

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Modern Auth & SSO for Networkers

Making sense of modern auth suites for those that miss the good ol' days of RADIUS and TACACS+ :)

Jeff Groesbeck – Leader, Duo Tech Marketing Engineering
Aaron T. Woland – Distinguished Engineer
BRKSEC-2061

\$ whoami



Cisco role: Distinguished Engineer

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder how I have been doing this for ~30 years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco now! Youngest is 3 years old!

Fun fact 3: Just graduated from SANS: MS in Cyber Security

Who is Jeff?



Cisco role: Leader, Duo TME (5 years)

Experience: Over 30 years industry experience. Worked for Cisco partners for 20 years

Fun fact 1: Loves the outdoors!

Fun fact 2: Apparently wears all the SWAG even while being outdoors.

Fun fact 3: No more kids living at home!

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2061>



Please fill out the survey



Drop your email in the comments – we WILL respond!

Important: Hidden Slide Alert



Look for this “For Your Reference”
Symbol in your PDF’s

There is a tremendous amount of
hidden content, for you to use later!



For Your Reference

Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

As the unofficial “Cisco History Professor” I tend to explain technology with a bit of a history lesson, so you can understand how we got to where we are.

–Aaron T. Woland
random guy in IT since the Dinosaurs

“Authentication, Authorization & Accounting is an age-old security principal that should apply to all things Security related”

– Aaron T Woland, pompous windbag

AAA



I'd like 40K from Chuck Robbins' Account

Do You Have Identification?

Yes, I Do. Here it Is.

Authentication

X

Sorry, Aaron Woland is not Authorized

Authorization

Access to Chuck Robbins' Account



Who
Did What
When
Accounting

CISCO *Live!*

AAA in a networking world

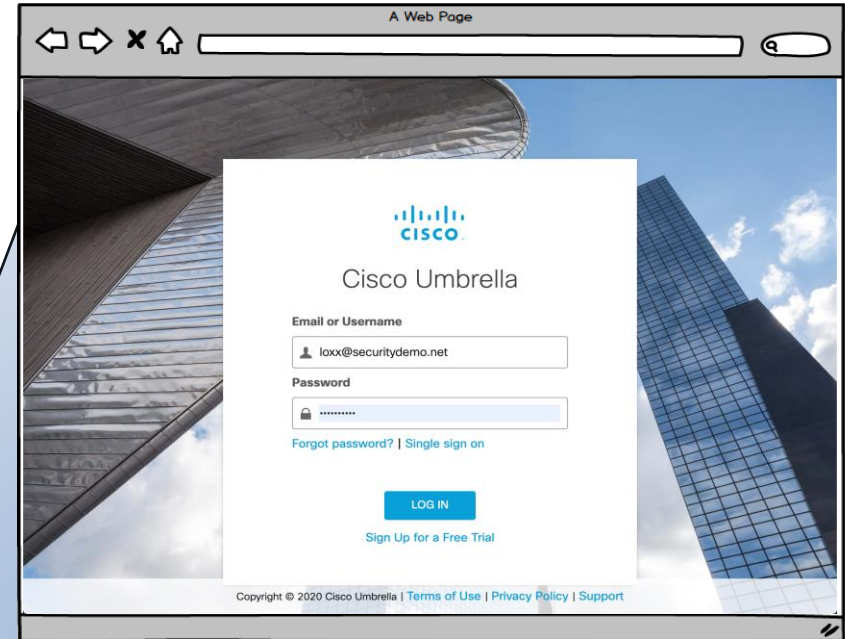
- In “our” world, we have thought of AAA for controlling access to networks.
 - 802.1X
 - Remote Access VPN
 - Or access to our terminals / CLI's (i.e.: TACACS+)
- Know who and what is connecting to your network before granting access, and let that access be specific.

Network access AAA

- ISE is sort of like the TSA agent of the network, if you will.
- It validates who you are by checking your credential (username/password/certificate) and that the credential is trusted.
 - Did the username/password match
 - Was the certificate signed by a trusted authority
 - Proof of possession
- It validates the device is allowed
 - Is it an allowed type (Profile)
 - Does it meet the security requirements (Posture)

Application Access

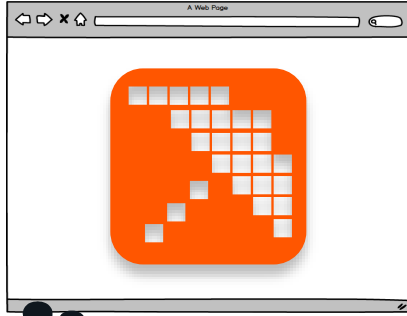
- While WE spend so much time focused on network authentication:
- The same principals are applicable to applications & web sites



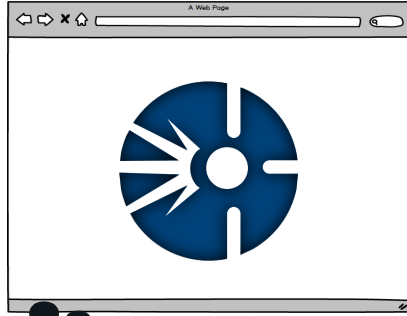
Application Access

- Must login to web apps (like the Cisco Live app)
- Identify WHO the human is & what access they get to the app
- Speakers get different access than attendees

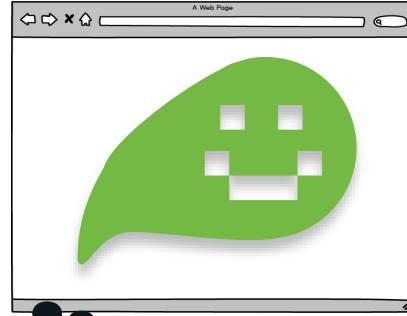
Each App maintains its own User DB



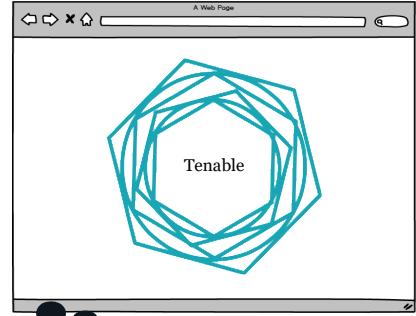
- user1 / pwd
- user2 / pwd
- user3 / pwd



- user1 / pwd
- user2 / pwd
- user3 / pwd



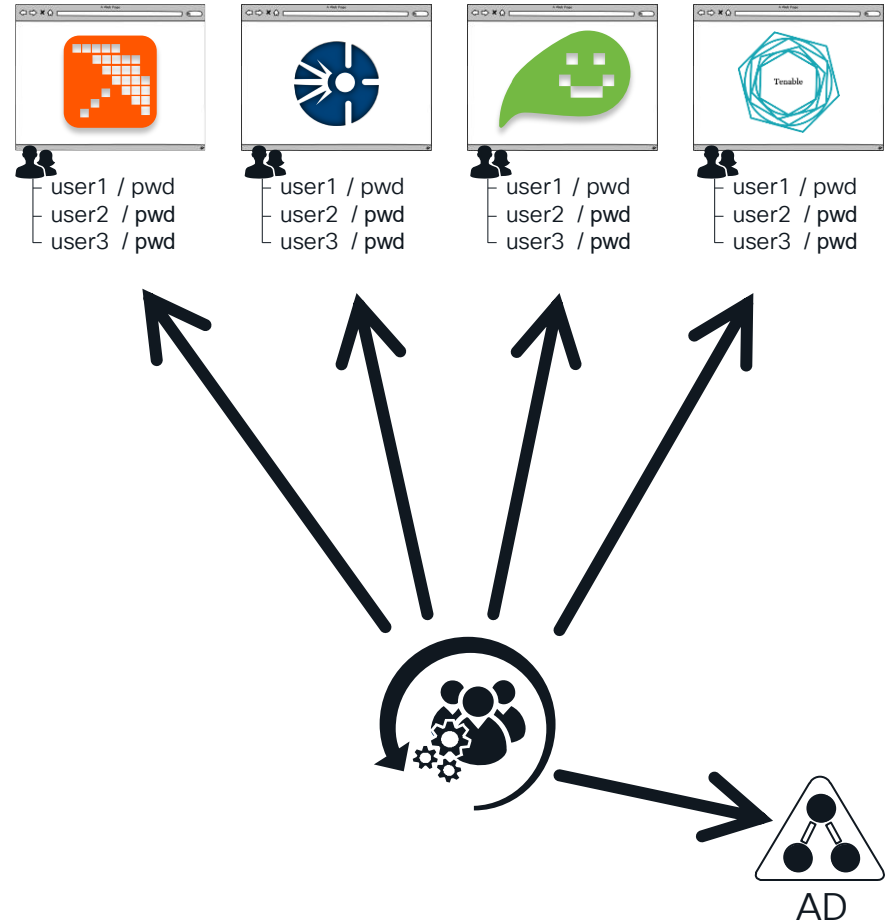
- user1 / pwd
- user2 / pwd
- user3 / pwd



- user1 / pwd
- user2 / pwd
- user3 / pwd

Enter: Identity Management Products

- Solution to keep all user accounts across all these web apps in sync.
 - Examples:
 - - Tivoli Identity Manager
 - - Oracle Identity Manager
 - - Okta Identity Management
 - - etc.



Example

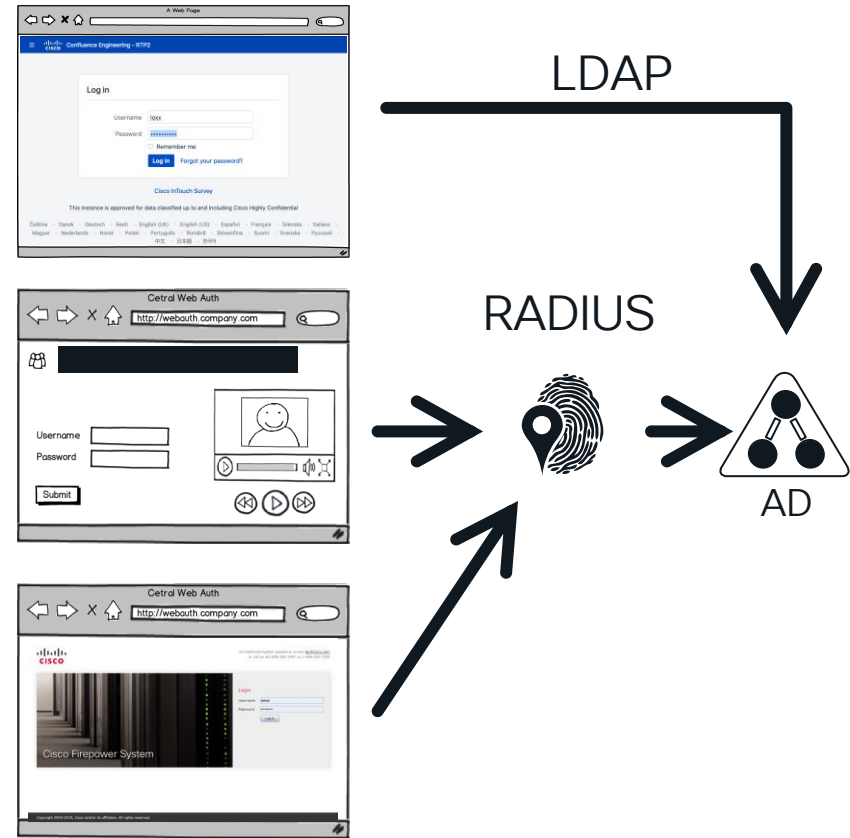
- Example of what an IAM would do when you change your password
- *** Cisco Infosec policy won't let me show you the REAL screen, so I mocked up a fake*

<http://password.company.com>

Account	Target System	Password Changed?	Result
loxx	Prod AD	Yes	Success
loxx	Linux NIS	Yes	Success
loxx	Stage AD	Yes	Success
aawoland	OpenLDAP	Yes	Success
loxx	Call Mgr	Yes	Success
loxx	WebEx	Yes	Success

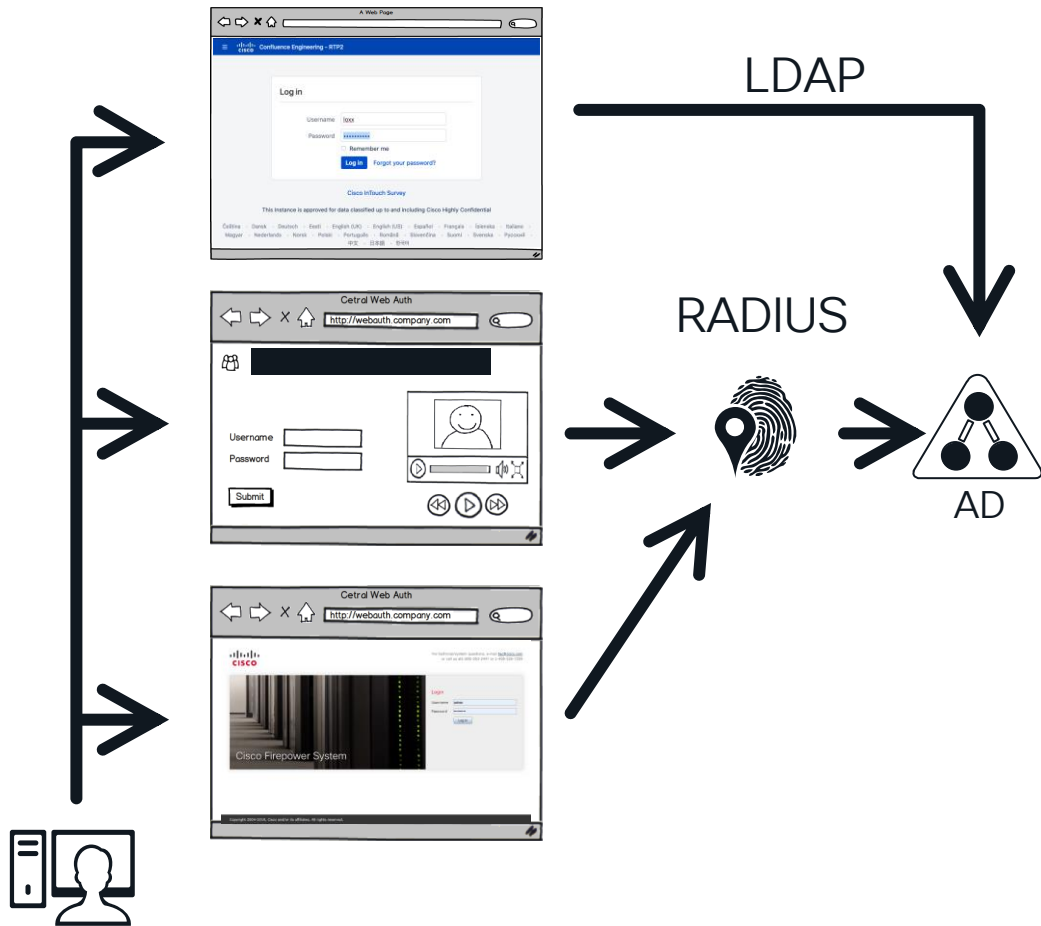
Some tried RADIUS or LDAP logins

- Provided a single location for username/passwords
- But still requires user to login each & every app separately



Bad User Experience

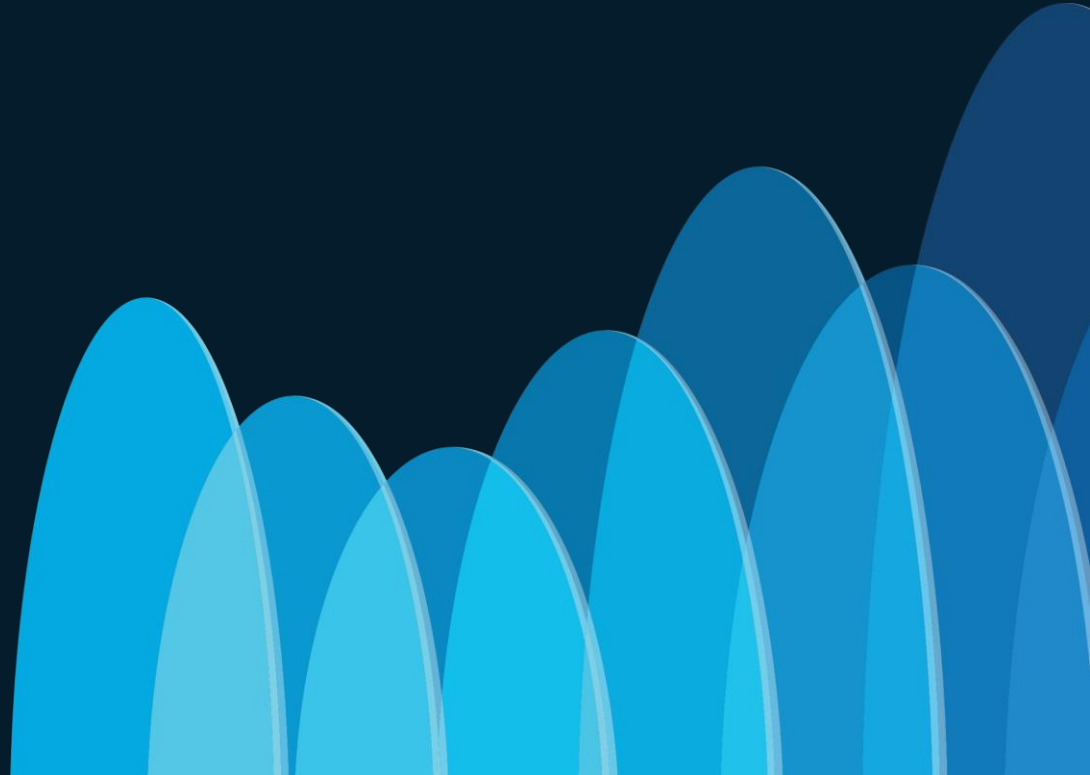
- Still requires a user to log in to each app
- Same username / password
- But must use it separately
- Is this Single-Sign-On?



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

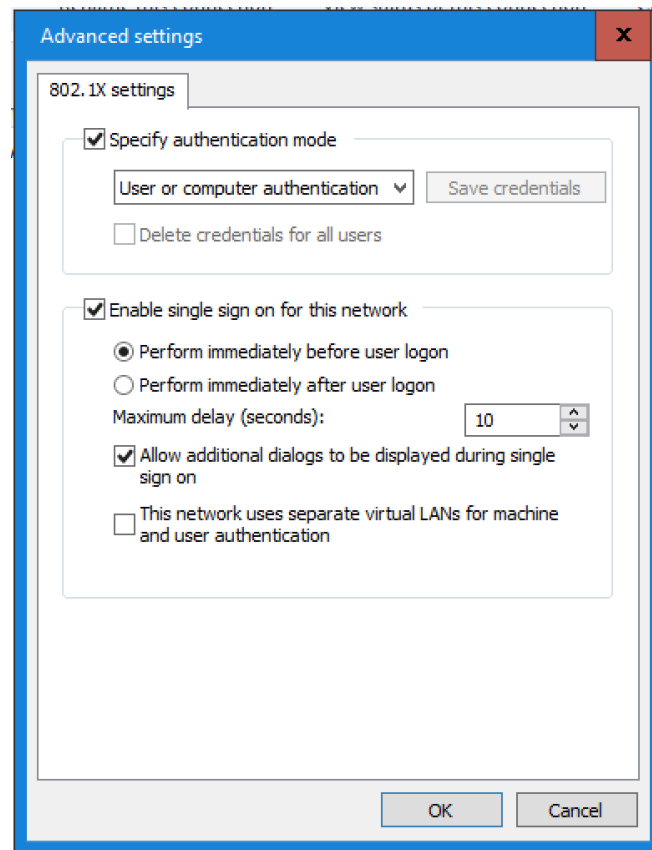
Enter: Single Sign On



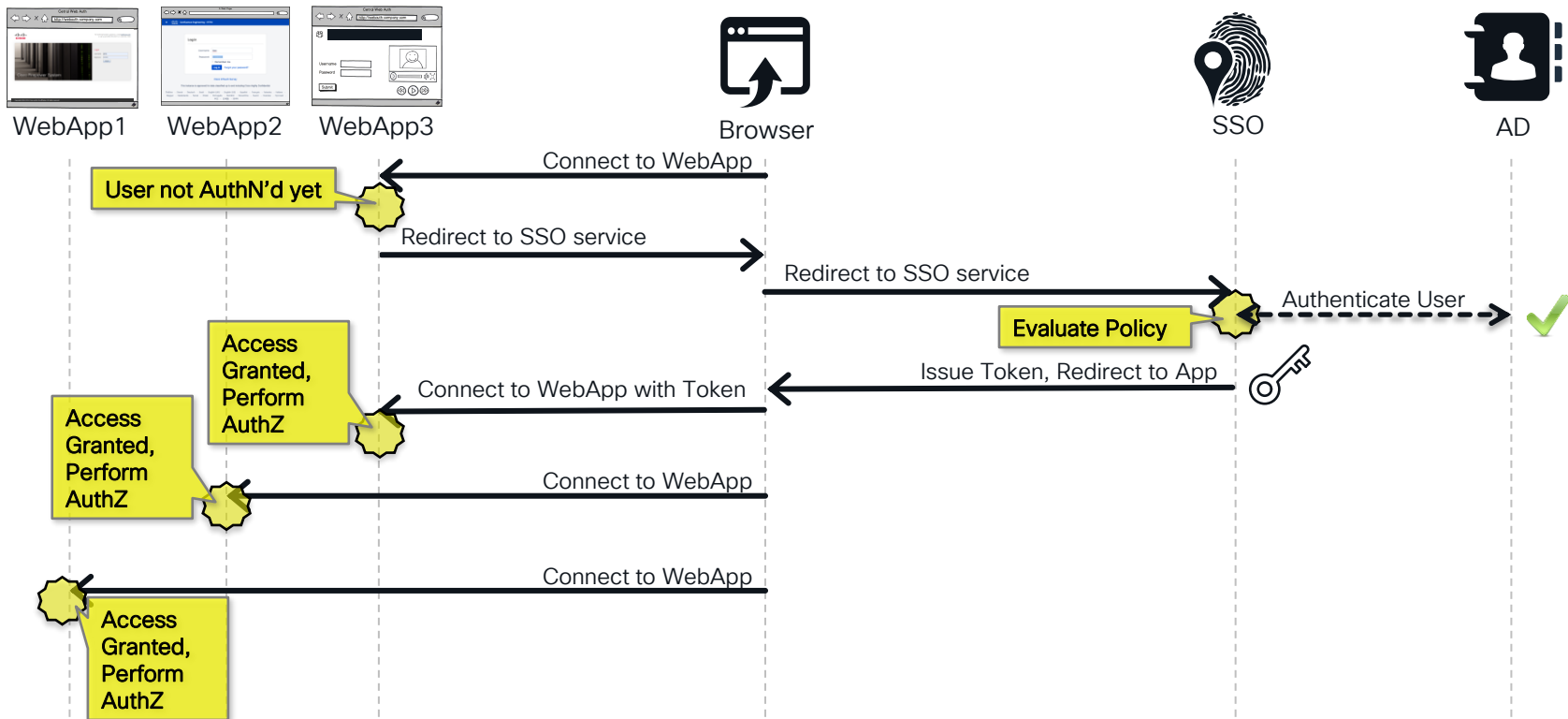
Single Sign On
(SSO): one key to
unlock multiple
doors

*SSO itself is the process that
allows a single
authentication to be used
across multiple web sites or
applications*

SSO w/ Dot1X Supplicant



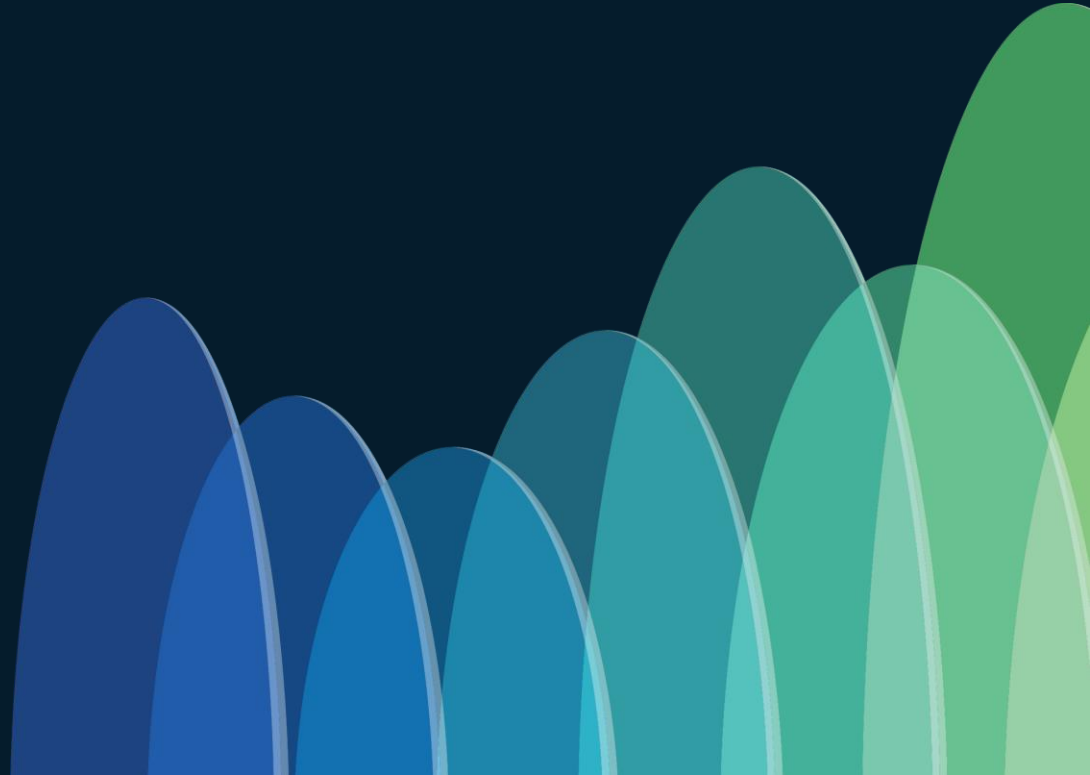
SSO [somewhat] Explained

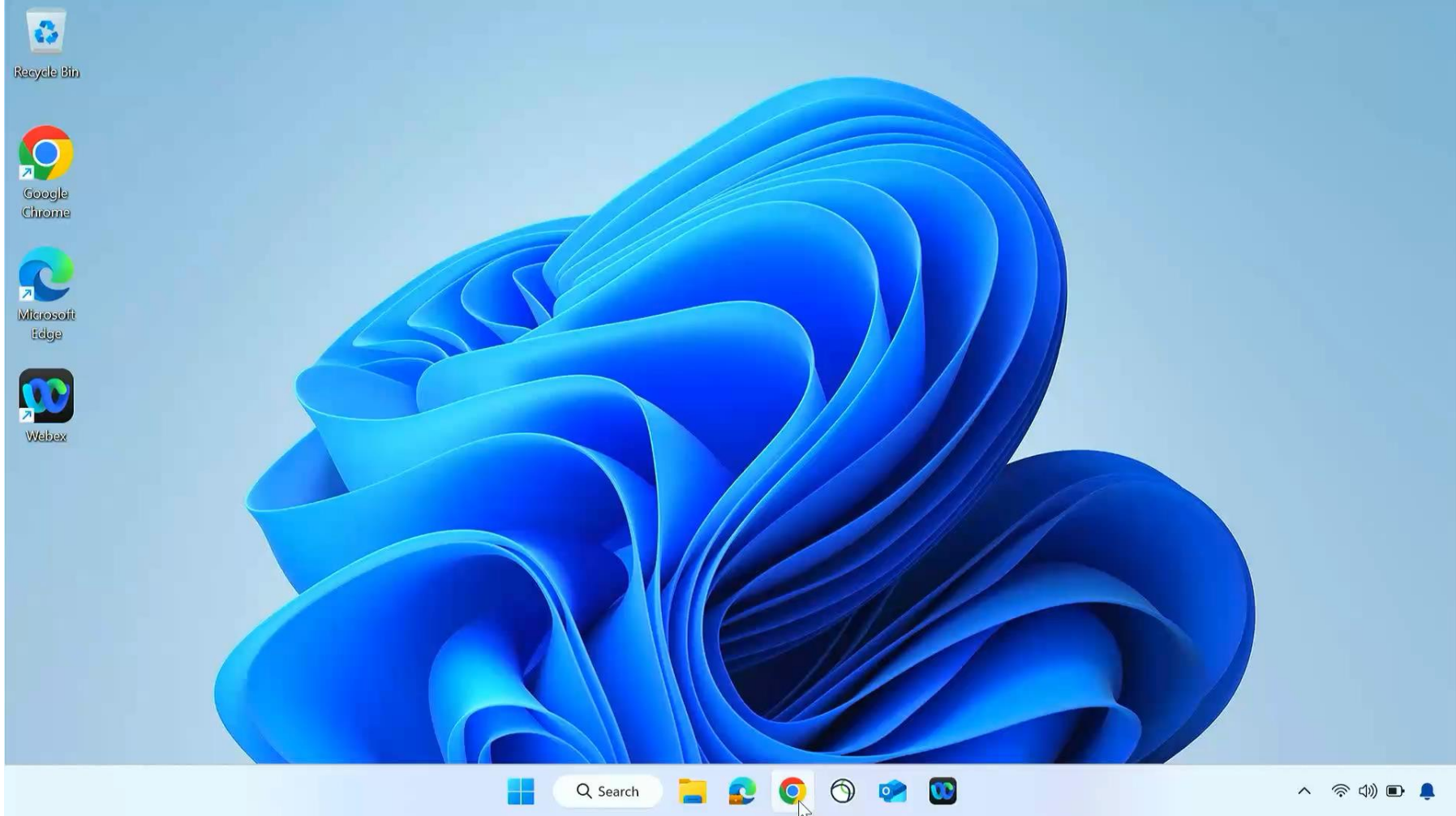


SSO principals

- AuthN One Time
 - Each app uses the same AuthN, performs AuthZ locally
- Tries to use existing auth
 - If no existing, will send user for authentication

Demo Video: Single Sign On with Duo





Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

Enter: Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML)

- Open Standard (OASIS Consortium)
 - v2 is most common, standardized back in 2005
 - Allows the SSO product to pass credentials to applications, so a single credential can be used across many web sites / apps
 - Uses XML for the data

Definitions

Web-based
Auth's



Browser
aka: User Agent

Acts as the “client”. Each AuthN session is stored per-UserAgent (ex: Outlook, Chrome, Safari, etc.)

Like combo of supplicant & authenticator in dot1x.



Service
Provider (SP)



IdP



Directory

802.1X



Supplicant



Authenticator



Authentication
Server



Directory

Definitions

Web-based
Auth's



Browser
aka: User Agent



Service
Provider (SP)



IdP



Directory

The application that needs to be
logged into.
(ex: ServiceNow, Salesforce, etc.)

Like the Authenticator in dot1x

802.1X



Supplicant



Authenticator



Authentication
Server



Directory

Definitions

Web-based
Auth's



Browser
aka: User Agent



Service
Provider (SP)



Identity
Provider (IdP)



Directory

Handles the authentication, user
management, etc.

(ex: PING, EntraID, Shibboleth, etc.)

Like the Authentication Server in dot1x

802.1X



Supplicant



Authenticator



Authentication
Server



Directory

Definitions

Web-based
Auth's



Browser
aka: User Agent



Service
Provider (SP)



Identity
Provider (IdP)



Directory

The ID store. Could be built into the IdP or could be separate (like AD).
(ex: AD, LDAP, JDBC, etc.)

Same as the ID Store with dot1x

802.1X



Supplicant



Authenticator

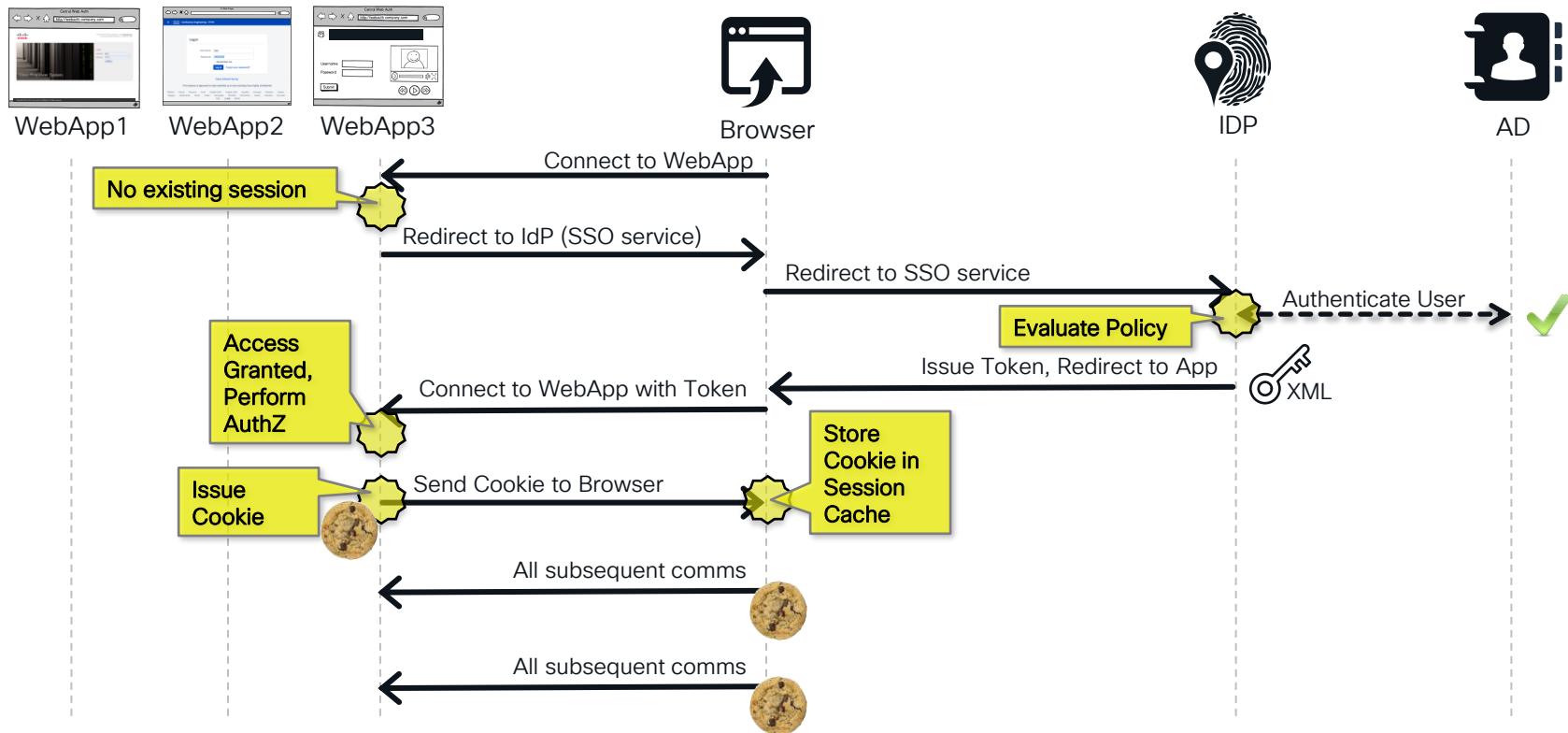


Authentication
Server

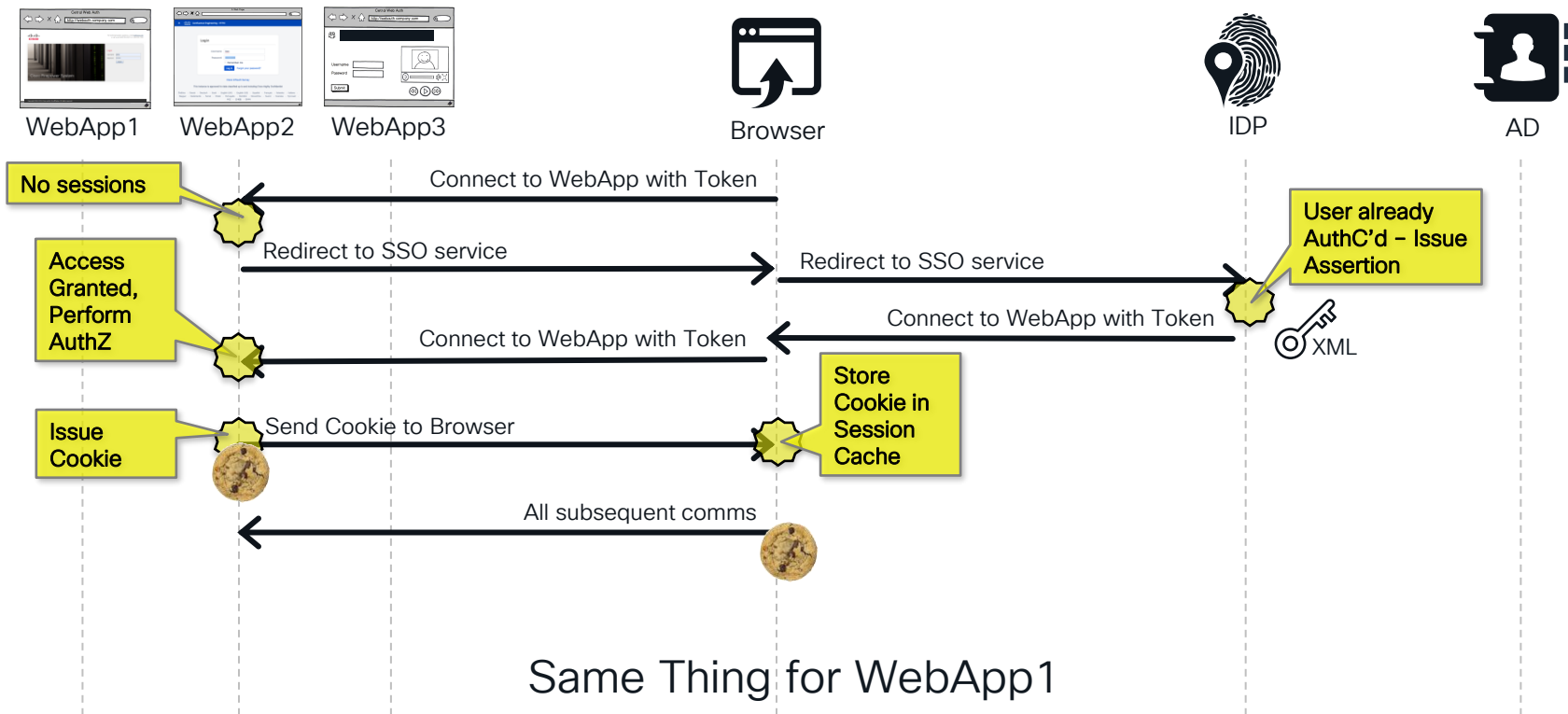


Directory

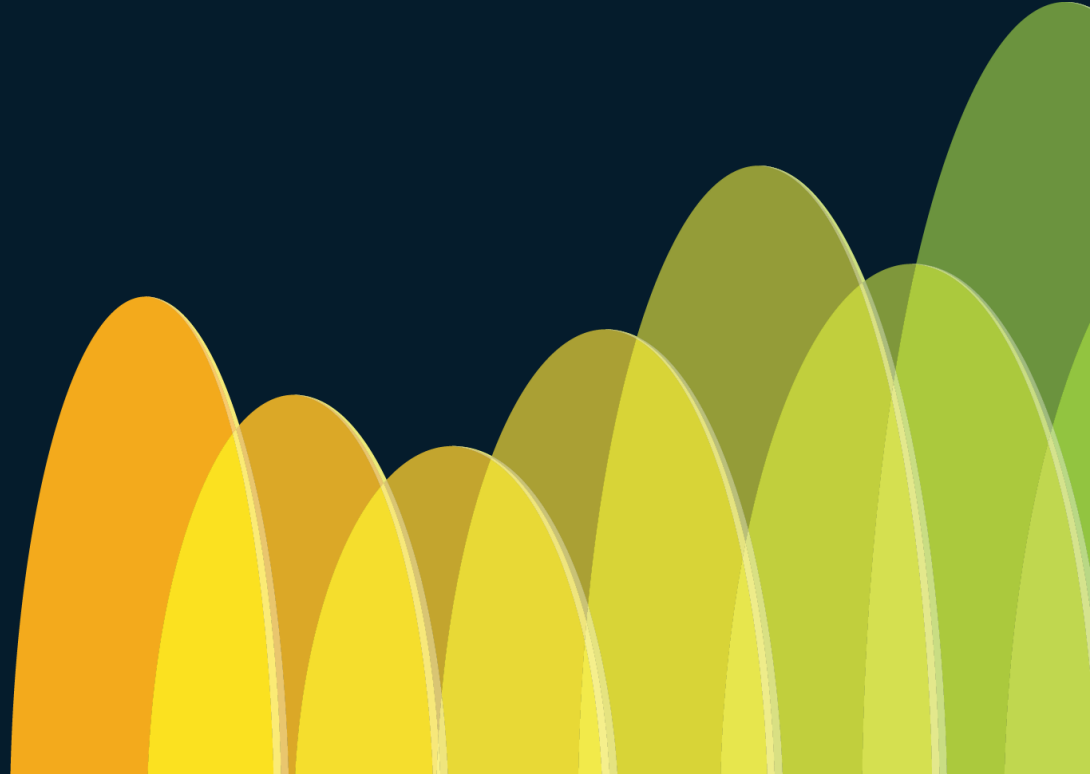
SAML for Single-Sign-On



SAML for Single-Sign-On



Example: Moving from RADIUS to SAML for SSO with VPN



FTD VPN SAML conversion

The screenshot shows the Cisco Duo Security web interface. The left sidebar contains navigation links: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Accounts, Billing, and Settings. The main content area is titled 'Applications' and shows the configuration for 'FTD ravpn01 - Single Sign-On'. It includes links for 'Authentication Log' and 'Remove Application'. A note directs users to the 'Cisco Firepower SSO documentation' for integration. The 'Metadata' section lists the Identity Provider Entity ID, SSO URL, and Logout URL, each with a 'Copy' button. The 'Downloads' section provides buttons to 'Download certificate' and 'Copy certificate', along with an expiration date of 'Expires: 01-19-2038'. The 'Service Provider' section contains input fields for the 'Cisco Firepower Base URL' (set to 'ravpn01.zerotrustdemo.com') and the 'Connection Profile Name' (set to 'ravpn').

admin-1a4ab80e.duosecurity.com/applications/DIG3UJWCYARPJ6CTFKT

Account Duo Security | Help | Jeff Groesbeck

← Applications

FTD ravpn01 - Single Sign-On

Authentication Log | Remove Application

See the [Cisco Firepower SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Identity Provider Entity ID <https://sso-1a4ab80e.sso.duosecurity.com/saml2/sp/DIG3UJWCYARPJ6CTFKT/me> [Copy](#)

SSO URL <https://sso-1a4ab80e.sso.duosecurity.com/saml2/sp/DIG3UJWCYARPJ6CTFKT/ssc> [Copy](#)

Logout URL <https://sso-1a4ab80e.sso.duosecurity.com/saml2/sp/DIG3UJWCYARPJ6CTFKT/slo> [Copy](#)

Downloads

Identity Provider Certificate [Download certificate](#) [Copy certificate](#) Expires: 01-19-2038

Service Provider

Cisco Firepower Base URL *
Enter the Cisco Firepower Base URL hostname.

Connection Profile Name *
Enter the Connection Profile Name you are protecting with SSO.

FTD VPN SAML conversion

The screenshot displays the Cisco Defense Orchestrator (FMC) Object Manager interface. The left sidebar shows navigation options: Home, Analysis, Policies, Devices, Objects (selected), and Integration. The main content area is titled 'Edit Single Sign-on Server' and contains the following fields:

- Name***: Duo_SSO
- Identity Provider Entity ID***: https://sso-1a4ab80e.sso.duose...
- SSO URL***: https://sso-1a4ab80e.sso.duose...
- Logout URL**: (empty)
- Base URL**: https://ravpn01.zerotrustdemo.c...
- Identity Provider Certificate***: Duo_SSO_new (+)
- Service Provider Certificate**: 2024_star_zerotrustdemo_com (+)
- Request Signature**: --No Signature--
- Request Timeout**: (empty)

At the bottom of the modal are 'Cancel' and 'Save' buttons. The background shows a table of Single Sign-on Servers with 4 rows, currently displaying the first row.

FTD VPN SAML conversion

The screenshot displays the Cisco Defense Orchestrator (FMC) Object Manager interface. The left sidebar shows navigation options: Home, Analysis, Policies, Devices, Objects (selected), and Integration. The main content area is titled 'Edit Single Sign-on Server' and contains the following fields and options:

- URL:** `https://sso-1a4ad8ue.sso.ouose...`
- Logout URL:** (Empty field)
- Base URL:** `https://ravpn01.zerotrustdemo.c...`
- Identity Provider Certificate*:** Duo_SSO_new (dropdown menu with a plus icon)
- Service Provider Certificate:** 2024_star_zerotrustdemo_com (dropdown menu with a plus icon)
- Request Signature:** --No Signature-- (dropdown menu)
- Request Timeout:** 300 (field with a note: seconds (1-7200))
- ☐ Enable IdP only accessible on Internal Network
- ☐ Request IdP re-authentication on Login
- ☐ Allow Overrides

At the bottom of the dialog are 'Cancel' and 'Save' buttons. The background interface shows a table of Single Sign-on Servers with columns for Name, Action, and a plus icon. The table displays 1 row of data. The bottom status bar indicates 'Displaying 1 - 4 of 4 rows' and 'Page 1 of 1'.

FTD VPN SAML conversion

The screenshot displays the Cisco Defense Orchestrator (FMC) interface for editing a VPN connection profile. The main window shows the 'Edit Connection Profile' dialog for a profile named 'ravpn'. The background interface includes a sidebar with navigation options: Home, Analysis, Policies, Devices (selected), Objects, and Integration. The top navigation bar shows 'FMC / Devices / VPN / Edit Connection Profile' and a search bar. The user is logged in as 'jgroesbe@cis.com'.

Edit Connection Profile

Connection Profile: ravpn

Group Policy: DfitGrpPolicy [Edit Group Policy](#)

Client Address Assignment: [AAA](#) [Aliases](#)

Authentication

Authentication Method: SAML

Authentication Server: Duo_SSO (SSO)

☐ Override Identity Provider Certificate ⓘ

SAML Login Experience:

- ☒ VPN client embedded browser ⓘ
- ☐ Default OS Browser ⓘ

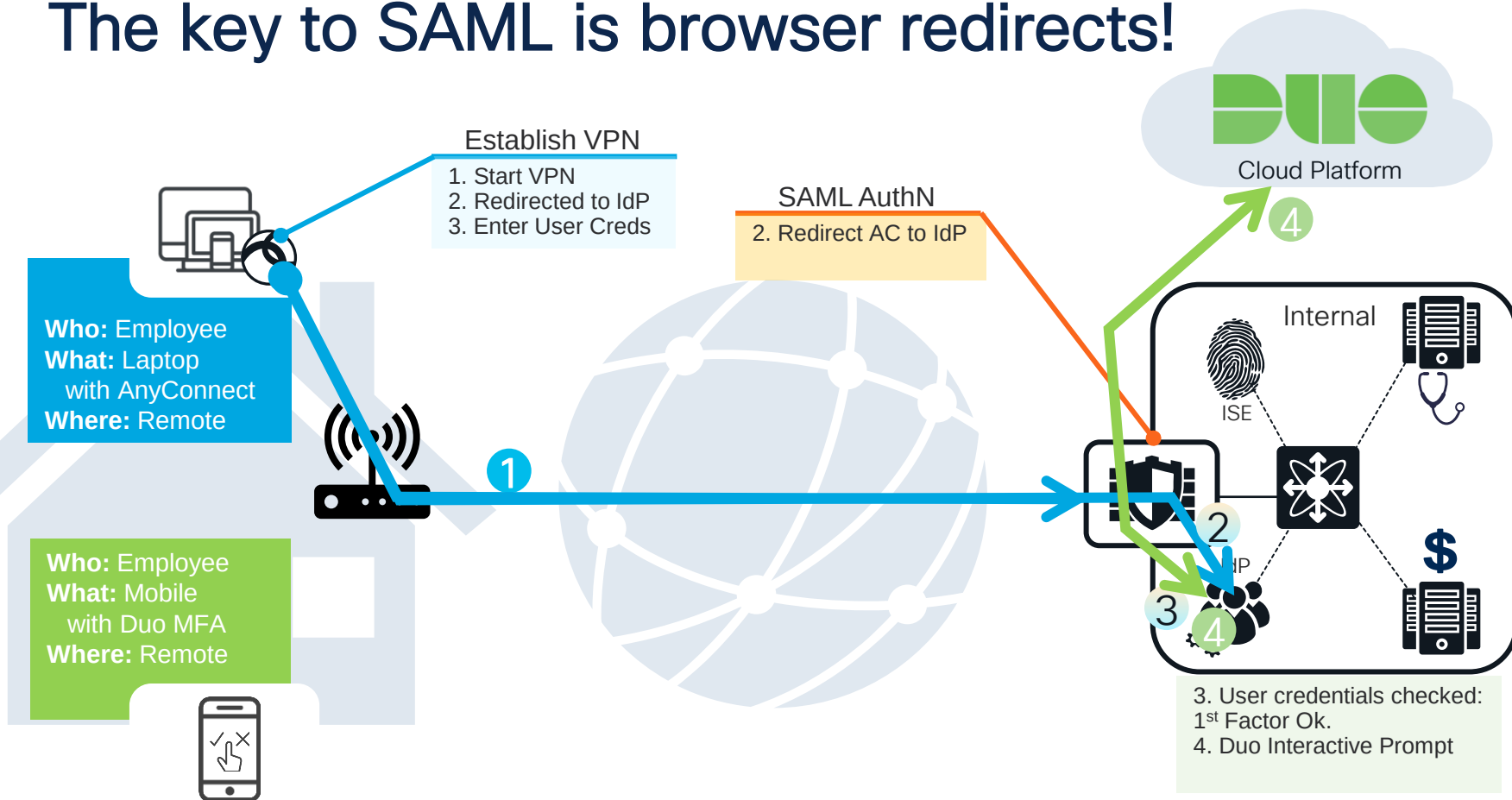
Authorization

Authorization Server: ise-authz (RADIUS)

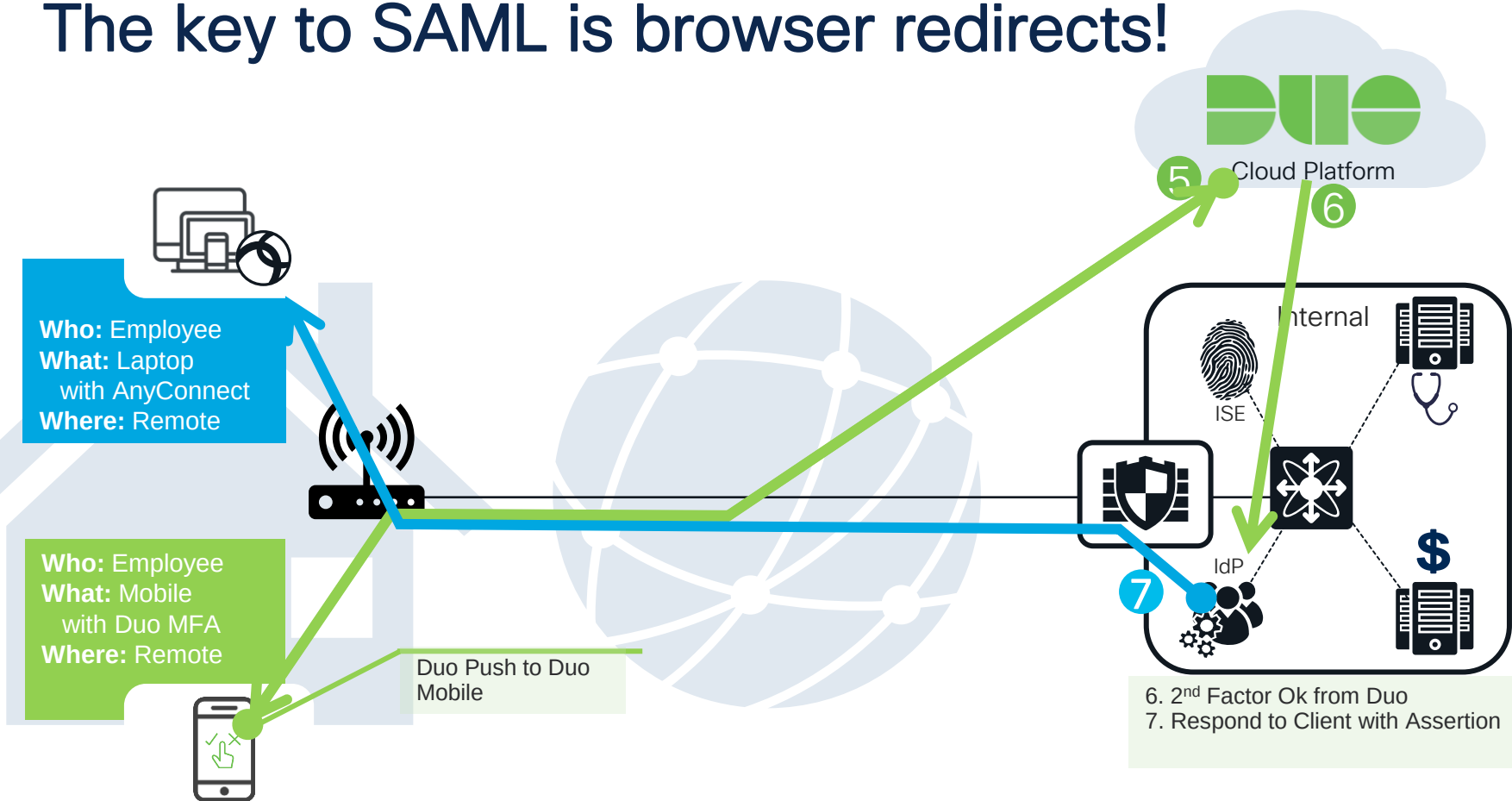
☐ Allow connection only if user exists in authorization database

[Cancel](#) [Save](#)

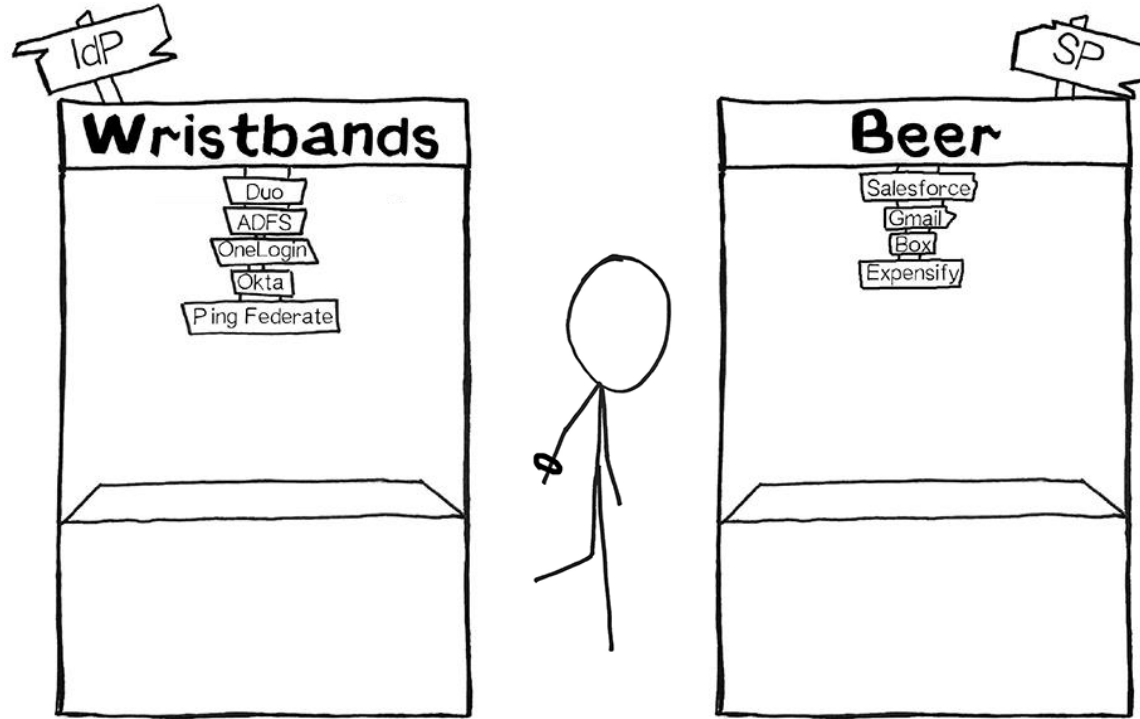
The key to SAML is browser redirects!



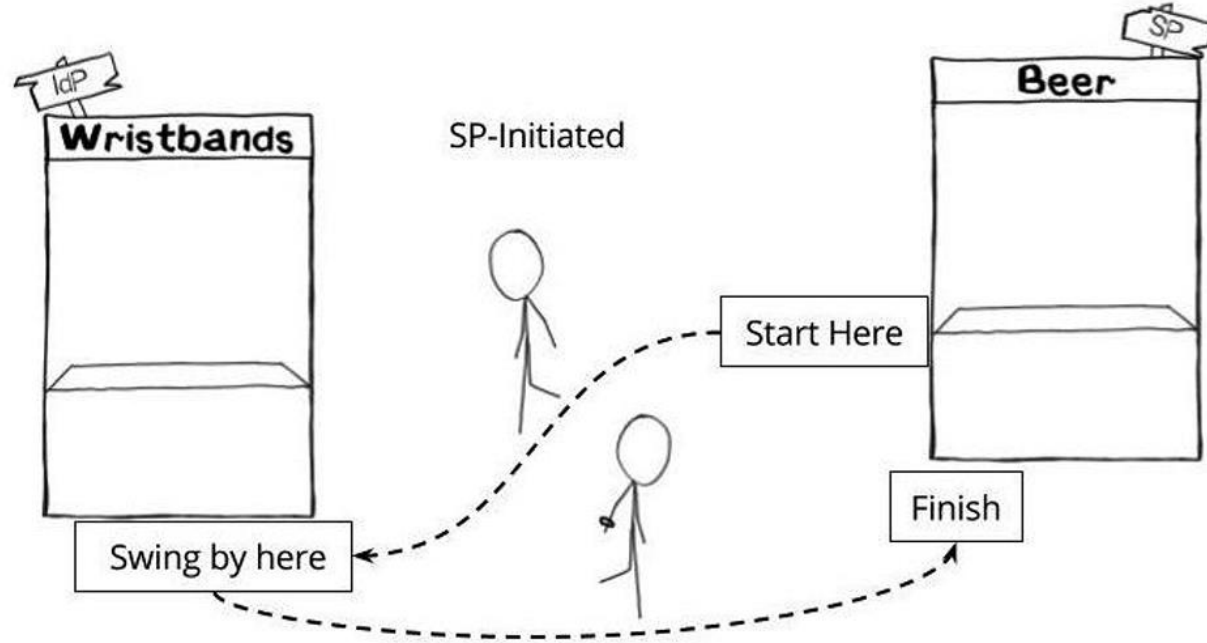
The key to SAML is browser redirects!



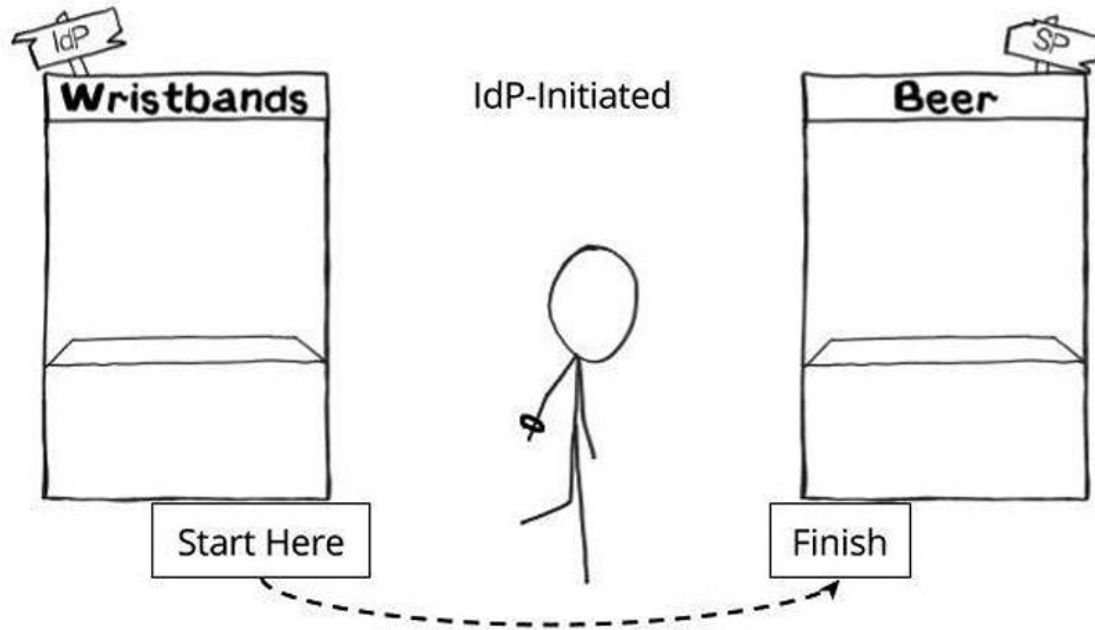
The Beer Drinker's Guide to SAML



The Beer Drinker's Guide to SAML



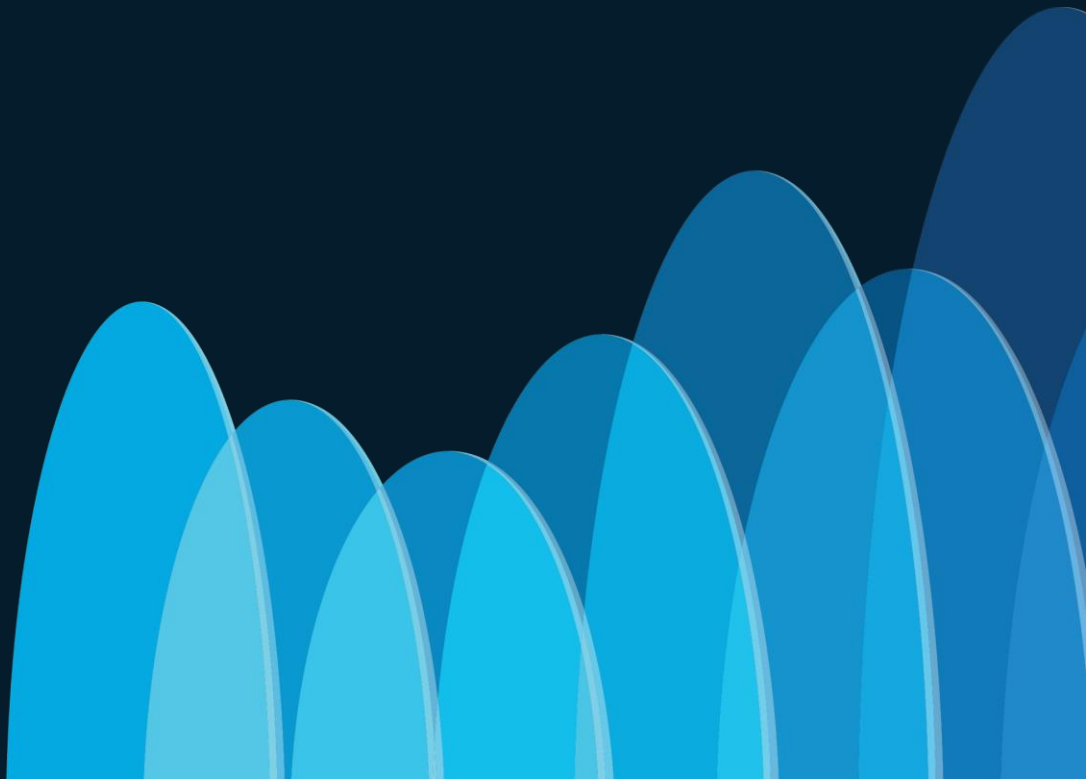
The Beer Drinker's Guide to SAML



Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

OAuth2

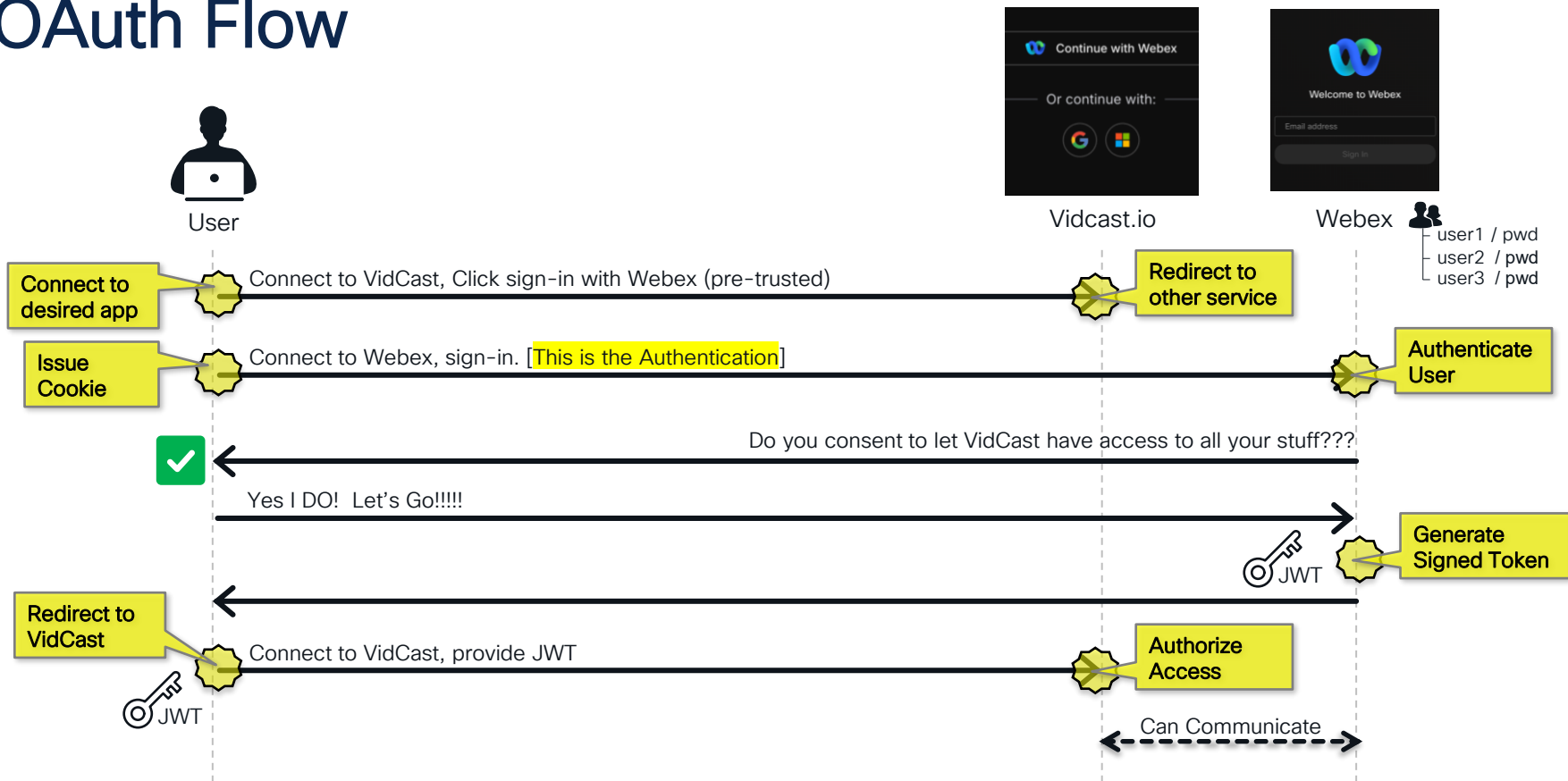


OAuth 2.0 is a security standard where you give one application permission to access your data in another application

Open Authorization v2 (OAuth2)

- Open Standard
 - Token exchange protocol
 - Originally meant for application to application, authorized by a user.
 - User authorizes the application. IdP issues a token (JSON Web Token) to the app, allowing the app to make API calls on behalf of the user.

OAuth Flow



Example of Consent

Sign in with Google



Sign in to Cisco Webex Social Login

L loxx@securitydemo.net ▼

By continuing, Google will share your name, email address, language preference, and profile picture with Cisco Webex Social Login. See Cisco Webex Social Login's [Privacy Policy](#) and [Terms of Service](#).

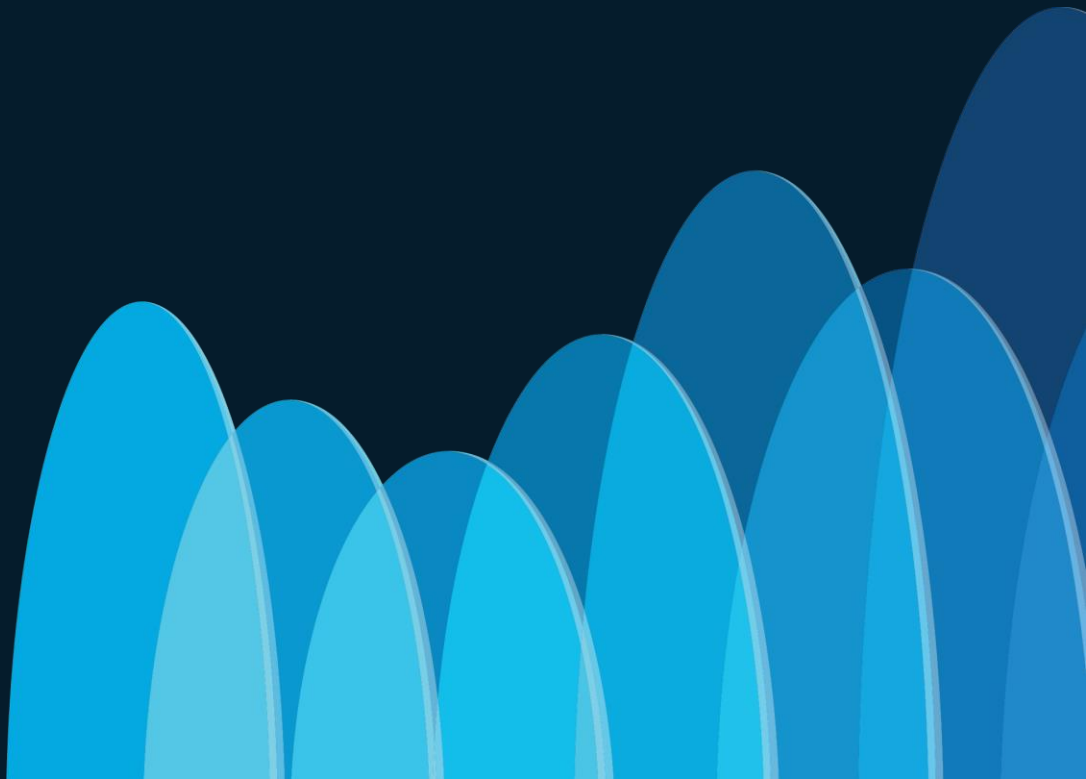
You can manage Sign in with Google in your [Google Account](#).

Cancel Continue

English (United States) ▼

Help Privacy Terms

Open ID Connect (OIDC)

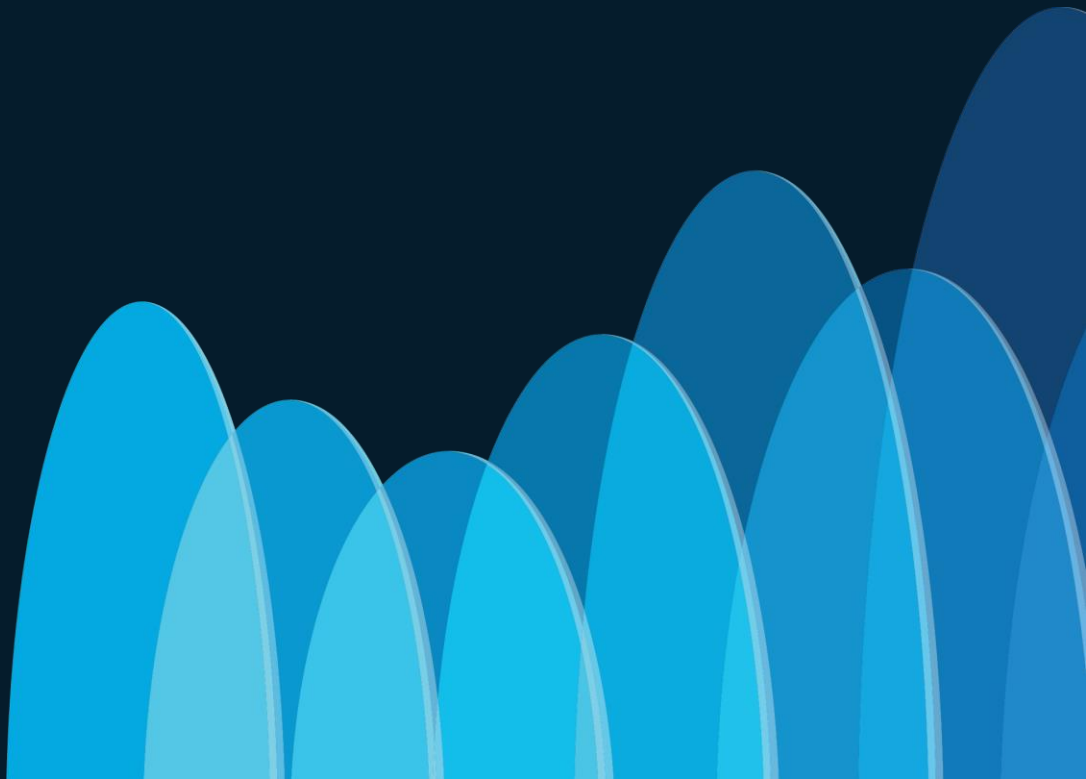


OIDC is a thin layer that sits **on top** of OAuth 2.0 to add login and profile information about the user into the exchange. This transforms the exchange to both **authorization** and **authentication**!

Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

Web Authentication



Web Authentication (WebAuthN)

- An API websites use to talk to web browsers
- An API spec for accessing public key credentials
- Developed by FIDO Alliance, ratified by the W3C
- Manages both registration and authentication
- Can be used for primary or secondary authentication

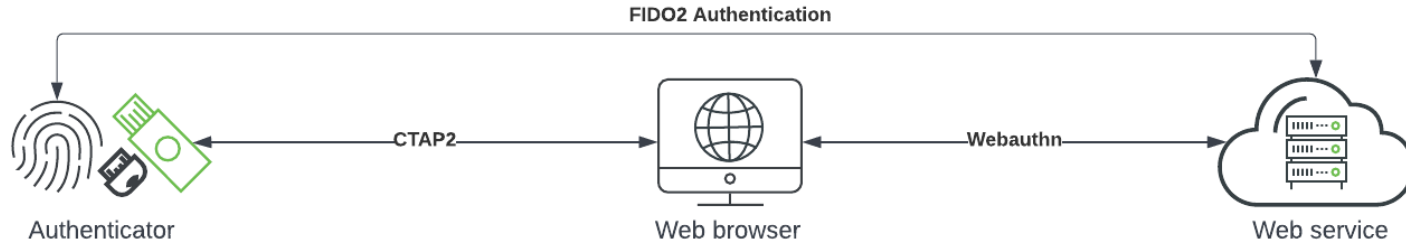


[WebAuthn.io](https://webauthn.io)

FIDO2 Authentication



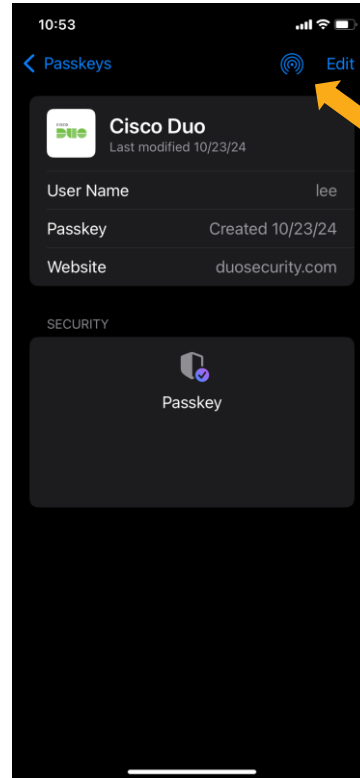
- Developed by FIDO alliance
- WebAuthN + Client to Authenticator Protocol v2 (CTAP2)
- CTAP: API for browser to authenticator communication
- Can be used for MFA or password-less



Passkeys

- Passkeys are essentially just a new (and easier) name for WebAuthn + FIDO2 credentials
- Passkeys, however, don't have to just be device bound
- Shared passkeys make things a whole lot easier for end users
 - Credentials can be synced using secure methods (icloud keychain/passwords app, Google password manager, etc)
- There 'may' be security concerns with sharing.... Think personal icloud account across possibly work AND personal device
- AND...

Shared Passkeys



Airdrop!

To ANYONE!

Authentication

Authenticator



Private Key

Browser



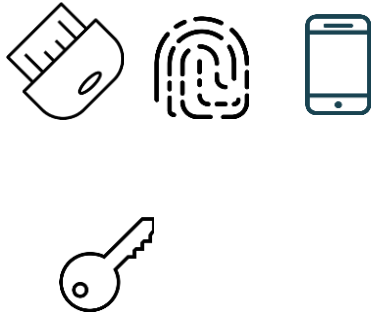
User Bob

Web Server



Authentication : Send User Info

Authenticator



Browser



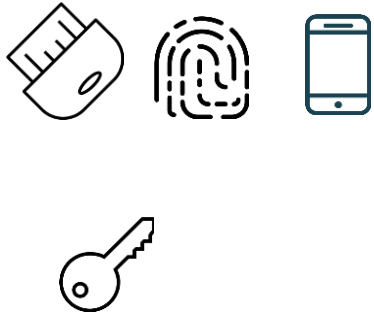
User Bob

Web Server



Authentication : Challenge

Authenticator

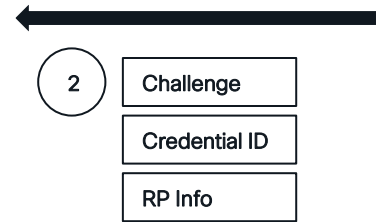


Browser



User Bob

Web Server

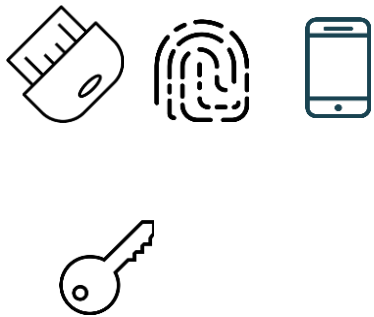
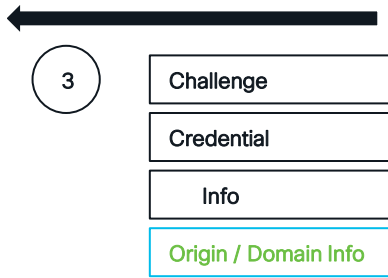


Authentication : Challenge + Domain

Authenticator

Browser

Web Server

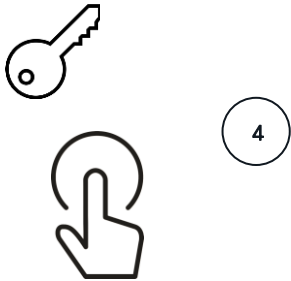


User Bob



Authentication : User Verification

Authenticator



CISCO *Live!*

User Verification

Perform Biometric

Security Key Gesture

Mobile Push

Browser



User Bob

Web Server



Authentication : User Verification & Assertion

Authenticator

Browser

Web Server



4

Signed Assertion



User Bob

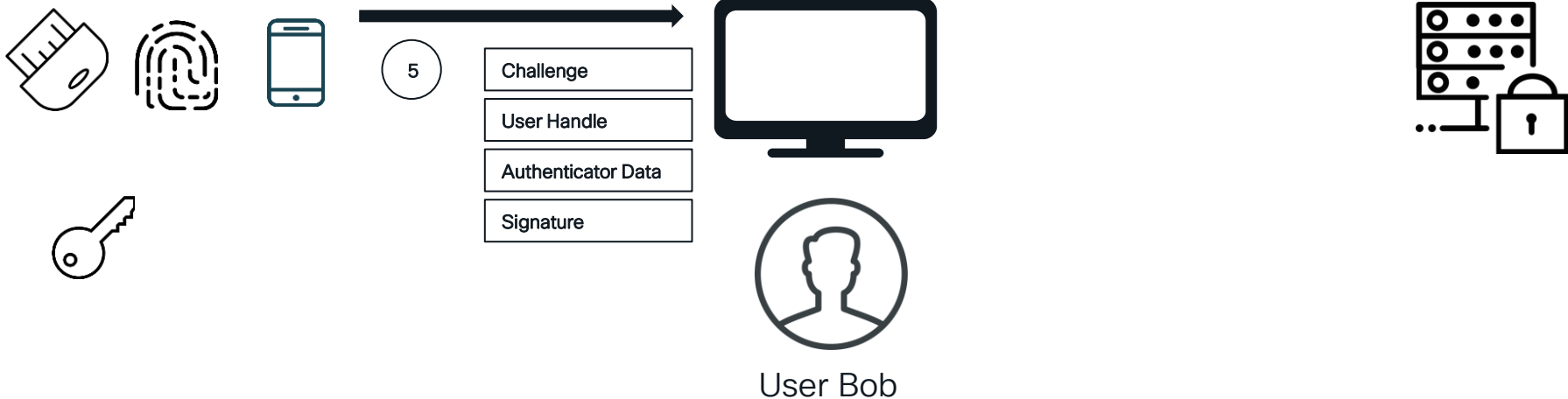


Authentication : Authenticator Assertion

Authenticator

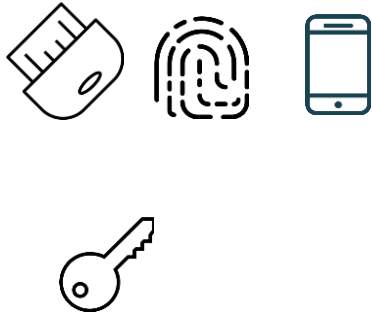
Browser

Web Server



Authentication : Challenge Response

Authenticator

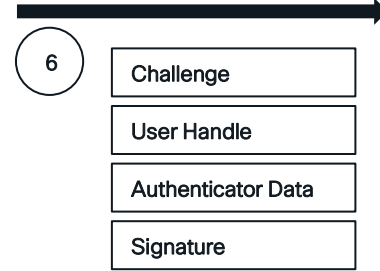


Browser



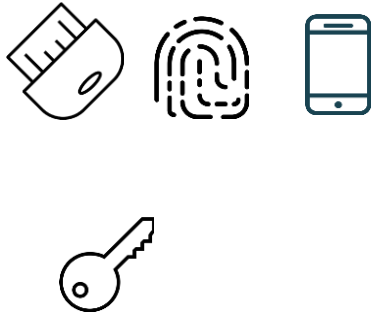
User Bob

Web Server



Authentication : Success!

Authenticator



Browser



User Bob

Web Server



7

Verify Signature

Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

Gotcha's (it's not all Sunshine & Roses)





Long Live the King: RADIUS

- With RADIUS: there was structure:
- Attribute Value Pairs (AVPs)
 - i.e.: User-Name: [username]
 - The RADIUS server knew what to expect
 - It could be extended with Vendor Specific Attributes (VSAs).

```
▼ Attribute Value Pairs
  ▸ AVP: l=24  t=User-Name(1): host/winxp.example.com
  ▸ AVP: l=6   t=Service-Type(6): Framed(2)
  ▸ AVP: l=6   t=Framed-IP-Address(8): 192.168.2.100
  ▸ AVP: l=6   t=Framed-MTU(12): 1500
  ▸ AVP: l=19  t=Called-Station-Id(30): 00-1A-A2-7E-7F-03
  ▸ AVP: l=19  t=Calling-Station-Id(31): 00-16-D4-2E-E8-BA
  ▸ AVP: l=89  t=EAP-Message(79) Last Segment[1]
  ▸ AVP: l=18  t=Message-Authenticator(80): 1a71a57045f7ea6
  ▸ AVP: l=2   t=EAP-Key-Name(102):
  ▸ AVP: l=49  t=Vendor-Specific(26) v=Cisco(9)
  ▸ AVP: l=6   t=NAS-Port-Type(61): Ethernet(15)
  ▸ AVP: l=6   t=NAS-Port(5): 50001
  ▸ AVP: l=17  t=NAS-Port-Id(87): FastEthernet0/1
  ▸ AVP: l=74  t=State(24): 333743504d53657373696f6e49443d4
  ▸ AVP: l=6   t=NAS-IP-Address(4): 192.168.1.60
```

SAML / OAuth

- SAML & OAuth: part of the Token but can have many different schemas
- Must program each side to know what field is
- Dictate the schema via URL
 - Ex: Use “email” as username

! – Example: XDR UI App OAuth Token

```
{
  "https://schemas.cisco.com/iroh/identity/claims/user/email": "loxx@securitydemo.net",
  "https://schemas.cisco.com/iroh/identity/claims/user/idp/id": "sxso",
  "https://schemas.cisco.com/iroh/identity/claims/user/nick": "Aaron Woland",
  "email": "loxx@securitydemo.net",
  "aud": [
    "iroh-ui",
    "login"
  ],
  "https://schemas.cisco.com/iroh/identity/claims/user/role": "admin",
  "sub": "9992027f-a88b-4b0e-8a38-58ad317c58af",
  "iss": "IROH Auth",
  "https://schemas.cisco.com/iroh/identity/claims/scopes": [
    "event:read",
    "cisco/feature-flag/xdr",
    "insights",
    "vault/configs:read",
    "integration",
    "private-intel",
    "admin",
    "profile",
    "inspect",
    "asset",
    "ao"
  ],
  "exp": 1731003921,
  "https://schemas.cisco.com/iroh/identity/claims/oauth/client/name": "Threat Response",
  "https://schemas.cisco.com/iroh/identity/claims/oauth/user/id": "9992027f-a88b-4b0e-8a38-58ad317c58af",
  "https://schemas.cisco.com/iroh/identity/claims/org/id": "2e0e9eaf-eaf7-4449-9c07-9fb1828aec78",
  "https://schemas.cisco.com/iroh/identity/claims/oauth/grant": "login",
  ! - SNIP
}
```

Lack of Standards / Easy Behaviors

Example is Auth0, a CIAM

Integrating to a SAML IdP, it requires me to write this mapping out manually.

- Define which schema to figure out email.
- Define which attribute to use to find groups.

← Back to SAML

Aaron's Duo SSO

SAML Identifier `con_aRGGNZCr9ZENiCFz`

Settings Provisioning **Mappings** IdP-Initiated SSO Login Experience Setup Applications

These are the attributes in the SAML token that will be mapped to the user properties in Auth0. The format of the mappings are:

- **Simple mapping:** "auth0_user_attribute": "incoming_saml_attribute"
- **Multiple options mapping:** "auth0_user_attribute": ["incoming_saml_attribute1", "incoming_saml_attribute2", "etc.,"]

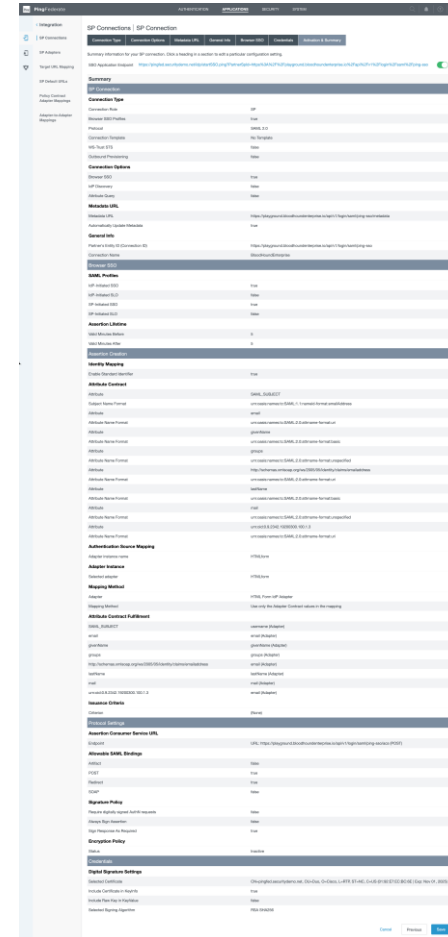
```
1 {
2   "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
3   "groups": "memberOf"
4 }
```

[Show full mappings example](#)

[Save Changes](#)

CISCO *Live!*

- 101



Lack of Standards / Easy Behaviors

Some Vendors try to make it easier (ahem: Duo)

- Supported schemas are selectable via a drop down.

Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

SAML Response

NameID format *

The format that specifies how the NameID is sent to the service provider.

NameID attribute *

NameID is a SAML attribute that identifies the user. Enter an IdP attribute or select a bridge attribute that automatically chooses the NameID attribute based on the IdP. Create custom attributes by clicking the plus icon. Supported attributes: <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name>.

Signature algorithm *

Signature encryption algorithm used in the SAML assertion and response.

Signing options * ☒ Sign response ☒ Sign assertion

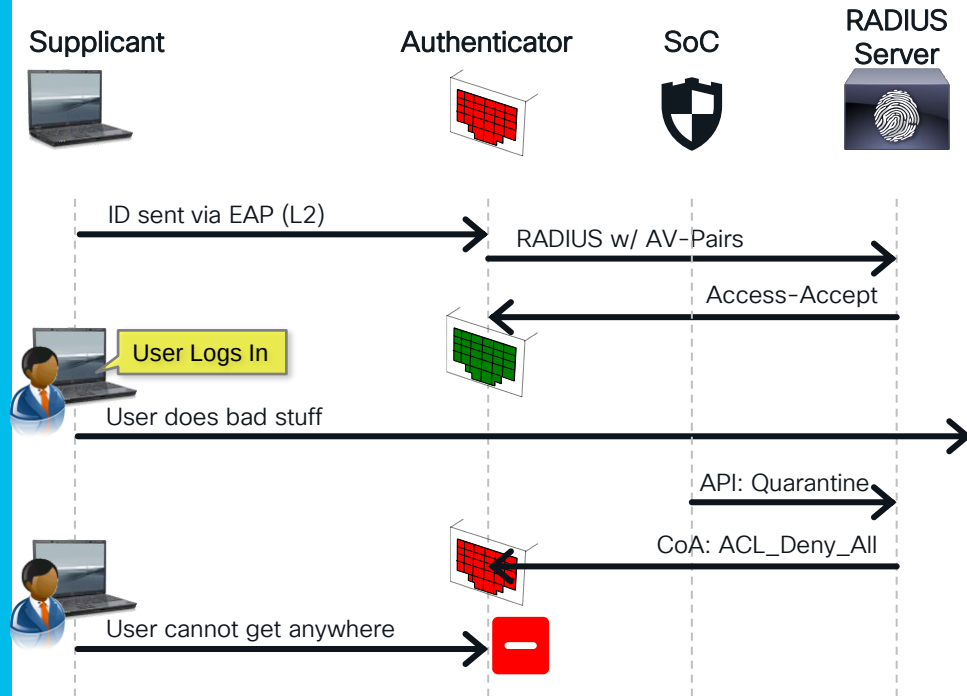
Choose at least one option for signing the SAML response. Your service provider will use these to verify the response's authenticity.

Assertion encryption ☐ Encrypt the SAML assertion

Change of Authorization (CoA)

Described in **RFC 3576** and its successor **RFC 5176**

- Allows RADIUS server to disconnect or force other change in the authorization status of a user/endpoint.
- Disconnect
- Port-bounce
- Re-Authenticate
- Apply ACL



Continuous Authorization Evaluation Protocol (CAEP)

- Designed for real-time access control adjustments
 - i.e: Change of Authorization
- Meant to overcome the AuthN once & AuthZ until token expires problem

Shared Signals

- Enables sharing of security-related information across different services or systems
 - Kind of like STIX, but not.
 - Because we have to re-invent everything in Web AAA
- Used with CAEP for identity-related security events

Requires Human Interaction

- SAML, OAuth & OIDC
 - Are interactive
 - Require someone to click objects, or input usernames to obtain the token.
 - Makes coding scripts more tricky
 - Think: Python script to automate certain actions
 - Once you have the Token it's easy, but how do you get it via script?

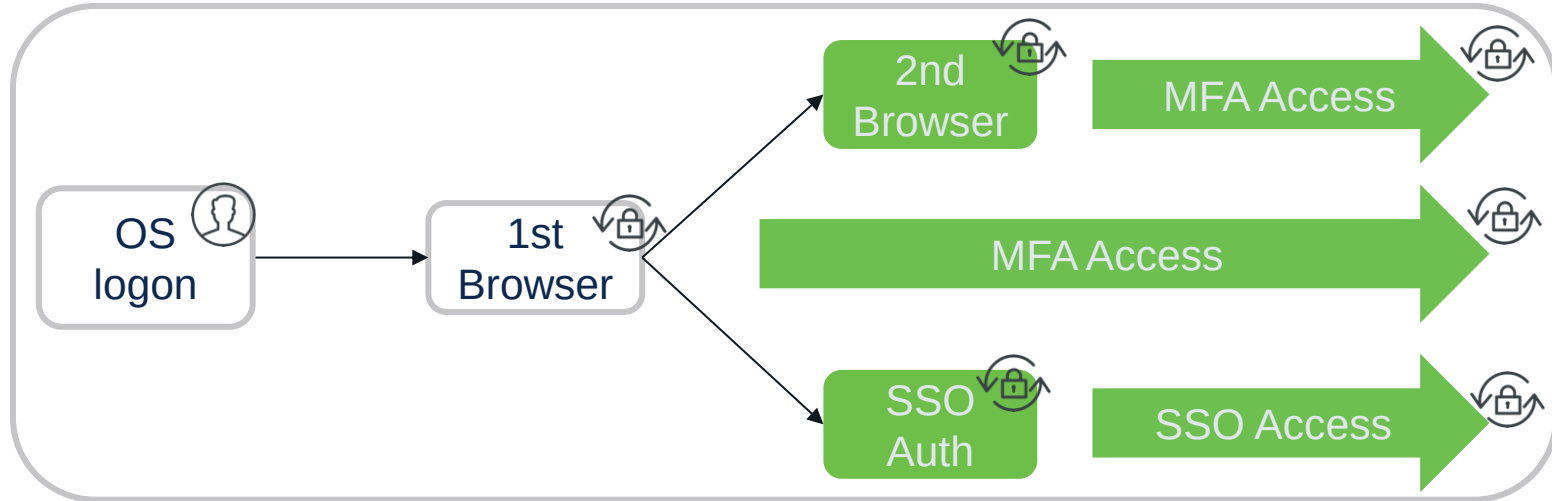
Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

Identity's Future
is so bright, it
needs shades!



Login Once, Access Everything Securely



Duo Desktop

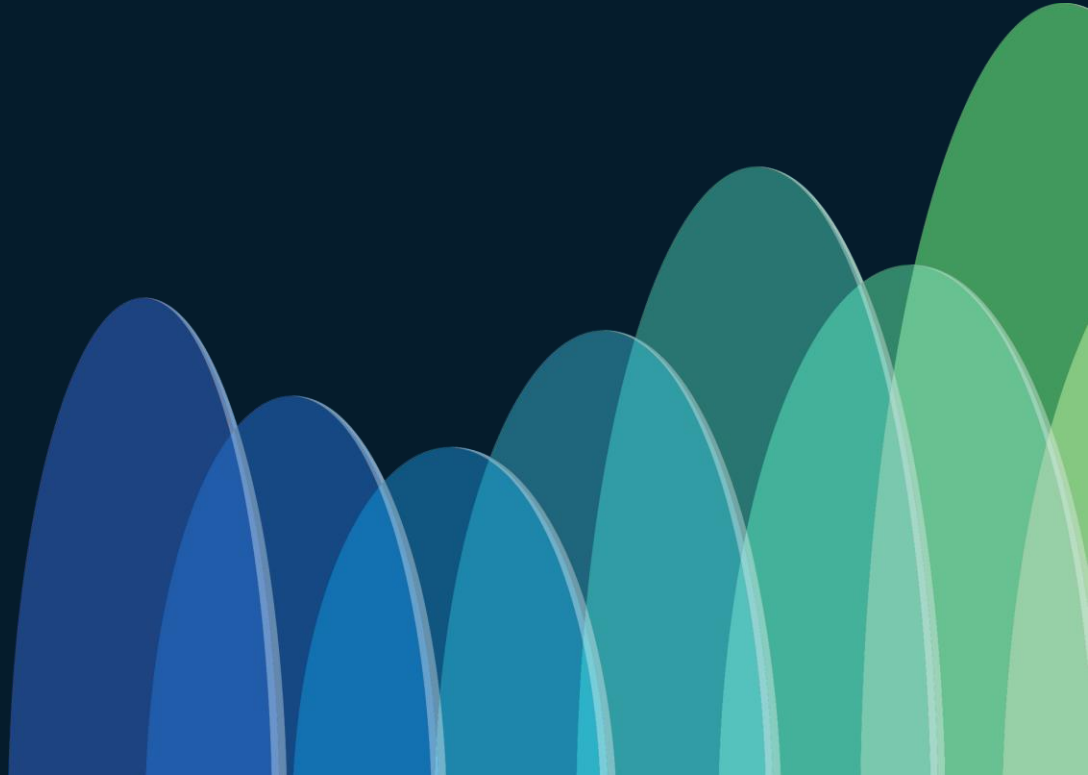
Granular Policy Coverage

High Security, Low Friction Auths: Device Posture and RBA

	Interactive authentication - end user friction
	Authentication brokered through device, Duo, and Duo Desktop

Remembered device
session border

Demo Video: Complete Single Sign On with Duo Passport





Lee

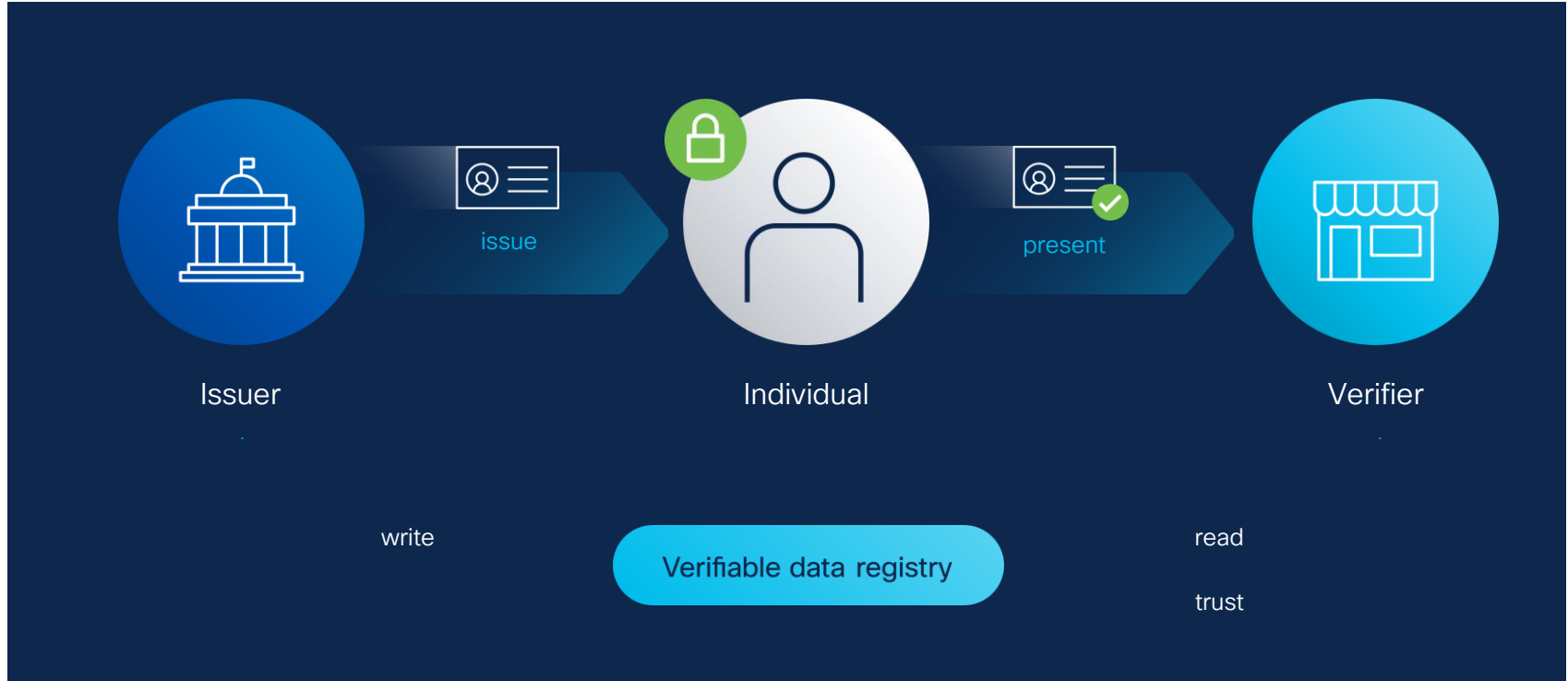
Sign in



Lee



Verified Identity- High level flow diagram



Identity Governance and Administration (IGA)

- IGA is the central point where entitlements (who can access what) are managed
- Managing entitlements has both security and compliance impact

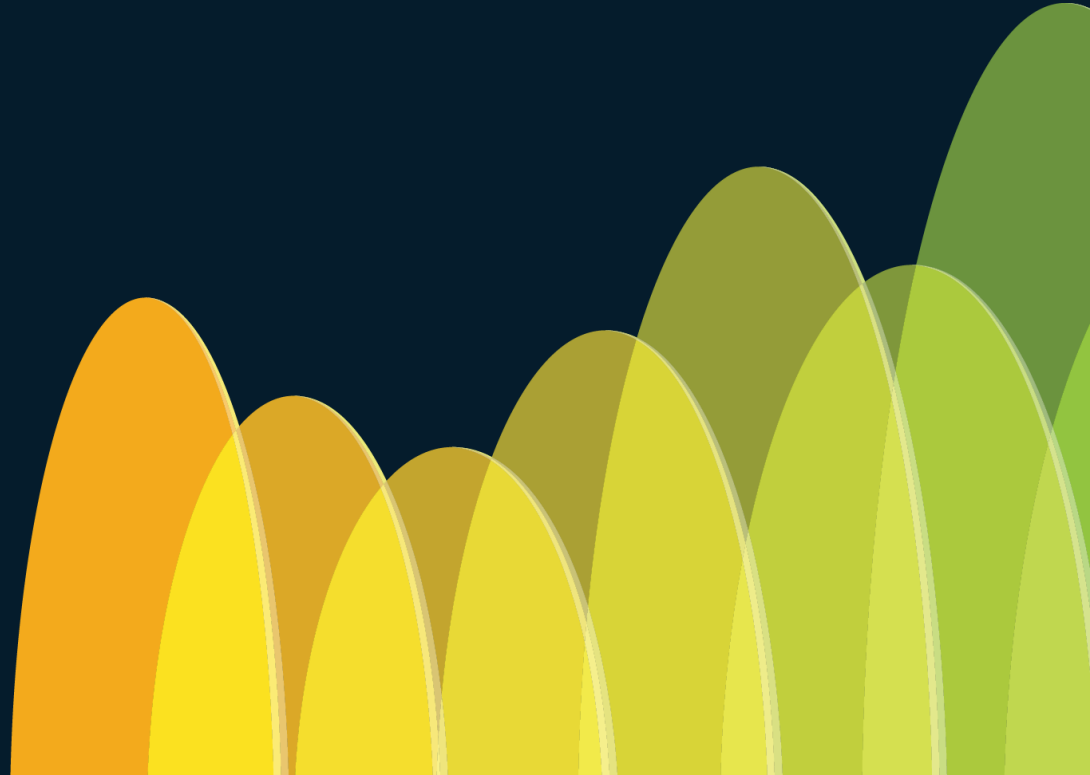
Cookie-less SSO

- Session Hijacking is a real attack vector
 - Bad guy sits between user & SP (the app)
 - App sends user the cookie
 - Bad guy copies those cookies & now uses the cookie to access the app “as the user”
- Removing cookies from the process, session hijacking becomes thing of the past
 - Duo will have cookie-less SSO w/ Duo Passport

Agenda

- Introduction
- History & AAA
- Enter: Single Sign On
- SAML
- OAuth & OIDC
- WebAuthN & Passkeys
- Gotcha's
- ID Needs Shades in Future
- Conclusion

Conclusions



Conclusions

- AAA is a basic security principle that is just as relevant today as it was 20 years ago.
- SAML & OIDC are for Single Sign On, while OAuth is for Application Authorization
- WebAuthN is more than just webauth in networking
- Passkeys are here, Passwordless is here – use them!
- Duo makes Identity Easy and Secure
- You had fun in this session, even though the topic is boring

Good Links

- Shibboleth Consortium: <https://www.shibboleth.net/index/>
- OASIS: <https://www.oasis-open.org>
- Beer Drinkers Guide to SAML: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>
- Fighting Cookie Theft: <https://blog.chromium.org/2024/04/fighting-cookie-theft-using-device.html>
- A demo of Webauthn and Passkeys: <https://webauthn.io>

Please fill out the survey



Drop your email in the comments – we WILL respond!

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



- Visit the Cisco Stand 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

Other Sessions

- Here at Cisco Live
 - Identity Intelligence Demystified [BRKSEC-2162]
Aaron Woland, Thursday 8:00am
 - Duo Identity Security: Protect your users and applications with MUCH more than MFA [CISCOU-2040]
Jeff Groesbeck, Thursday 11:15am in World of Solutions
- On Demand Sessions
 - Taking Authentication to the Next Level with Duo Security [BRKSEC-2584] (Stefan Duernberger)
 - Demystifying the World of Passkeys [BRKSEC-2202] (Clayton Ballreich)



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC