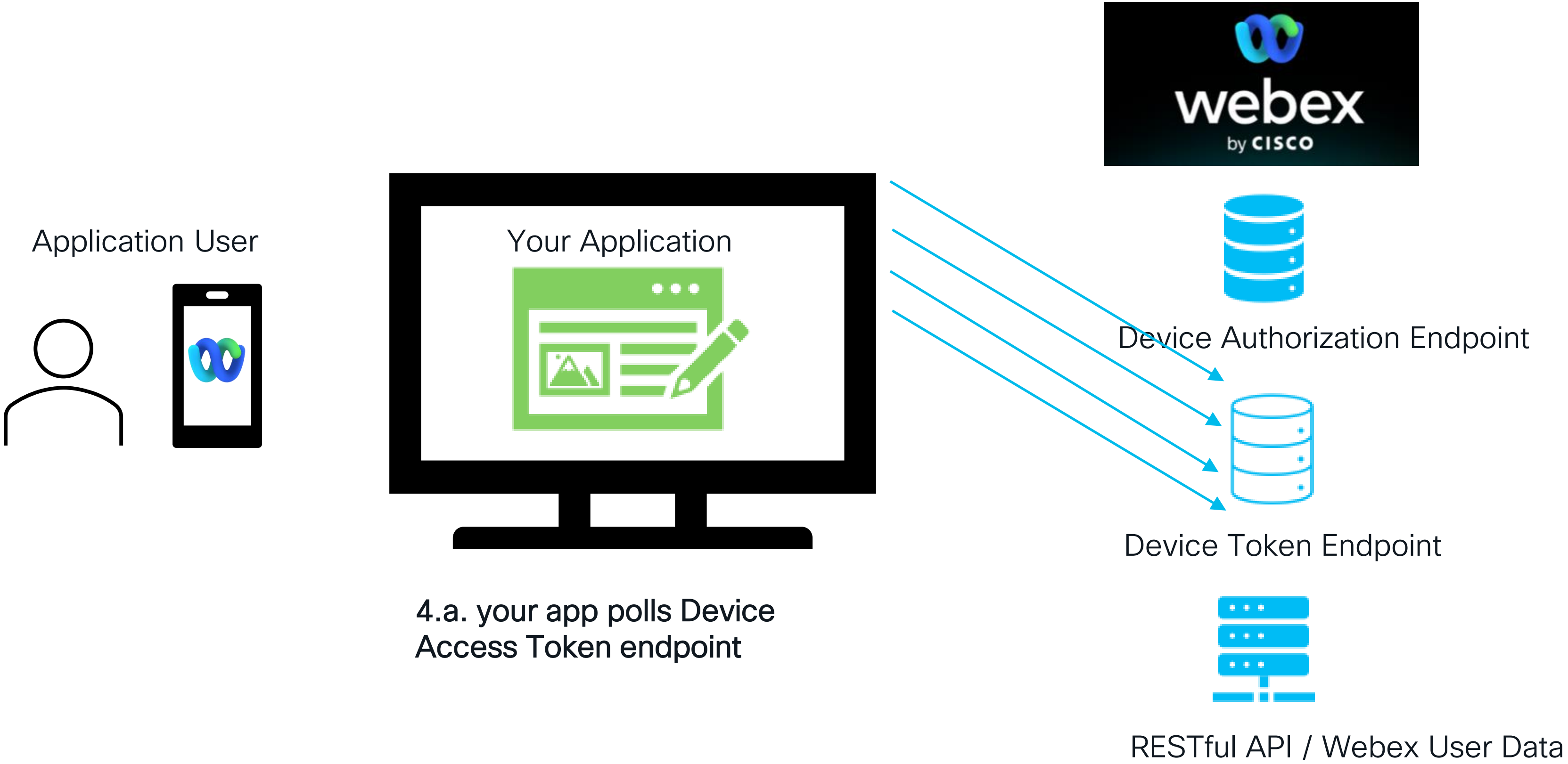
Device Token Endpoint

RESTful API / Webex User Data

3.b. Your app gets a "device_code", "user_code", and verify urls. Then presents user with verifier url and user code to kick off Oauth flow on separate device.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

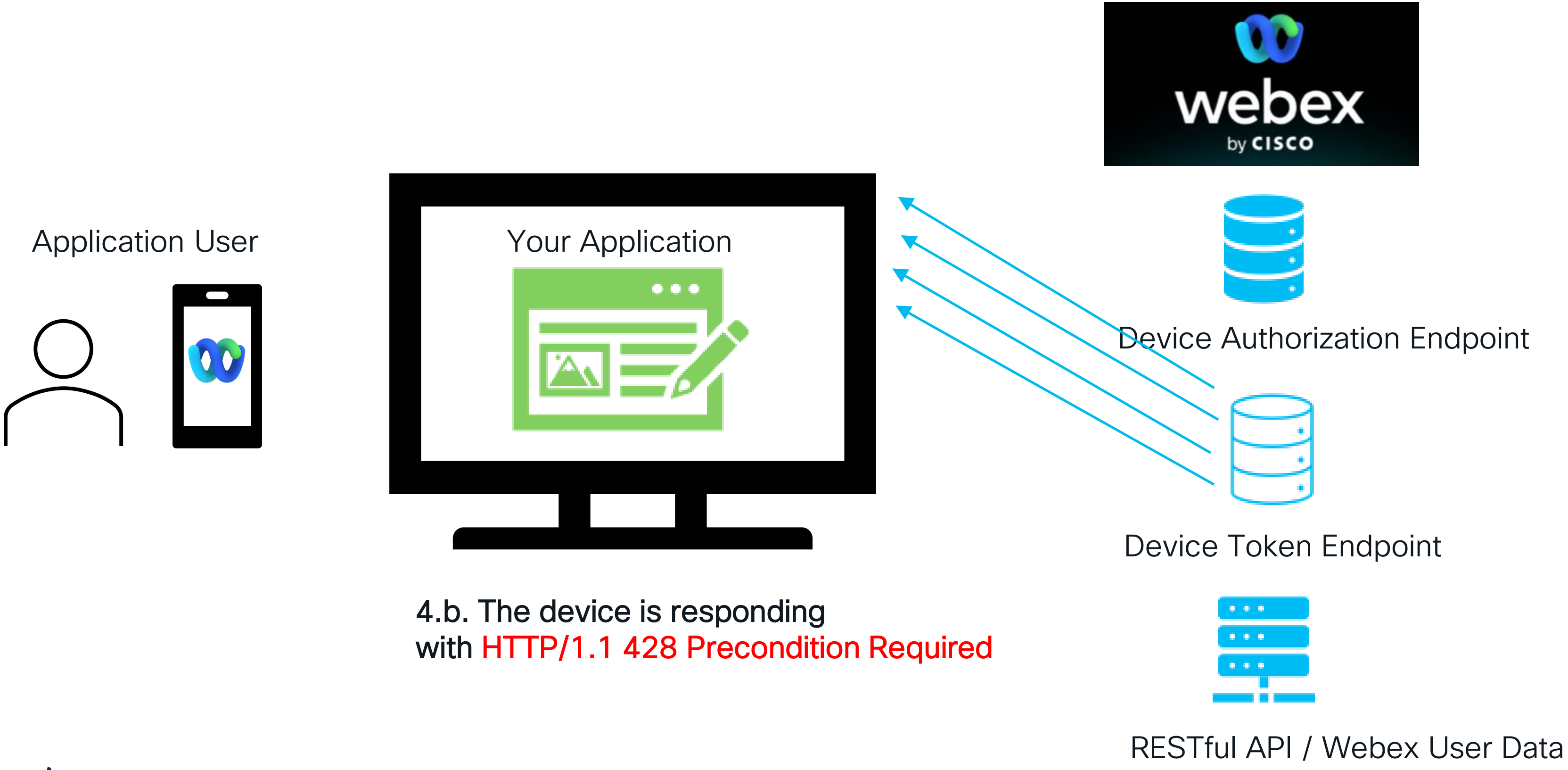
OAuth 2.0 : Device Grant Flow



4.a. your app polls Device Access Token endpoint

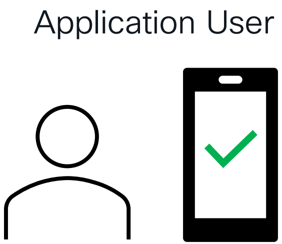
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

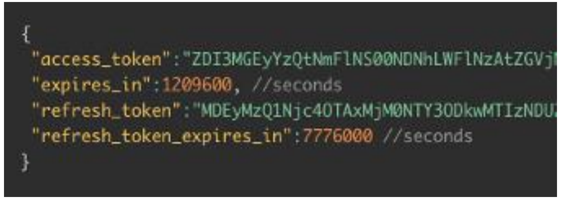
OAuth 2.0 : Device Grant Flow



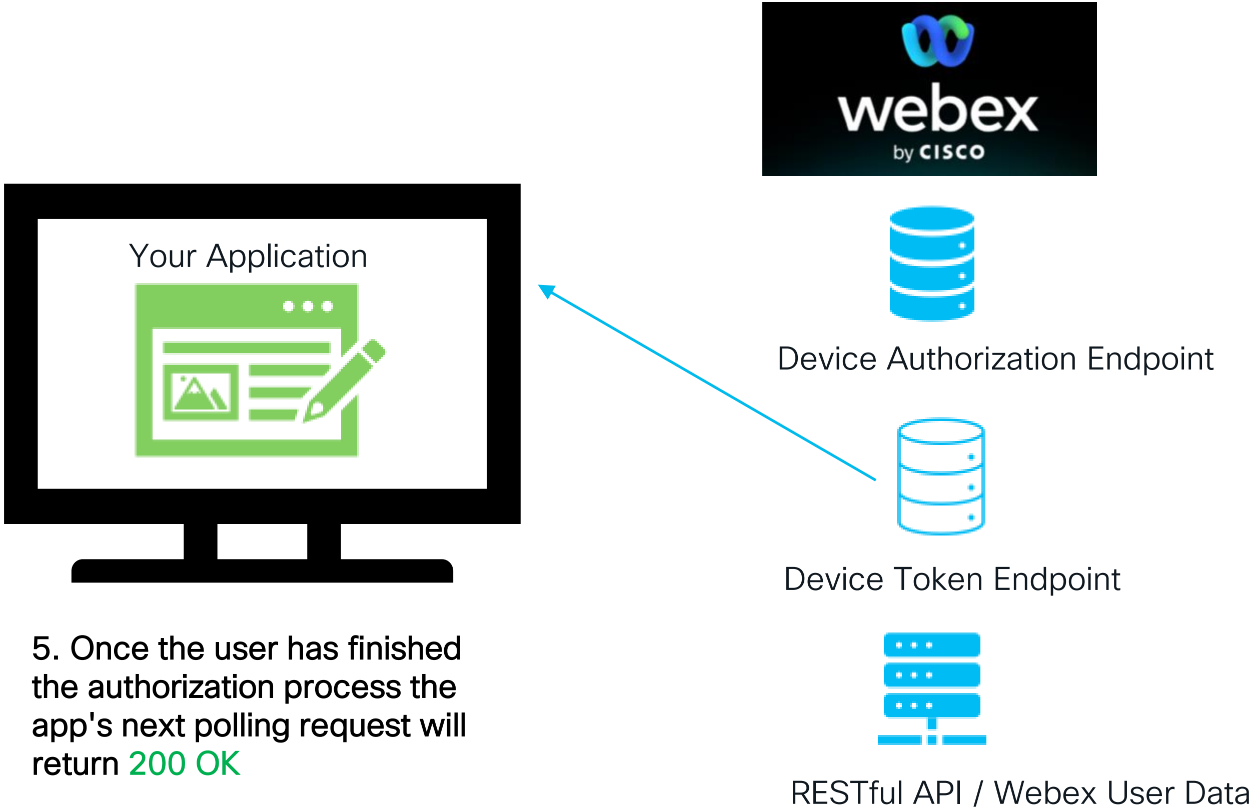
4.b. The device is responding
with HTTP/1.1 428 Precondition Required

OAuth 2.0 : Device Grant Flow





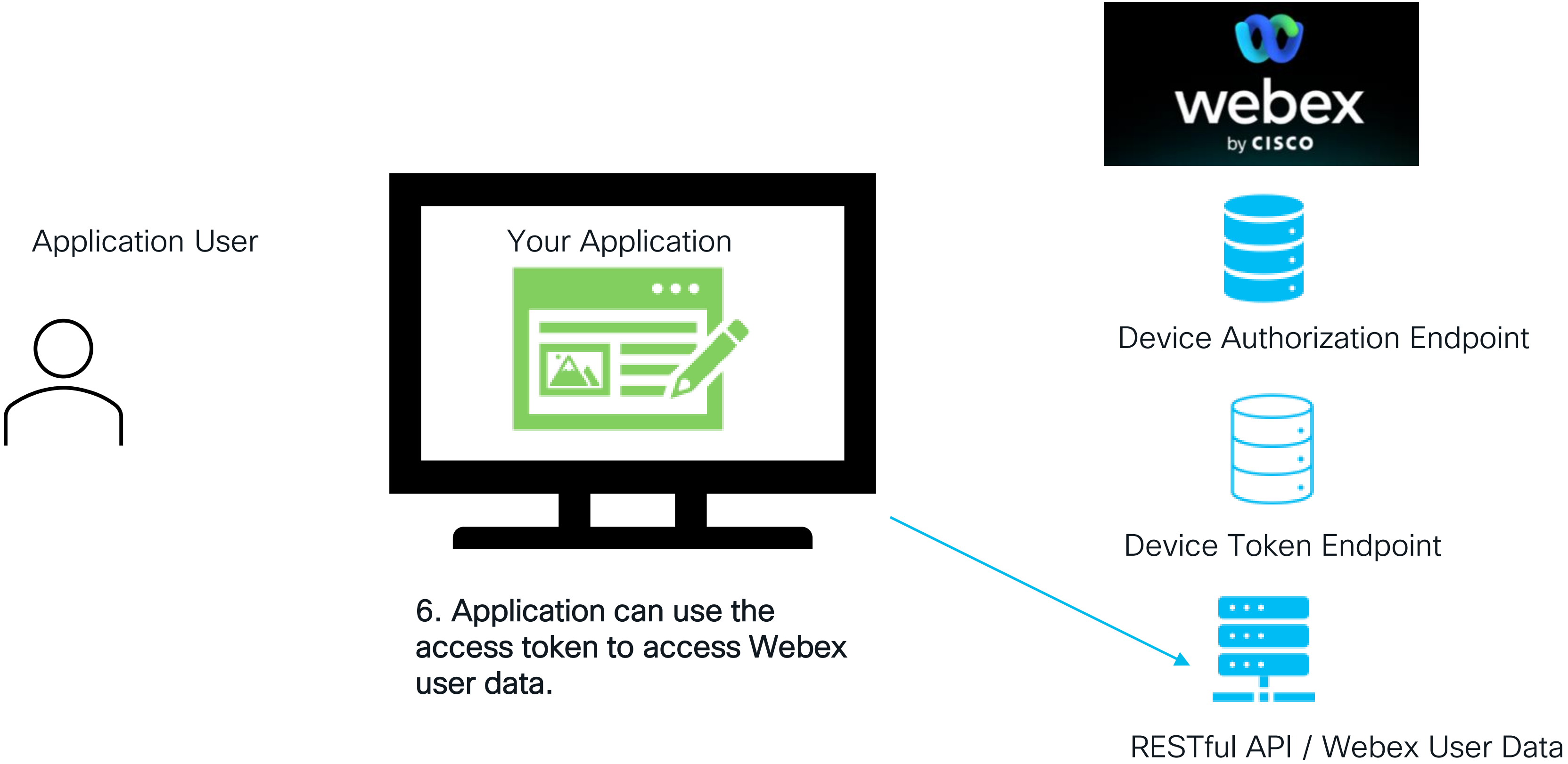
```
{
 "access_token":"ZDI3MGEyYzQtNmFlNS00NDNhLWFlNzAtZGVj
 "expires_in":1209600, //seconds
 "refresh_token":"MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU
 "refresh_token_expires_in":7776000 //seconds
}
```



5. Once the user has finished the authorization process the app's next polling request will return 200 OK

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

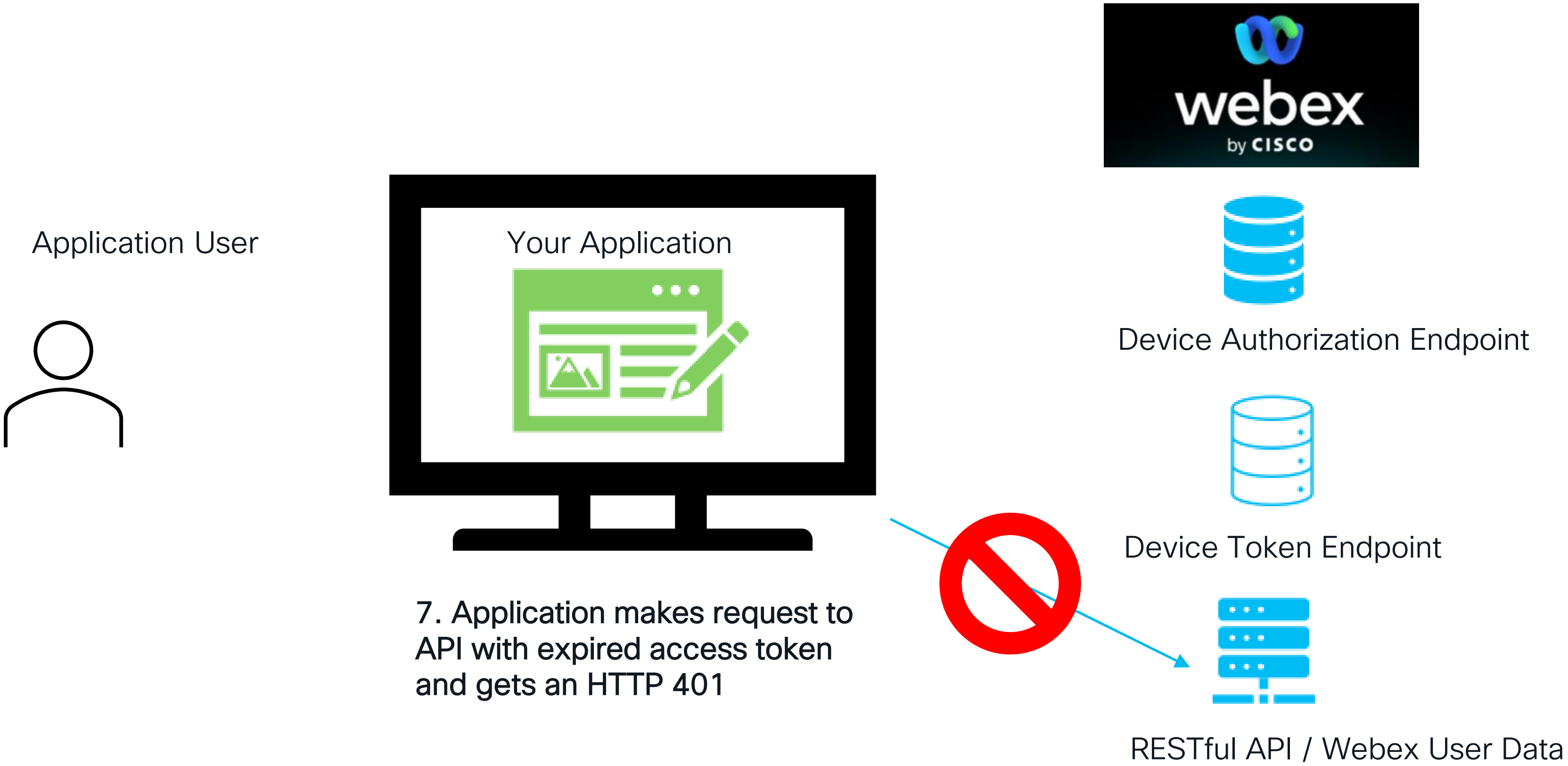
OAuth 2.0 : Device Grant Flow



6. Application can use the access token to access Webex user data.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Device Grant Flow



Application User

Your Application

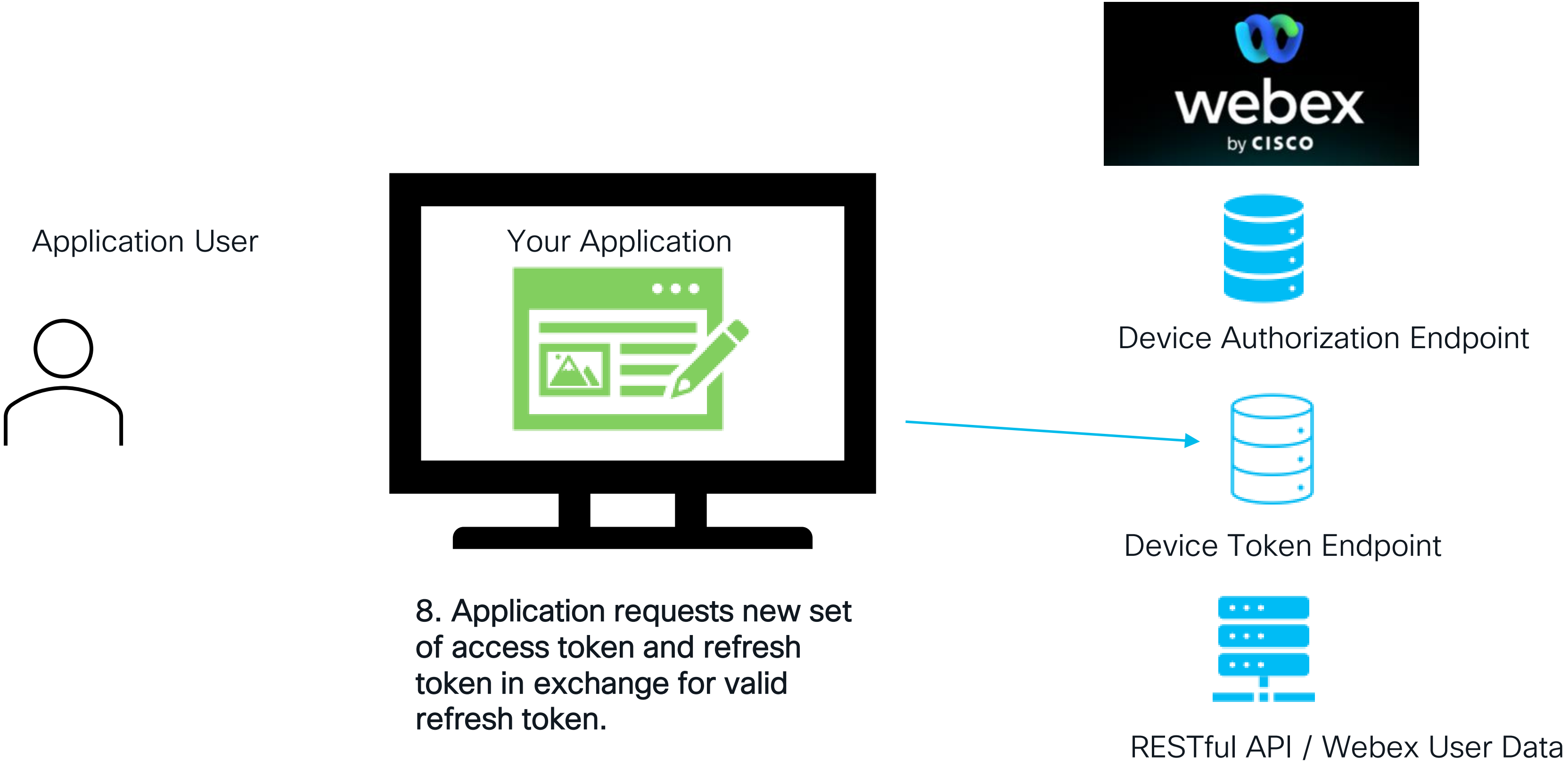
Device Authorization Endpoint

Device Token Endpoint

RESTful API / Webex User Data

7. Application makes request to API with expired access token and gets an HTTP 401

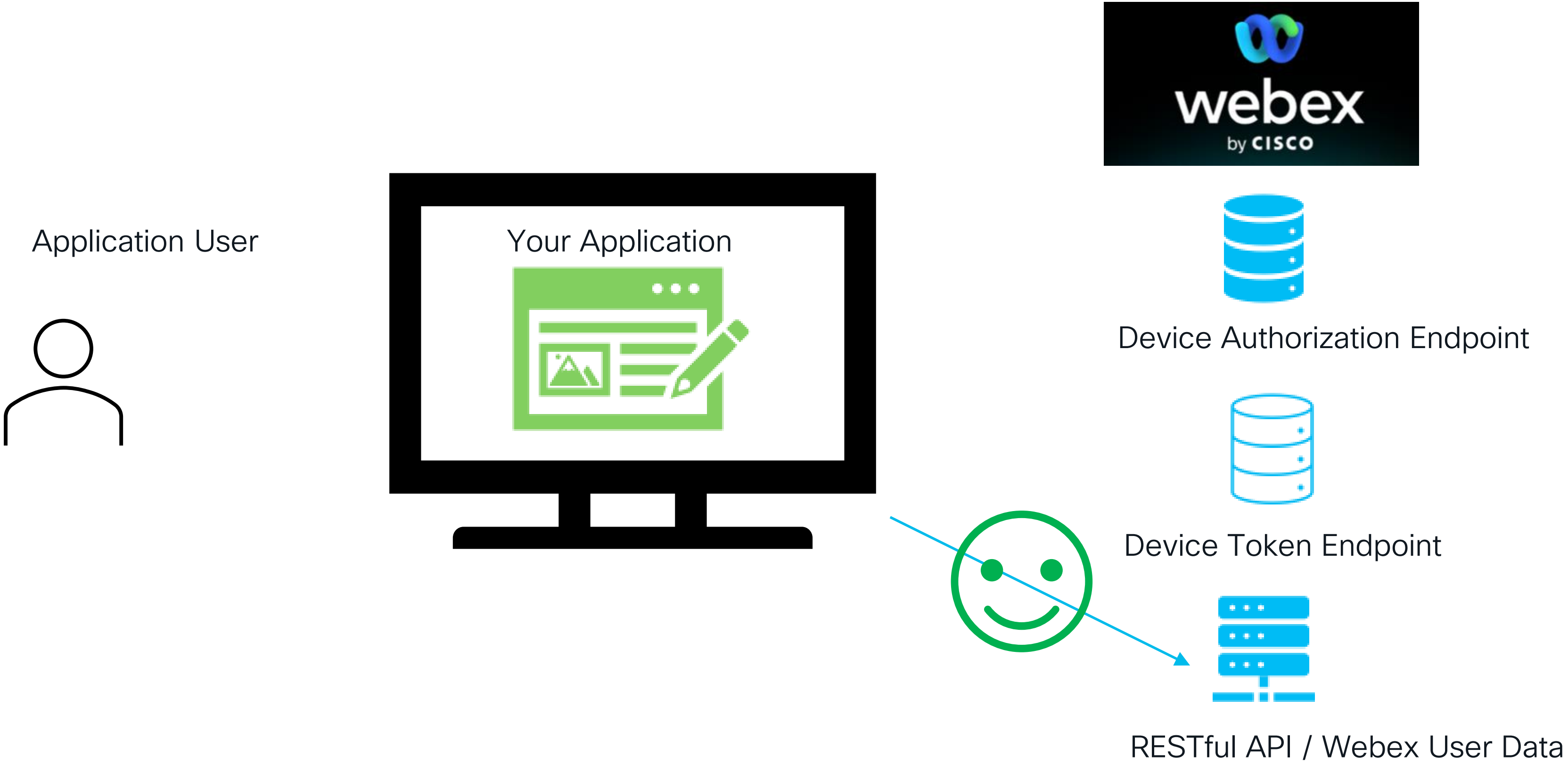
OAuth 2.0 : Device Grant Flow



8. Application requests new set of access token and refresh token in exchange for valid refresh token.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

OAuth 2.0 : Device Grant Flow

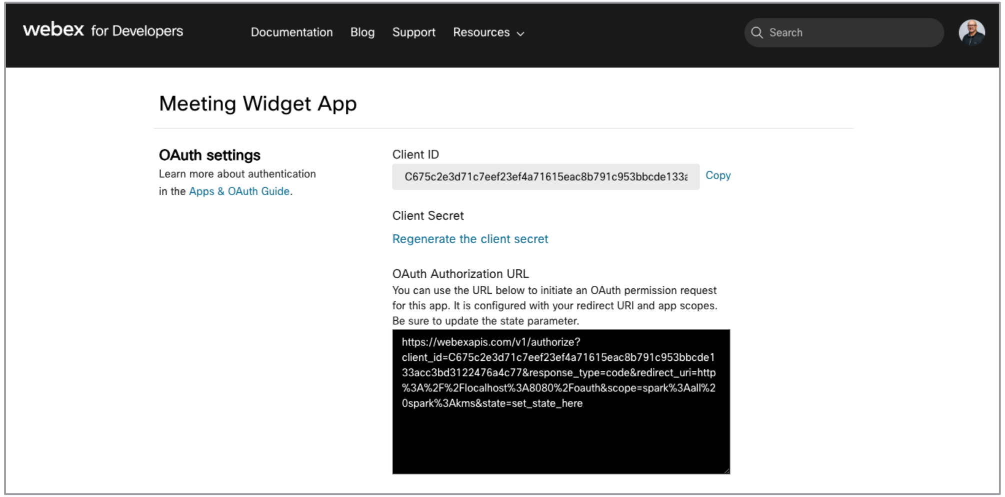


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex
and OAuth 2.0

Webex Integrations

- Developers register an integration on Webex Developer Portal
- Developer selects scopes
- Tools for developing OAuth flow are provided
- Developers can use documentation and sample code.
- Webex users grant apps access to personal Webex Data



Meeting Widget App

OAuth settings
Learn more about authentication in the Apps & OAuth Guide.

Client ID
C675c2e3d71c7eef23ef4a71615eac8b791c953bbcde133a
Copy

Client Secret
Regenerate the client secret

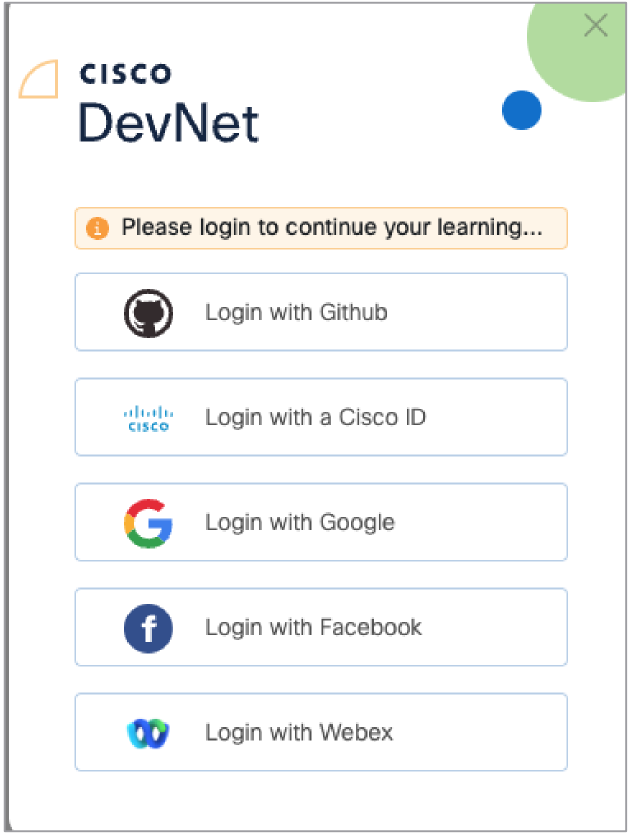
OAuth Authorization URL
You can use the URL below to initiate an OAuth permission request for this app. It is configured with your redirect URI and app scopes. Be sure to update the state parameter.

```
https://webexapis.com/v1/authorize?
client_id=C675c2e3d71c7eef23ef4a71615eac8b791c953bbcde1
33acc3bd3122476a4c77&response_type=code&redirect_uri=http
%3A%2F%2Flocalhost%3A8080%2Foauth&scope=spark%3Aall%2
0spark%3Akms&state=set_state_here
```

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Login with Webex

- Same exact steps as an integration
- Based on OpenID Connect
- Selecting scopes is optional
- Developer adds "open_id" and user info scopes to Authorize URL
- Requests return an "id_token" with claims about the authorizing user



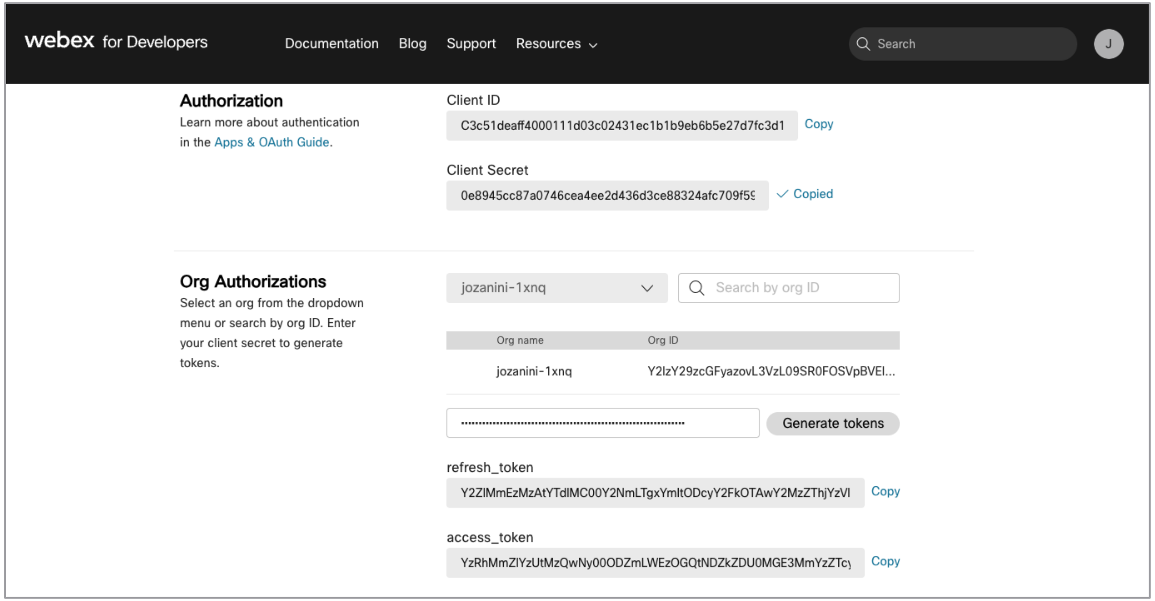
cisco DevNet

Please login to continue your learning...

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex Service Apps

- Developer registers a Service App
- Developer selects scopes
- Developer requests Admin Authorization
- Admin authorizes Service App in Control Hub
- Developer gets access_token and refresh_token from developer portal.



Authorization

Learn more about authentication in the Apps & OAuth Guide.

Client ID: C3c51deaff4000111d03c02431ec1b1b9eb6b5e27d7fc3d1 Copy

Client Secret: 0e8945cc87a0746cea4ee2d436d3ce88324afc709f5 ✓ Copied

Org Authorizations

Select an org from the dropdown menu or search by org ID. Enter your client secret to generate tokens.

jozanini-1xnq

Search by org ID

Org name	Org ID
jozanini-1xnq	Y2lzY29zcGFyazovL3VzL09SR0FOSVpBVEl...

••• Generate tokens

refresh_token: Y2ZlMmEzMzAtYTdlMC00Y2NmLTgxYmltODcyY2FkOTAwY2MzZThjYzVl Copy

access_token: YzRhMmZlYzUtMzQwNy00ODZmLWEzOGQtNDZkZDU0MGE3MmYzZTc Copy

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: jozanini@cisco.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The bridge to possible

Thank you

#CiscoLive