

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Building Duo SSO Into Your Custom Application

Alvin Lau, Systems Engineer
DEVNET-2555

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

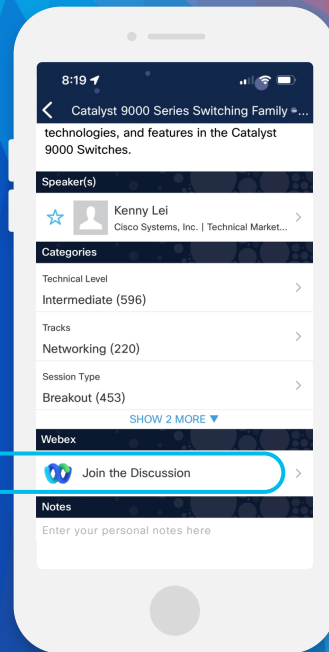
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2555>

Recent attacks highlight risk in weaker identity protection



2FA Compromise Led to \$34M Hack



The Hack Shows Push Notification 2FA Has a Downside: It's Too Annoying



MFA Fatigue: How Hackers Breached 3 Big Companies



New Gmail Attack Bypasses Passwords and 2FA To Read All Email



Russian hackers exploited MFA and 'PrintNightmare' vulnerability in NGO breach, U.S. says



Oktapus phishing campaign exploit MFA to compromise 130 companies



Cybercriminals Launching More MFA Bypass Attacks



Identity is the
new perimeter

+



Attackers actively
exploit identity gaps
and weaknesses

+



80% of organizations
are NOT prepared

[2023 Cisco's Cybersecurity Readiness Index](#)

The Perfect Storm



Secure access

+



Protect against
identity targeting
attacks

+



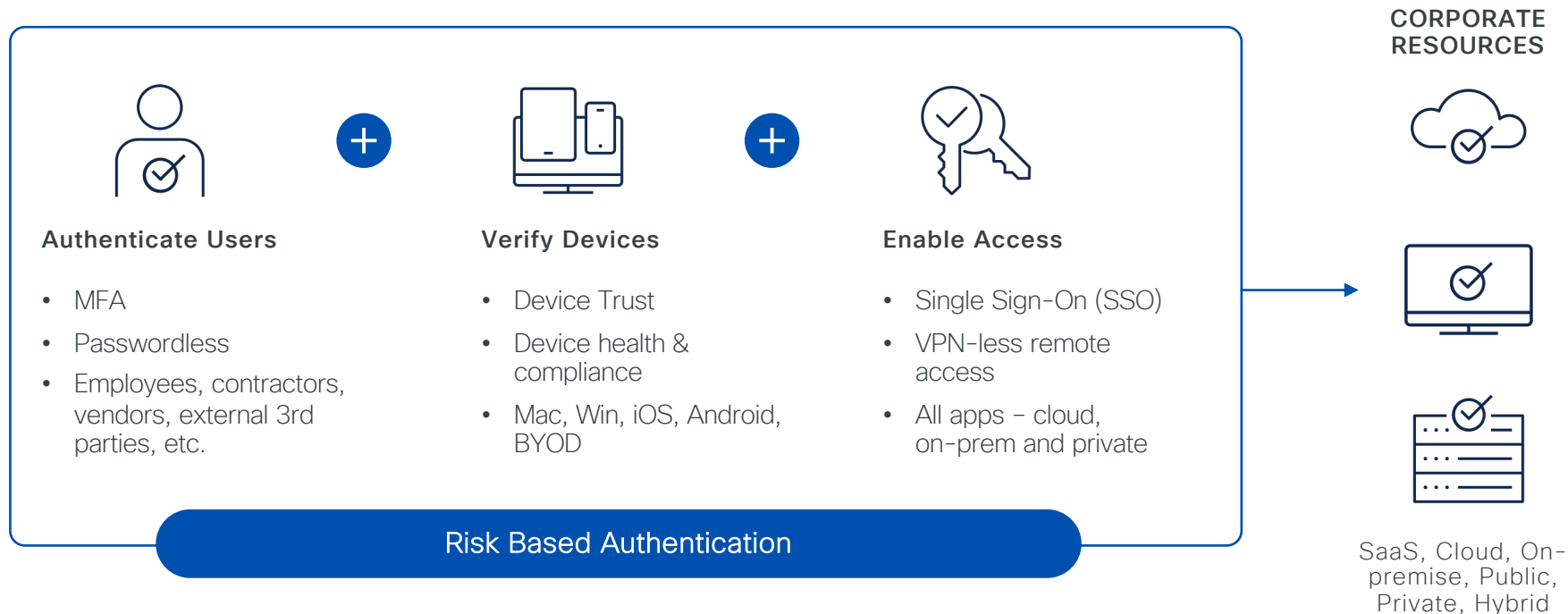
Simple, easy to use,
fast to deploy &
cost-effective for all

Duo provides what is needed

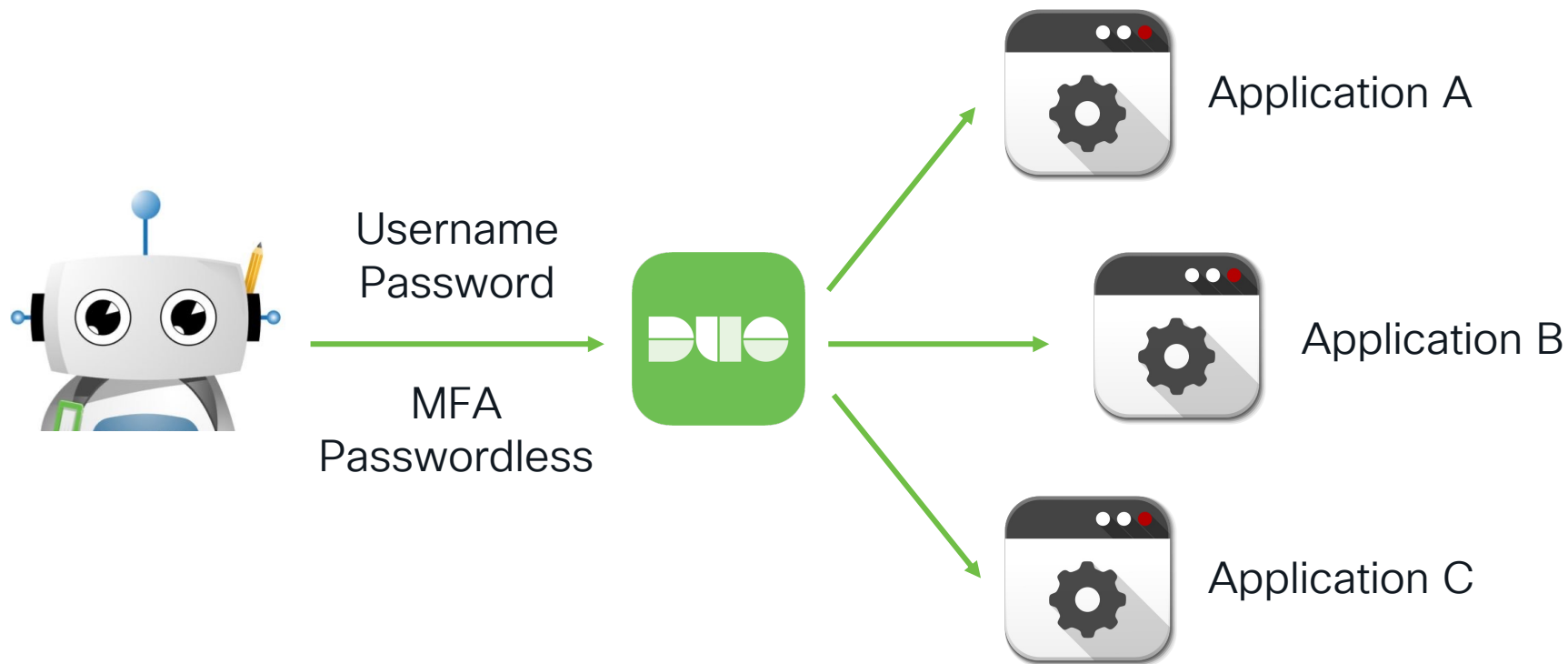
Agenda

- Benefits
- Building Duo SSO Strategies
- Demo
- Application Implementation

Quick Recap on Duo



Single Sign-On (SSO)

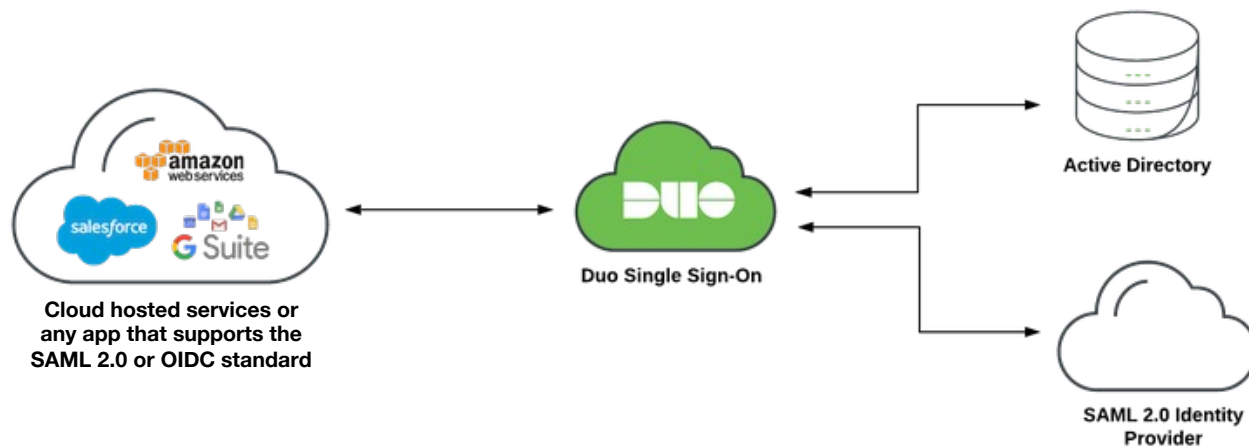


Why Extending Duo SSO to Custom Application?

- Inherit Duo features – stronger security
- Don't let one application be the security loophole!
- Ensure full compliance
- Consistent user experience

Duo SSO Strategies

- MFA through Web SDK (No SSO)
- SSO with SAML 2.0
- SSO with OIDC

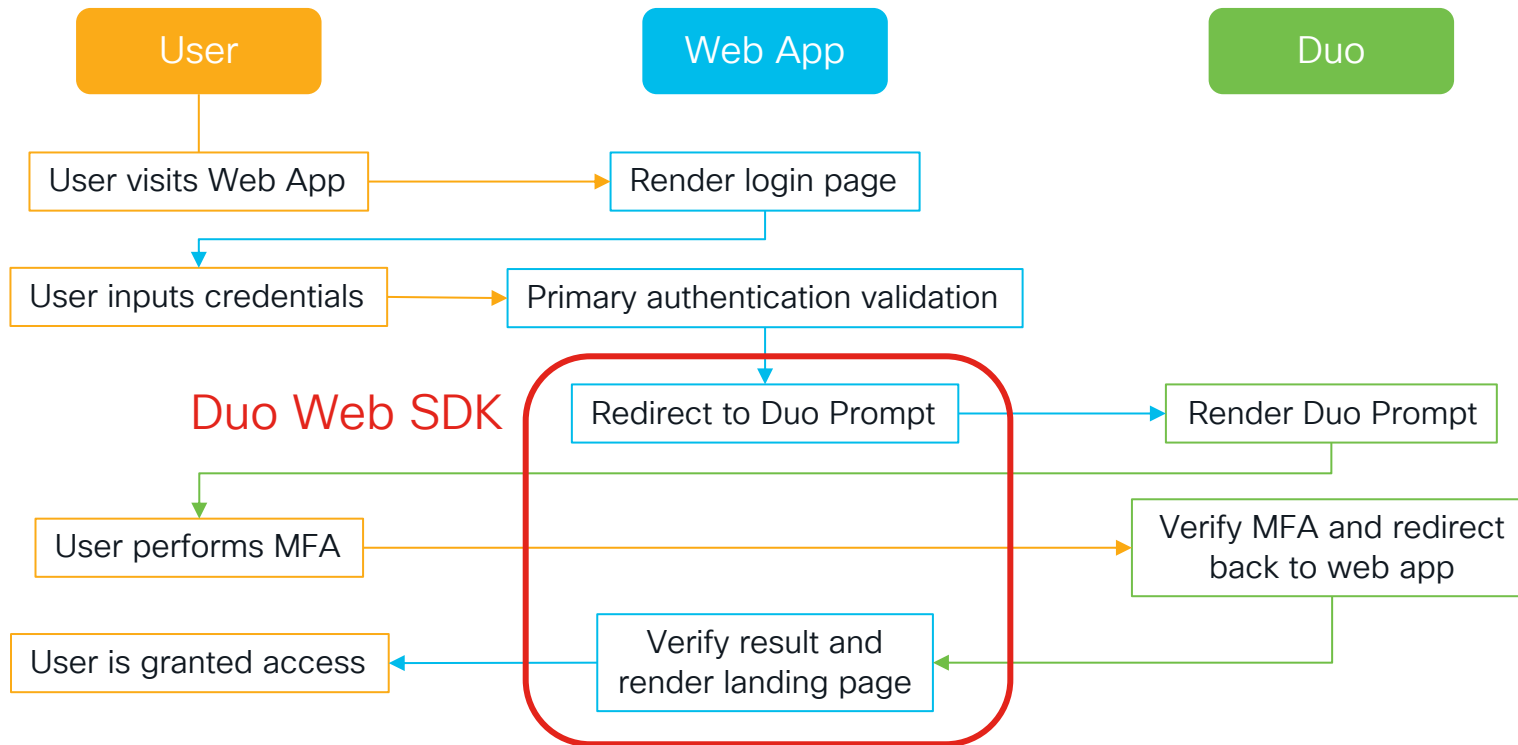


Duo Web SDK

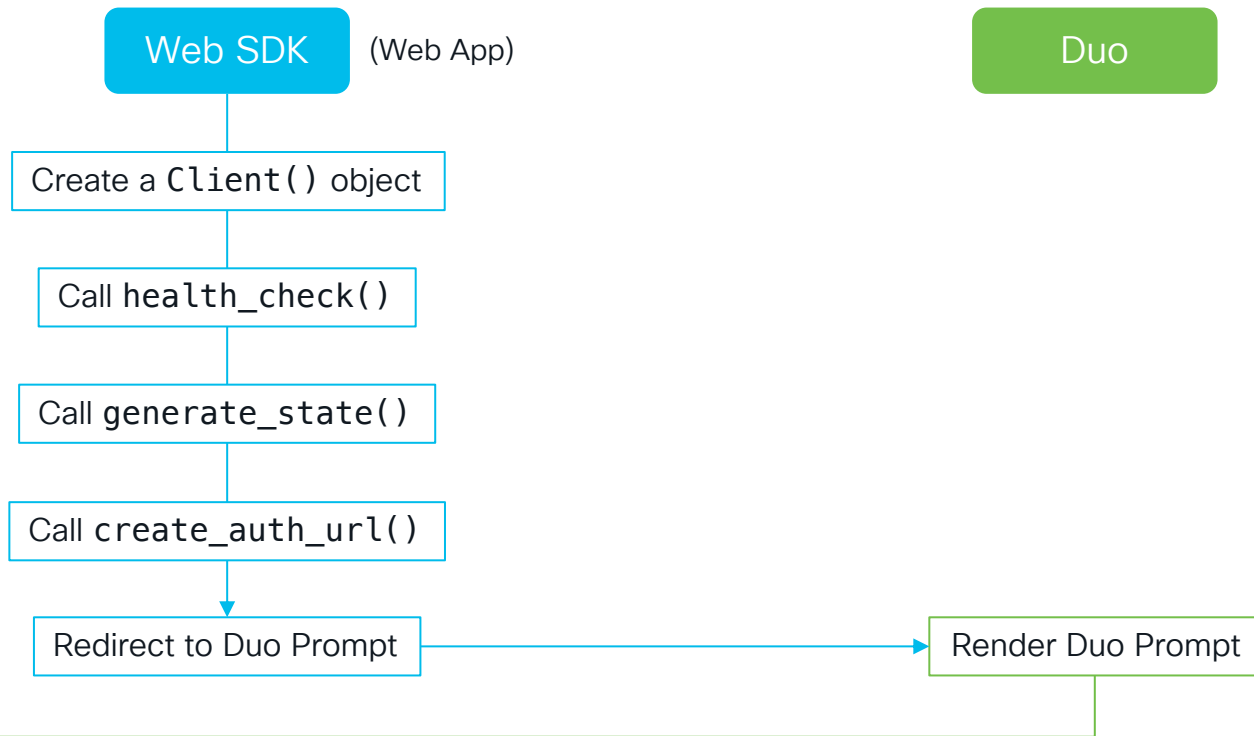
- Client libraries are available for Python, Java, Go, PHP, Node.js, and C# (.NET)
- Language-specific implementations of the OIDC Auth API
 - An OIDC standard-based API for adding two-factor authentication to your web application



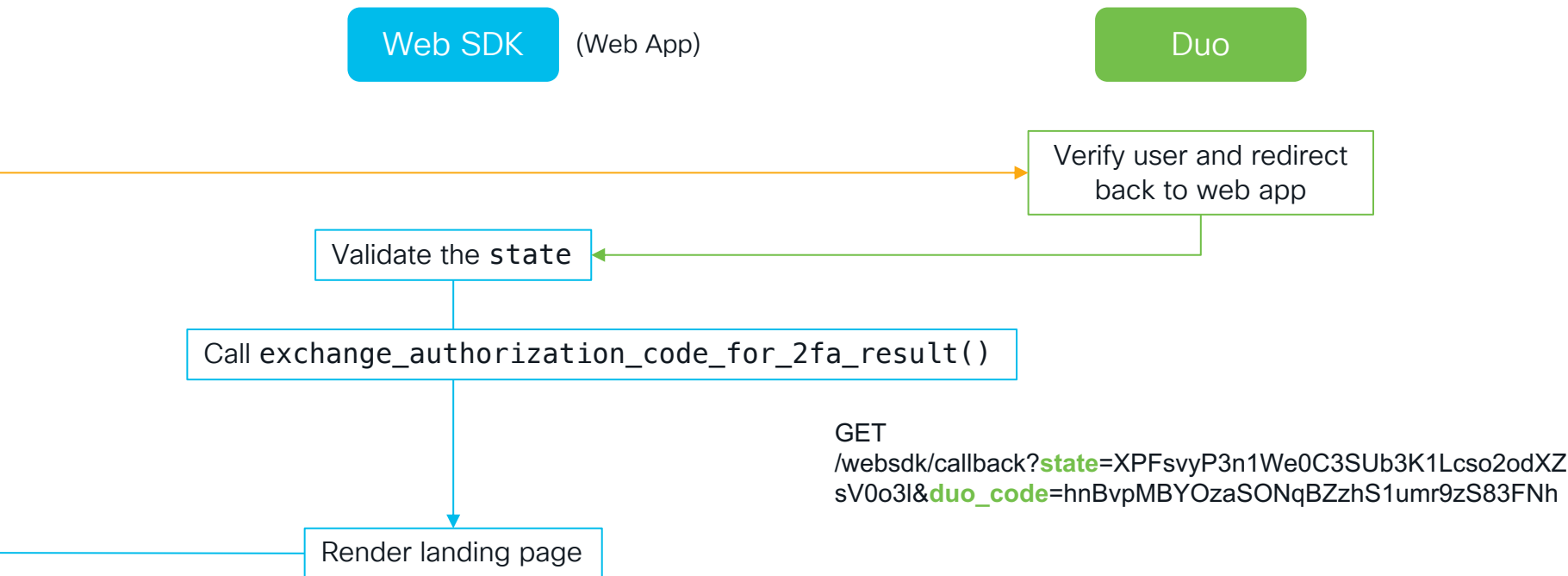
Duo Web SDK Workflow



Breaking down Duo Web SDK



Breaking down Duo Web SDK

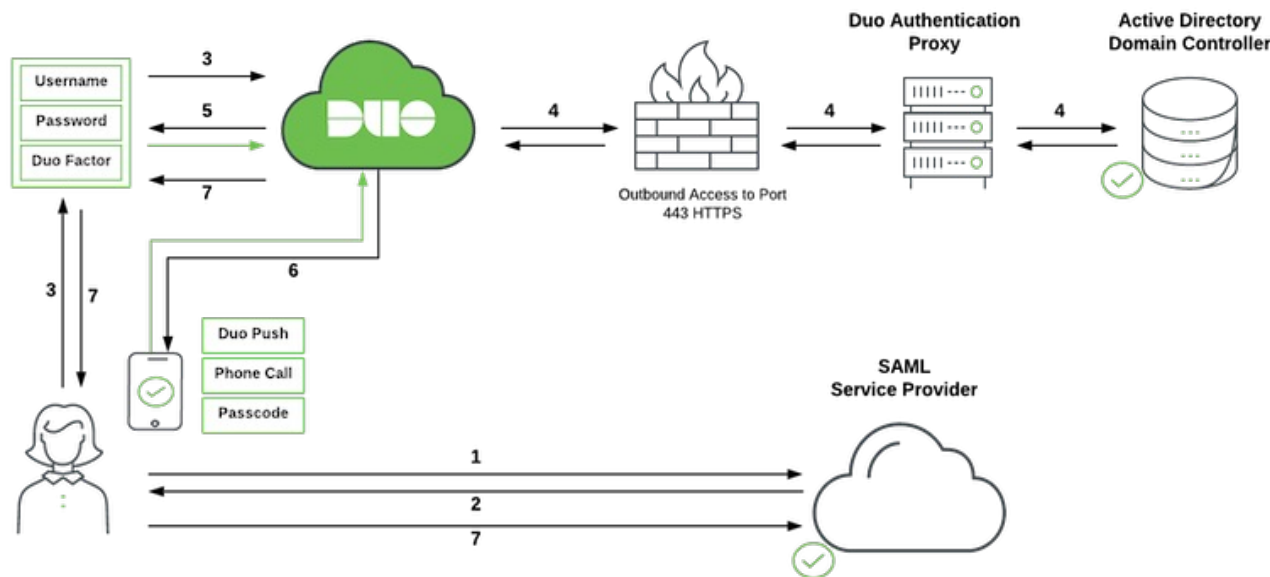


Duo SSO with SAML 2.0

- SAML 2.0 – version 2.0 of the Security Assertion Markup Language
 - A mature technology dating from 2005 and supports a wide range of identity functionality
 - Provides a mechanism for federated identity
 - Uses XML as data format, HTTP or SOAP as transport
 - SAML Assertion contains user identity data
- Duo Single Sign-On acts as an Identity Provider (IdP) while the app acts as SAML Service Provider (SP)
 - Has IdP Validation and SP Validation mechanism

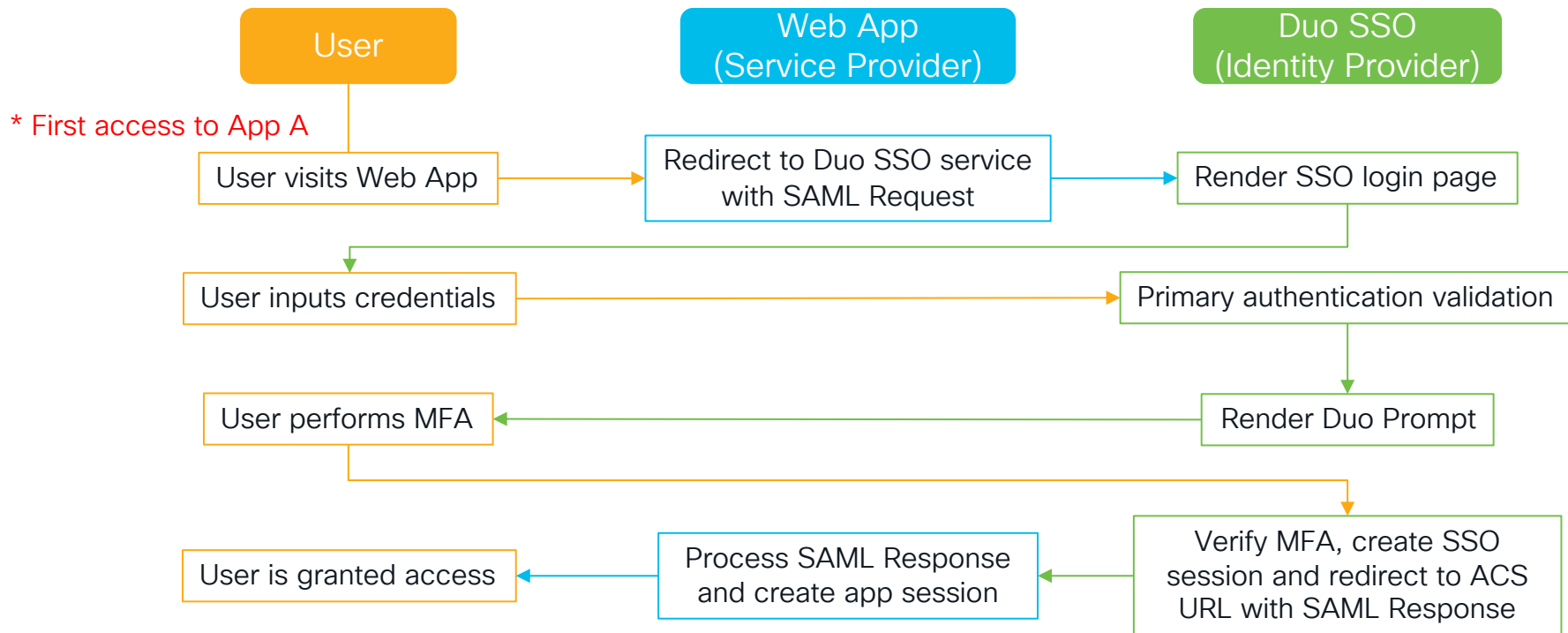


Network Diagram – Active Directory

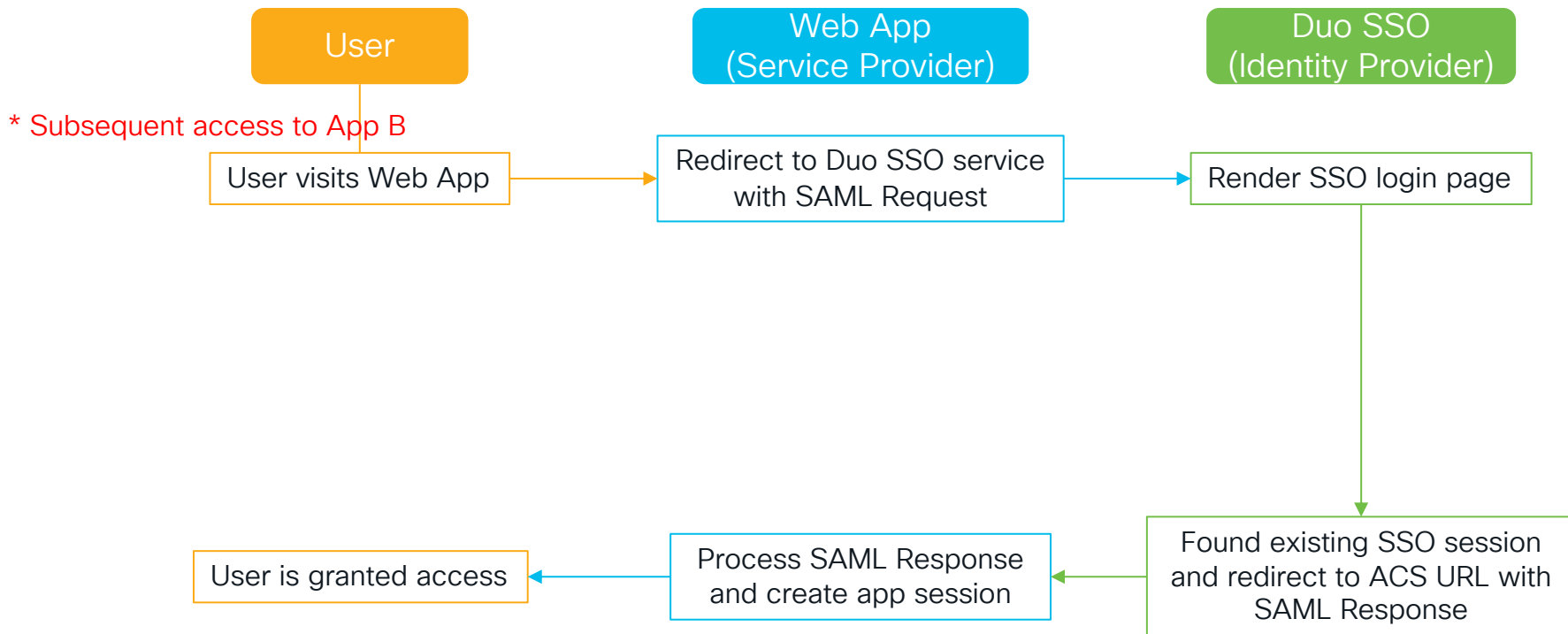


1. User initiates SAML service provider login.
2. SAML service provider redirects user's browser to Duo Single Sign-On with a SAML request message.
3. User logs in with primary credentials.
4. Duo Single Sign-On sends the credentials to the Duo Authentication Proxy in the customer's network. The Authentication Proxy forwards this to Active Directory which returns a response back to Duo Single Sign-On.
5. Duo Single Sign-On requires the user to complete two-factor authentication.
6. User completes Duo two-factor authentication.
7. Duo Single Sign-On redirects user's browser to the SAML service provider with response message.

Duo SSO with SAML 2.0 Workflow



Duo SSO with SAML 2.0 Workflow



SAML Request

```
1 <samlp:AuthnRequest
2   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
3   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
4   ID="ONELOGIN_4ea44aae1bf8c01758b2c7859af63ff1272c0bc3"
5   Version="2.0"
6   | ProviderName="alvlau.com"
7   IssueInstant="2023-11-09T04:09:38Z"
8   Destination="https://sso-1cbd47ef.sso.duosecurity.com/saml2/sp/DI5WNLH3TTFASNZ50TAA/sso"
9   ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
10  AssertionConsumerServiceURL="https://84c2-223-17-44-234.ngrok-free.app/saml/acs">
11    <saml:Issuer>DEVNET-2555-SAML-SSO</saml:Issuer>
12    <samlp:NameIDPolicy
13      | Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
14      | AllowCreate="true" />
15    <samlp:RequestedAuthnContext Comparison="exact">
16      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
17    </samlp:RequestedAuthnContext>
18  </samlp:AuthnRequest>
```

SAML Assertion

```
1  <samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
2    <samlp:Status>
3      <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
4    </samlp:Status>
5    <saml:Assertion ID="DU0_bee0ccddf7c7256d0064018d7257dbfba6c9d03b"
6      IssueInstant="2023-10-23T15:04:50Z" Version="2.0">
7      <saml:Issuer>https://sso-1cbd47ef.sso.duosecurity.com/saml2/sp/DI5WNLH3TTFASNZ50TAA/metadata</saml:Issuer>
8      <ds:Signature>
9        (truncated)
10     </ds:Signature>
11     <saml:Subject>
12       <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
13         alvin@alvlau.com</saml:NameID>
14       <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
15         <saml:SubjectConfirmationData NotOnOrAfter="2023-10-23T15:09:50Z"
16           Recipient="https://84c2-223-17-44-234.ngrok-free.app/saml/acs"
17           InResponseTo="ONELOGIN_f719f30a956bf911ff2c7a80d9e4f794b524b9f8" />
18       </saml:SubjectConfirmation>
19     </saml:Subject>
20     <saml:Conditions NotBefore="2023-10-23T15:04:20Z" NotOnOrAfter="2023-10-23T15:09:50Z">
21       <saml:AudienceRestriction>
22         <saml:Audience>DEVNET-2555-SAML-SSO</saml:Audience>
23       </saml:AudienceRestriction>
24     </saml:Conditions>
25     <saml:AuthnStatement AuthnInstant="2023-10-23T15:04:50Z"
26       SessionIndex="DU0_bee0ccddf7c7256d0064018d7257dbfba6c9d03b">
27     </saml:AuthnStatement>
28   </saml:Assertion>
29 </samlp:Response>
```

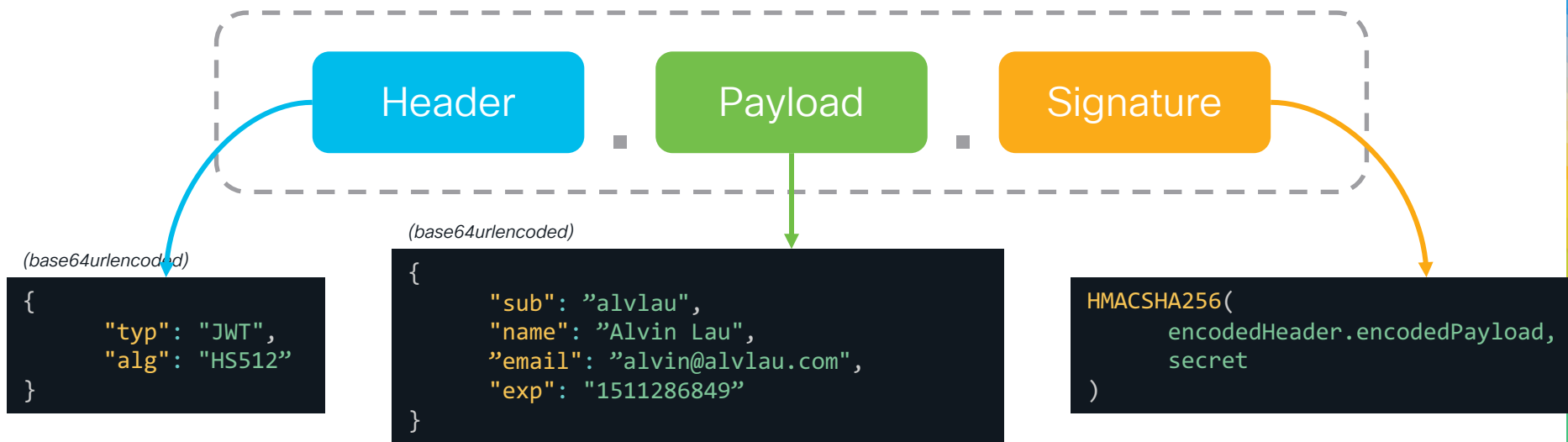
Duo SSO with OIDC

- OIDC – OpenID Connect, an extension of OAuth 2.0
 - allows third-party applications to verify the identity of the end-user and to obtain basic user profile information through RESTful HTTP API
 - Uses JSON web tokens (JWTs) that contain claims about a user's identity
 - Uses scope to define a set of user attributes (claims)
- Duo Single Sign-On acts as an OIDC Provider (OP) while the app acts as OIDC Relying Party (RP)
 - Supported grant type today
 - Authorization Code Flow
 - Authorization Code Flow with Proof Key for Code Exchange (PKCE)

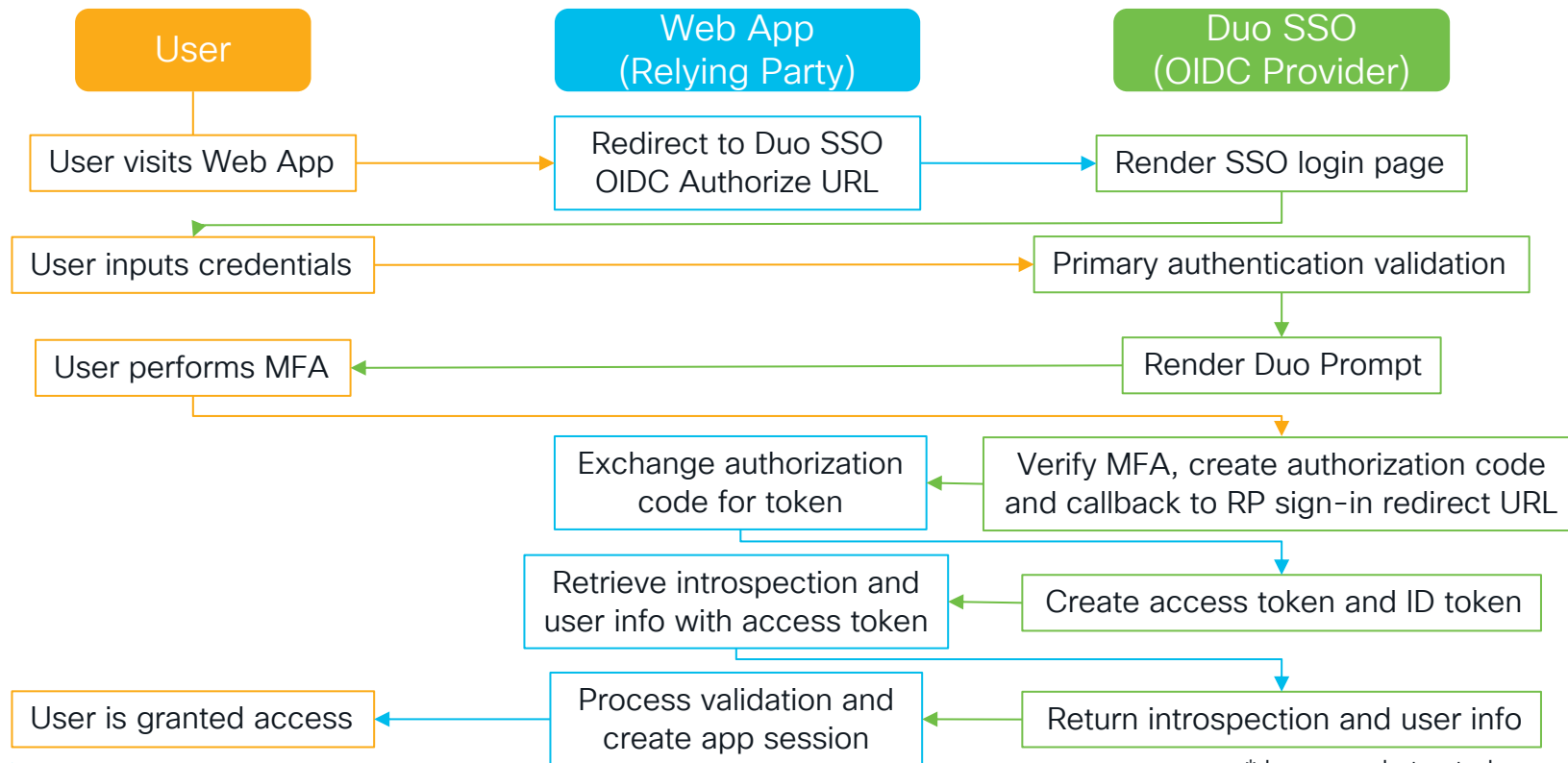


JSON Web Token (JWT)

- Use JSON Web Token (JWT) standard
- Composed of three parts, separated by a dot (.)



Duo SSO with OIDC Workflow





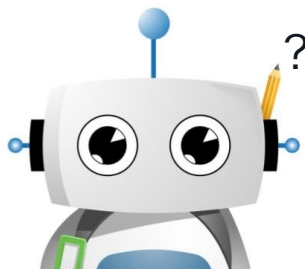
Demo

Application Implementation



SSO Strategy Planning

Corporate SSO readiness	Application type	Library support?	Implementation Difficulty?	SSO Strategy
No	Web	Cisco	Easy	Duo Web SDK (No SSO)
Yes	Web	Plenty	More complex	Duo SSO with SAML 2.0
Yes	Web, Mobile, SPA	Plenty	Easy	Duo SSO with OIDC



Application Dependencies / Libraries

Language	Duo Web SDK Required Version	SAML Library examples
Python	3.0 or later	python3-saml, python-saml, pysaml2
Java	8 or later	Shibboleth, SAML Java Toolkit, SpringSecurity SAML
PHP	7.4 or later	SAML PHP Toolkit
Node.js	14 or later	passport-saml, node-saml, saml2-js
.NET	Core 3.1 or later; Framework 4.7.1 or later	dotnet-saml

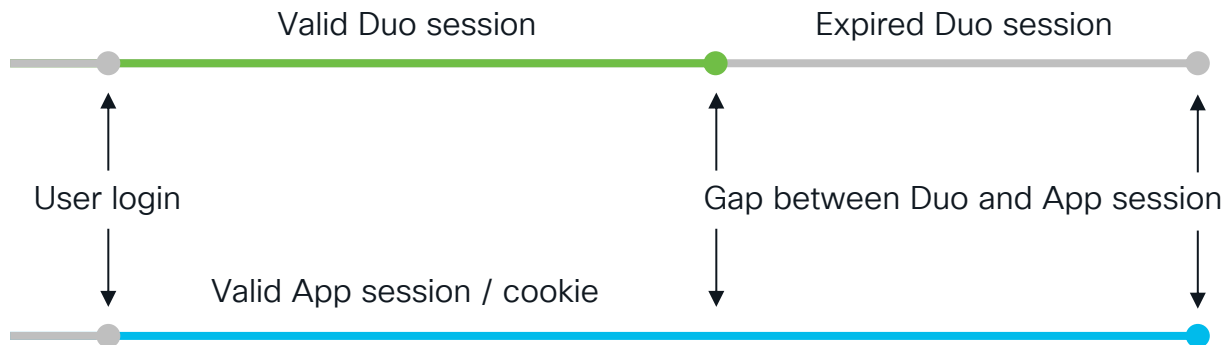


GOLANG



SSO Sessions / Cookies Management

- IdP's and OP's responsibility is to provide identity authentication
- Validation of sessions and cookies is application's responsibility



Summary

- Duo supports MFA and SSO with your in-house custom applications which inherit Duo features
- Duo SSO strategies provide flexibility for different applications and use cases
- Careful planning including application dependencies and workflow will lead to a successful SSO adoption

Call to Action



Developer Resources

- [Duo Web v4 SDK](#)
- [Duo Single Sign-On for Generic SAML Service Providers](#)
- [Duo Single Sign-On for Generic OpenID Connect \(OIDC\) Relying Parties](#)
- [Demo GitHub Repository](#)



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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

Continue to Learn, Code, and Build with Cisco DevNet

Get access to exclusive resources including API documentation, Code Exchange, self-paced learning labs, sandboxes, community forums and events!

Scan QR Code to get started.





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC