Modern Auth & SSO for Networkers

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

Aaron T. Woland, CCIE #20113
Distinguished Engineer, Identity Security

loxx@cisco.com | @aaronwoland | aaronwoland

BRKSEC-2144

Cisco Webex App

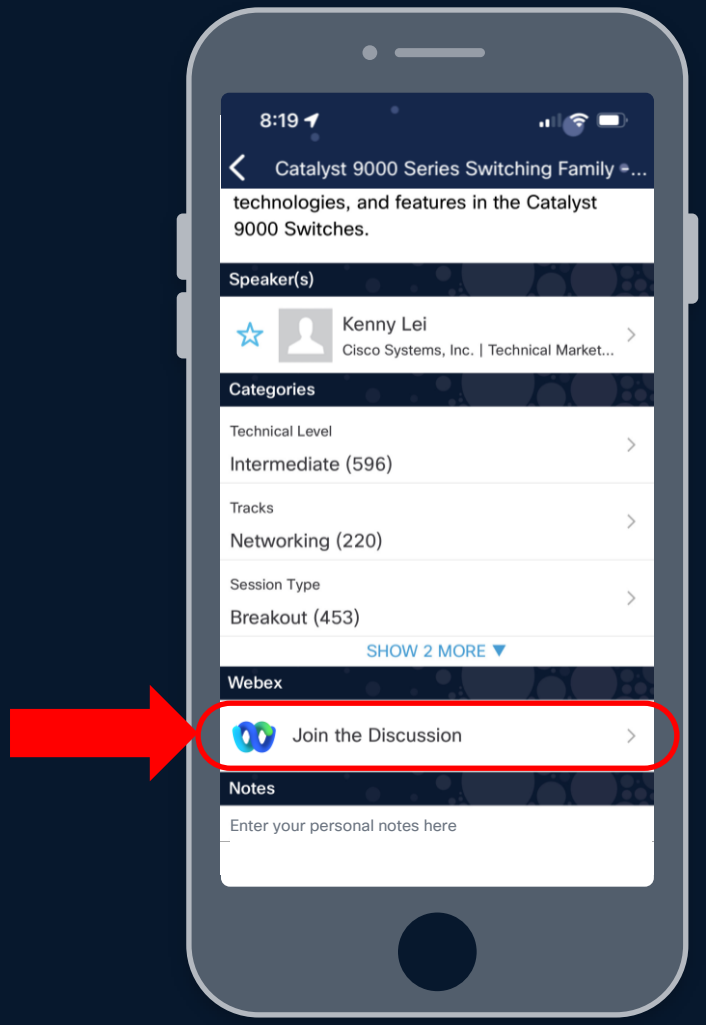
Questions?

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 13, 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/#BRKSEC-2144

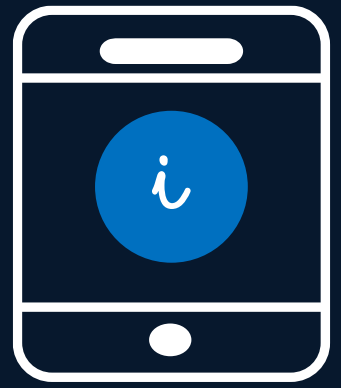
© 2025 Cisco and/or its affiliates. All rights reserved.

Important: Hidden Slide Alert

This deck has more information in it than I can present in the time allotted for this session.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Please fill out the Survey

If there is anything we can improve, please let us know!

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction

02 History & AAA

03 Enter: Single-Sign-On

04 SAML

05 OAuth & OIDC

06 WebAuthN & Passkeys

07 Gotcha's

08 Identity Security's Bright Future

09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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

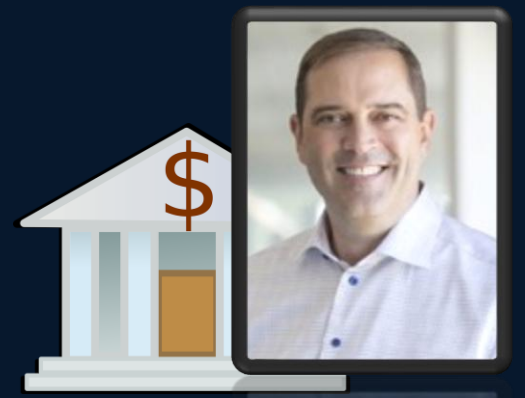
© 2025 Cisco and/or its affiliates. All rights reserved.

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

- Aaron T Woland, pompous windbag

© 2025 Cisco and/or its affiliates. All rights reserved.

AAA



I'd like 40K from Chuck Robbins' Account

Do You Have Identification?

Yes, I Do. Here It is:

Authentication

Sorry, Aaron Woland is not Authorized to Chuck Robbins' Account

Authorization

Accounting

© 2025 Cisco and/or its affiliates. All rights reserved.

AAA in a “networking world”

- In “our” world, we have thought of 2-types of AAA:
  - Controlling access to networks.
    - Dial-up (yes, I’m that old)
    - 802.1X
    - Remote Access VPN
  - Or access to our terminals / CLI’s
    - I.e.: TACACS+
- Basically, we want to know who and what is connecting to your network or CLI before granting access, and let that access be specific.

© 2025 Cisco and/or its affiliates. All rights reserved.

Network access AAA

ISE is sort of like the “airport security” of the network, if you will.

AuthN

- 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

AuthZ

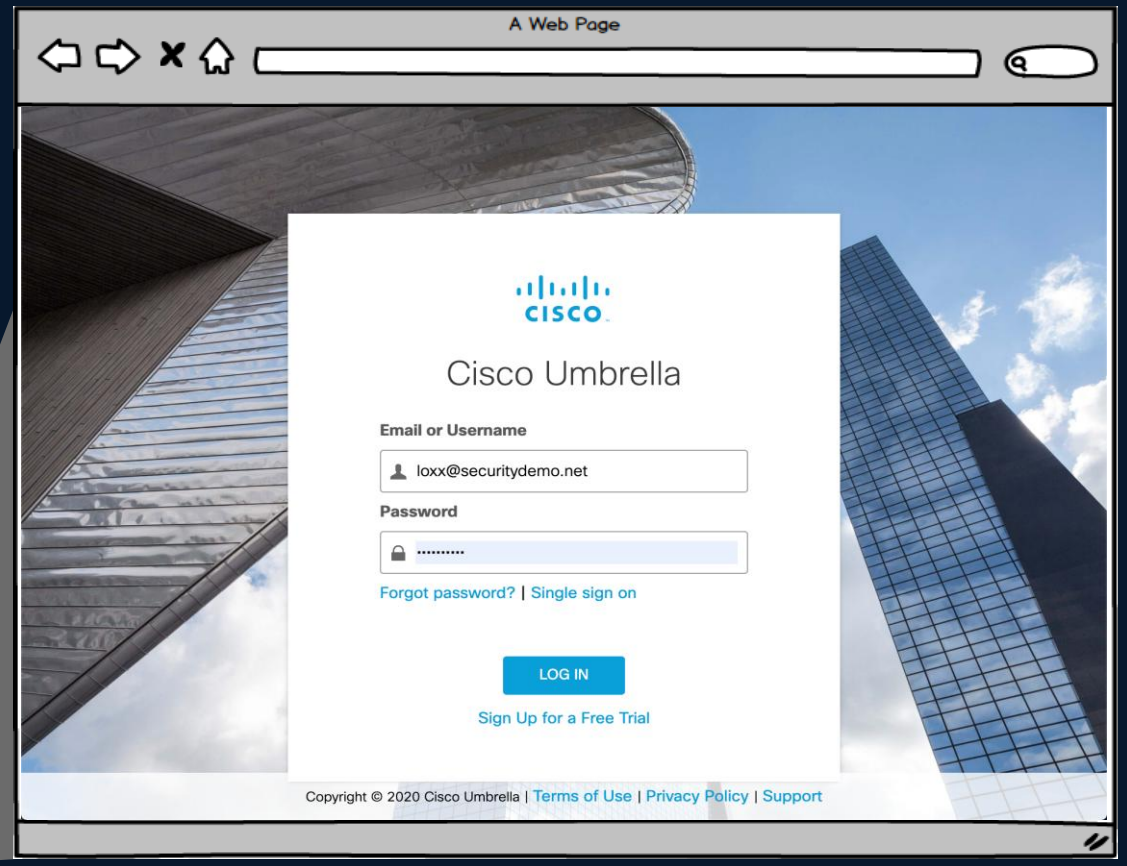
- It validates the device is allowed
  - Is it an allowed type (Profile)
  - Does it meet the security requirements (Posture)

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Application Access

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



© 2025 Cisco and/or its affiliates. All rights reserved.

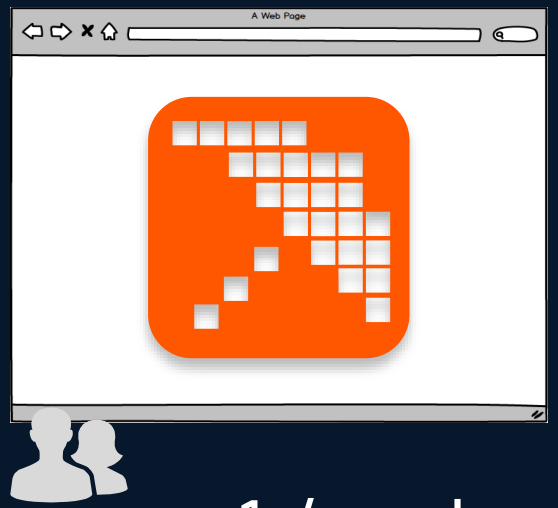
Application Access

- 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

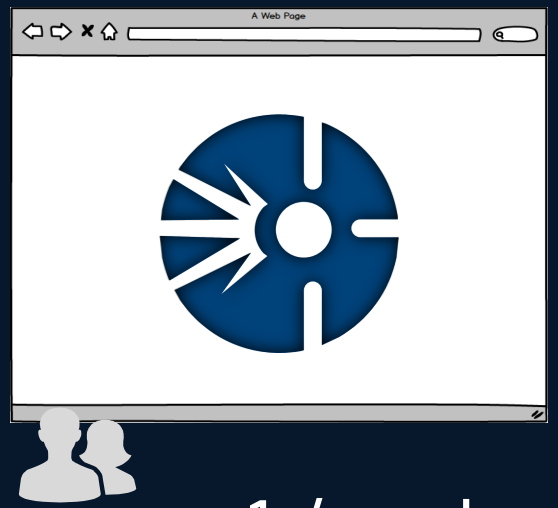
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

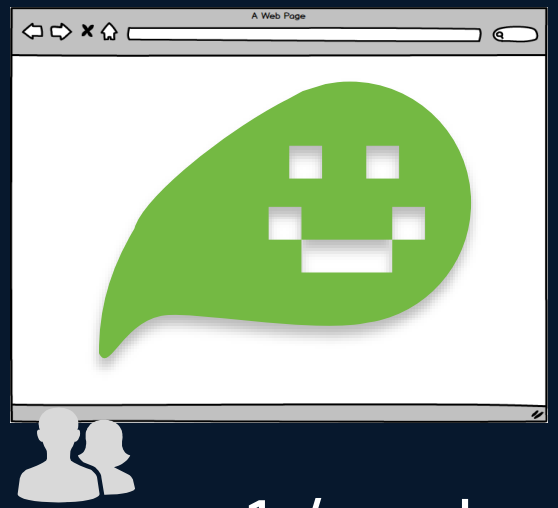
Apps could maintain its own User DB



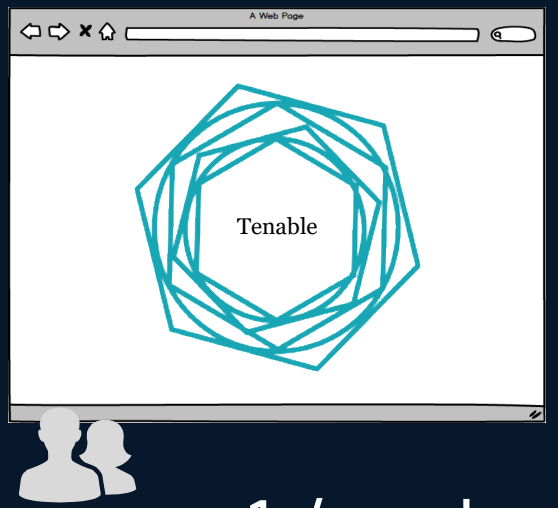
user1 / pwd
user2 / pwd
user3 / pwd



user1 / pwd
user2 / pwd
user3 / pwd



user1 / pwd
user2 / pwd
user3 / pwd



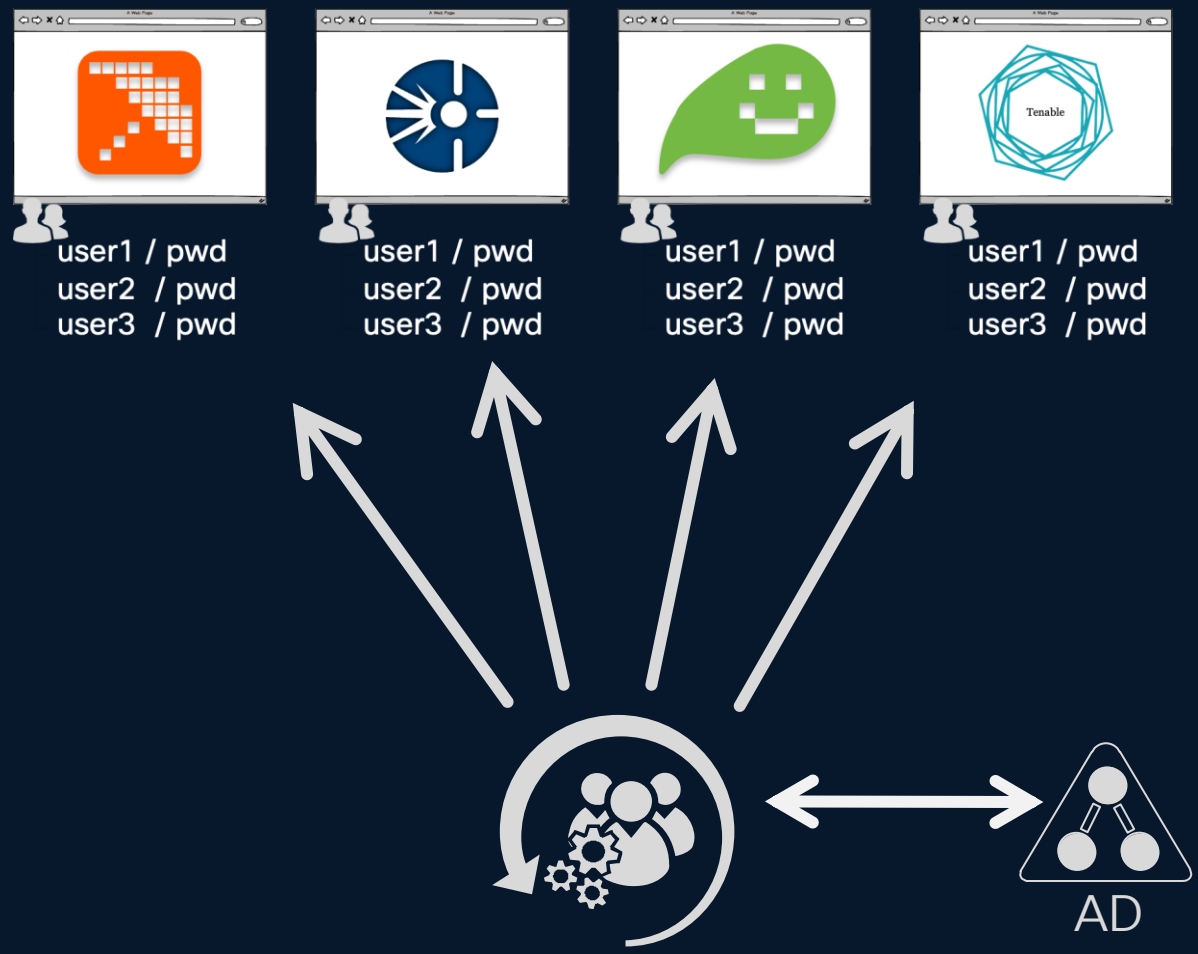
user1 / pwd
user2 / pwd
user3 / pwd

Note: this is not the case for many NEW apps, they rely on the Identity Provider for everything. No local user database. CII (aka: Oort) is an example.

© 2025 Cisco and/or its affiliates. All rights reserved.

Enter: Identity Management Products

- Solution to keep all user accounts & passwords in sync – across all these web apps.
  - Examples:
  - Tivoli Identity Manager
  - Oracle Identity Manager
  - Etc…



© 2025 Cisco and/or its affiliates. All rights reserved.

Example of what an ID Lifecycle Manager 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*

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

© 2025 Cisco and/or its affiliates. All rights reserved.

System for Cross-domain Identity Management

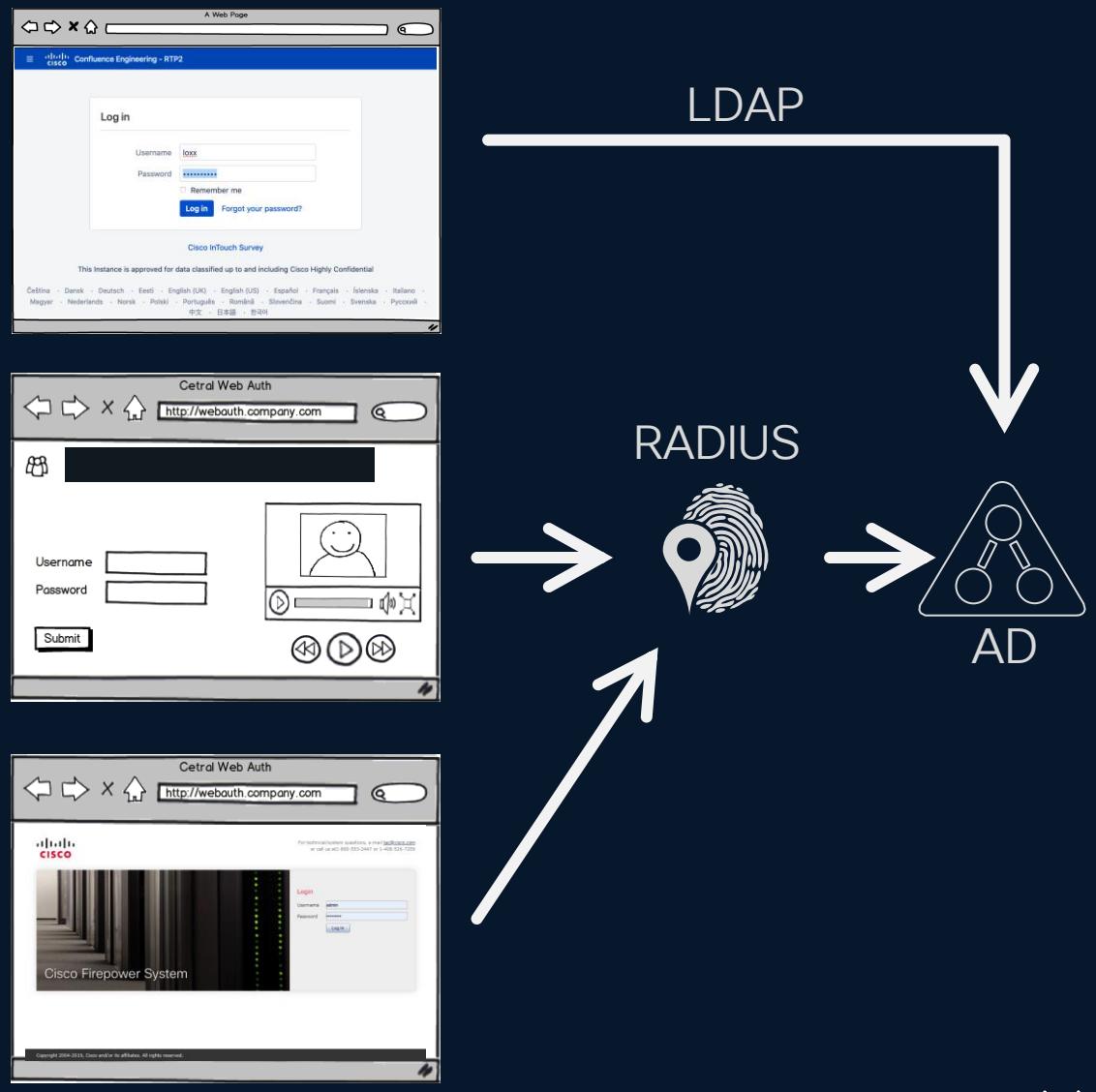
SCIM = standard for automating the exchange of user identity information between identity systems.

Aaron likes to equate it to an LDIF export & import in LDAP

© 2025 Cisco and/or its affiliates. All rights reserved.

Some tried RADIUS or LDAP logins

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

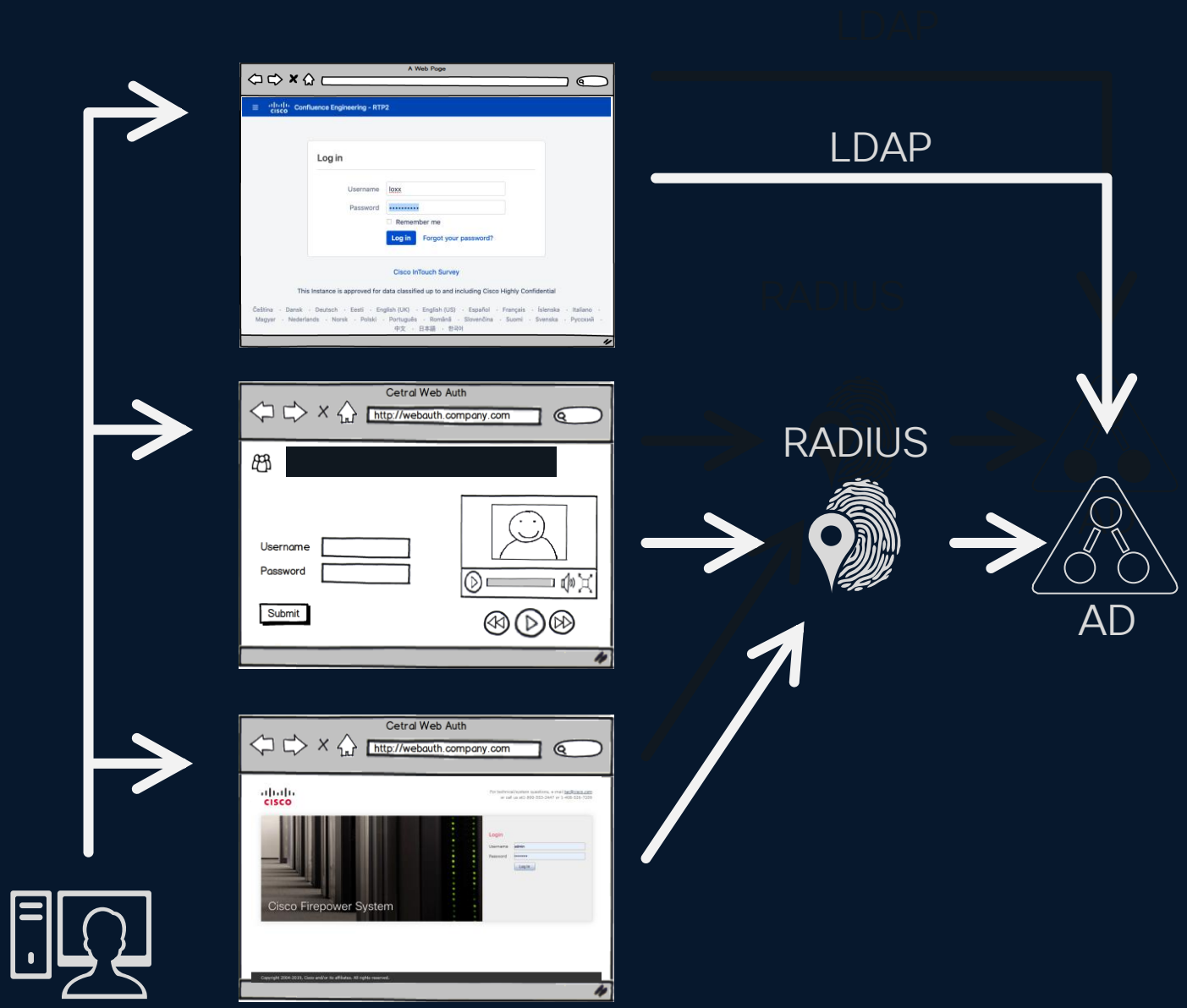


© 2025 Cisco and/or its affiliates. All rights reserved.

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?



© 2025 Cisco and/or its affiliates. All rights reserved.

New Term: Federation /fĕd" ə-rā'shən/

Delegation of authority by otherwise independent entities

-Josh Green, Geek

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

Enter:
Single Sign On

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

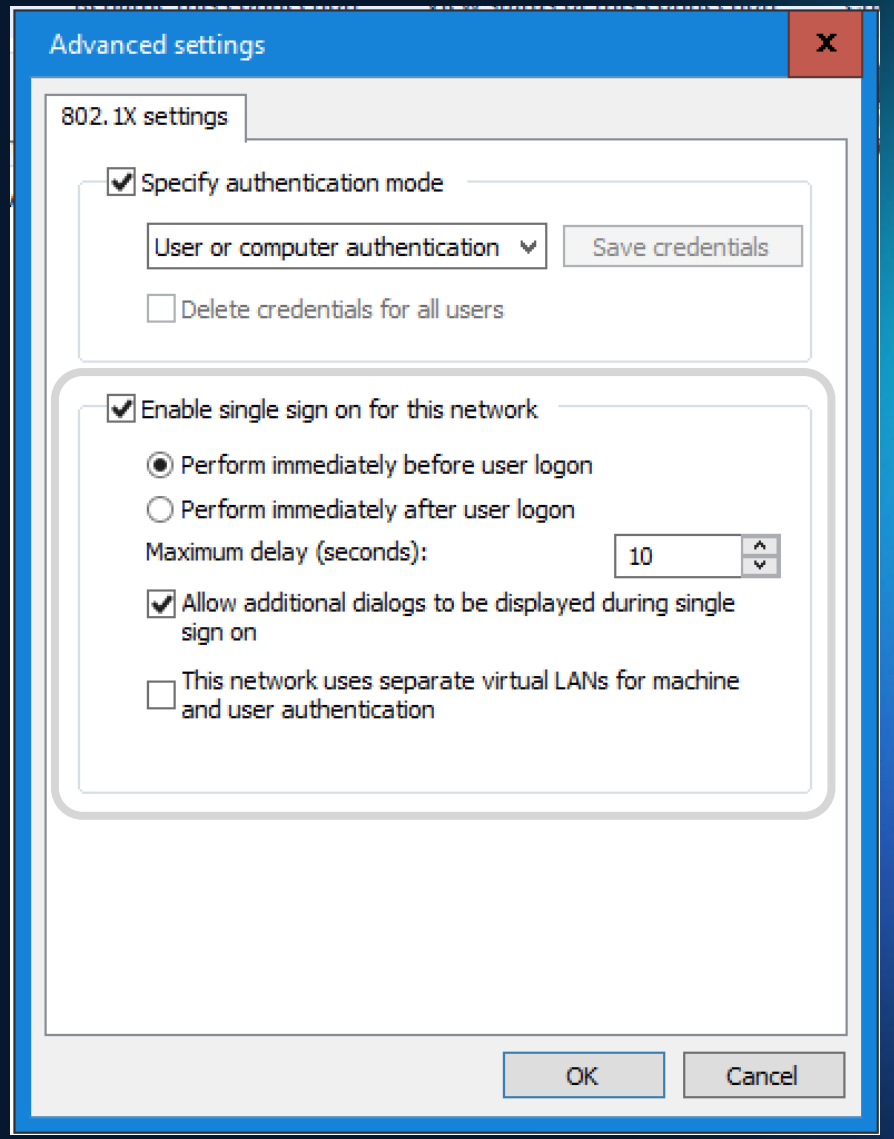
SSO itself is the process that allows a single authentication to be used across multiple web sites or applications

Note: you can have federation without SSO, but you cannot have SSO w/o federation

© 2025 Cisco and/or its affiliates. All rights reserved.

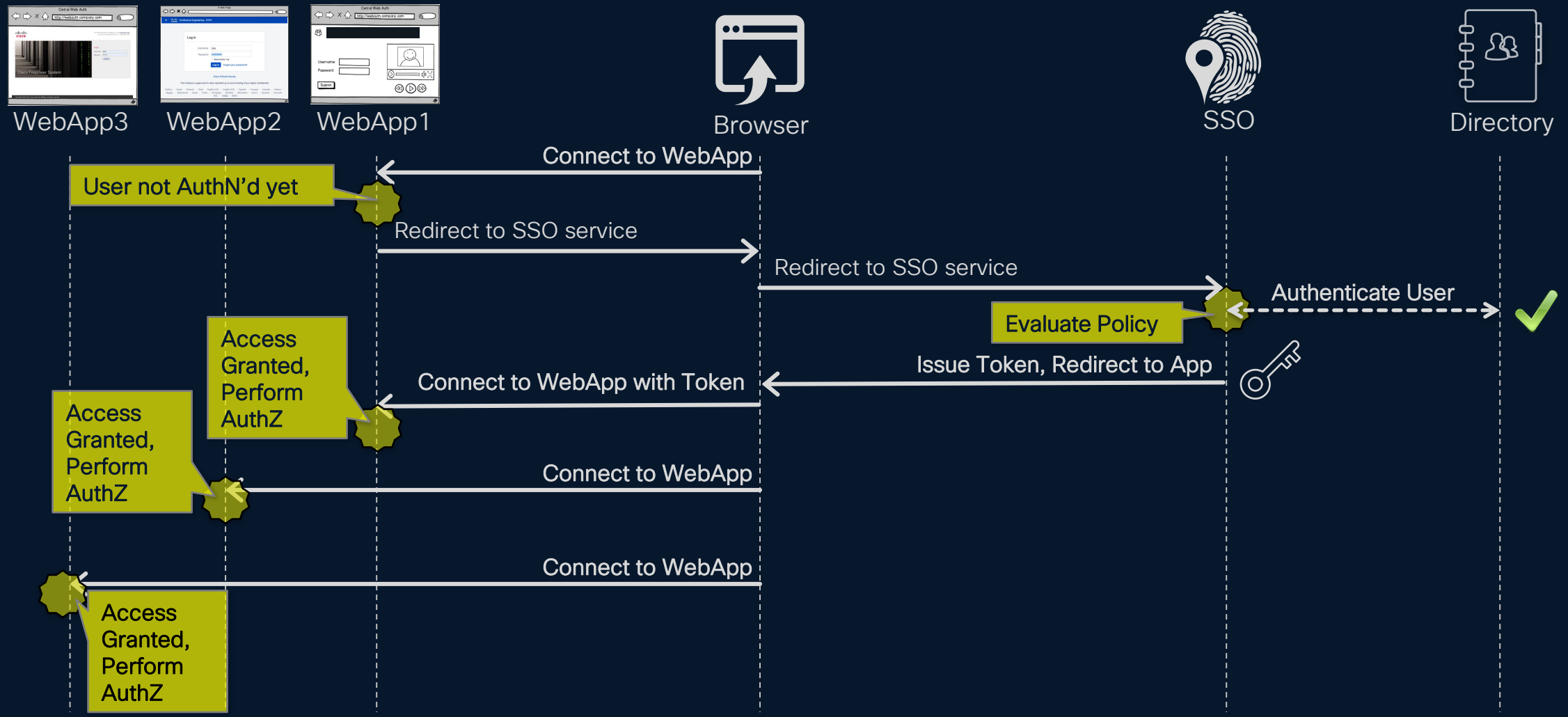
SSO w/ Dot1X Supplicant

- Leverages the login to the local OS
  - Sends those same credentials into the network for 802.1X authentication



© 2025 Cisco and/or its affiliates. All rights reserved.

SSO [somewhat] Explained



© 2025 Cisco and/or its affiliates. All rights reserved.

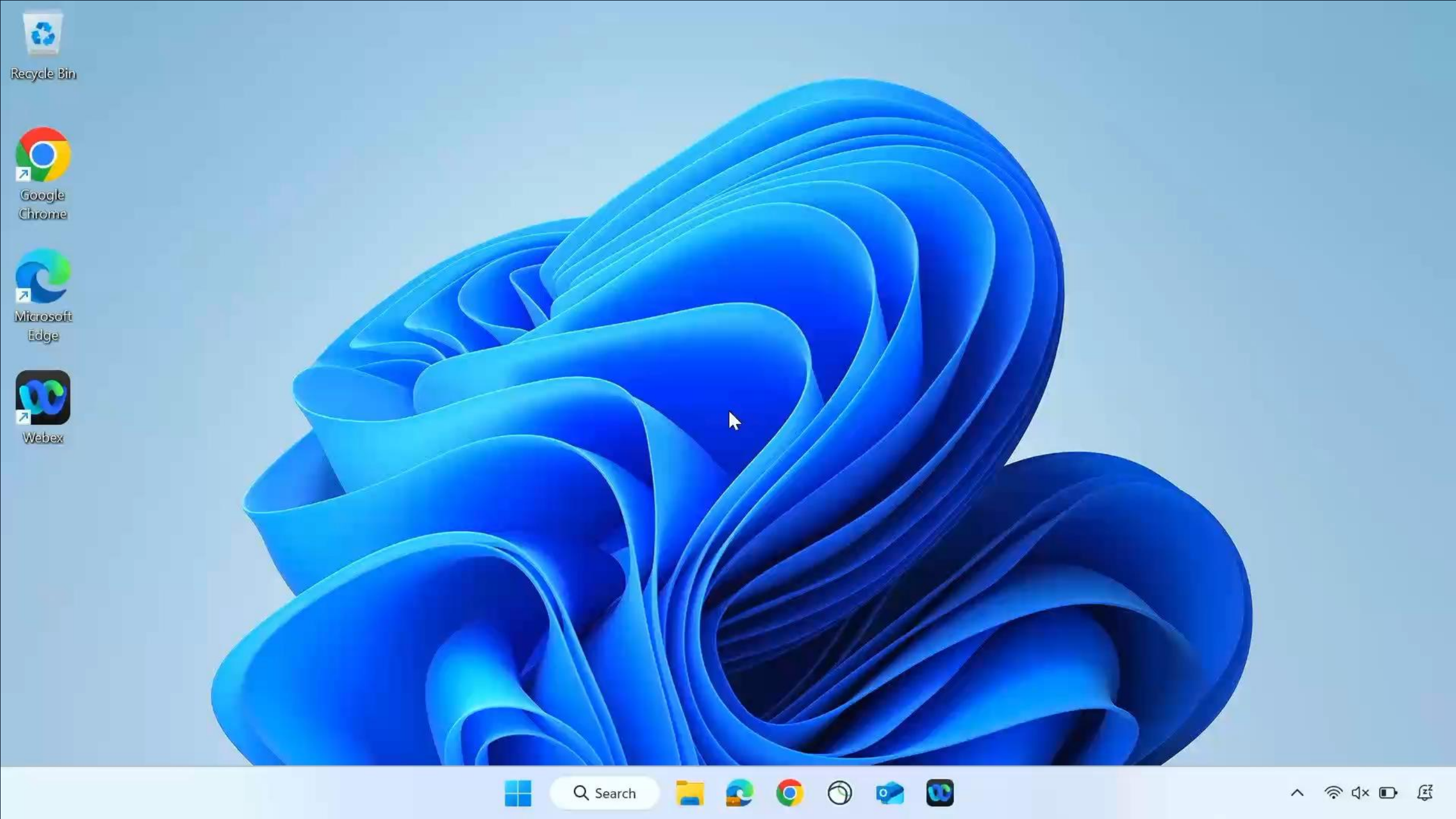
SSO principles

- 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

Note: the fact that the app is still still doing local AuthZ shows federation.

© 2025 Cisco and/or its affiliates. All rights reserved.

Demo Video: Single Sign On with Duo


Recycle Bin
Google Chrome
Microsoft Edge
Webex
Search

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

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

The XACML working group had to find something to do with their stuff ☺

© 2025 Cisco and/or its affiliates. All rights reserved.

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

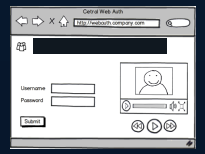
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Definitions

Web-based Auth's

Browser
aka: User Agent



Service Provider (SP)

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

Like the Authenticator in dot1x

IdP

Directory

802.1X

Supplicant

Authenticator

Authentication Server

Directory

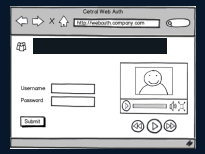
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Definitions

Web-based Auth's

Browser
aka: User Agent



Service Provider (SP)

IdP

Directory

Handles the authentication, issues assertion, etc.
(ex: PING, EntraID, Shibboleth, etc.)

Like the Authentication Server in dot1x

802.1X

Supplicant

Authenticator

Authentication Server

Directory

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Definitions

Web-based Auth's

Browser
aka: User Agent

Service Provider (SP)

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

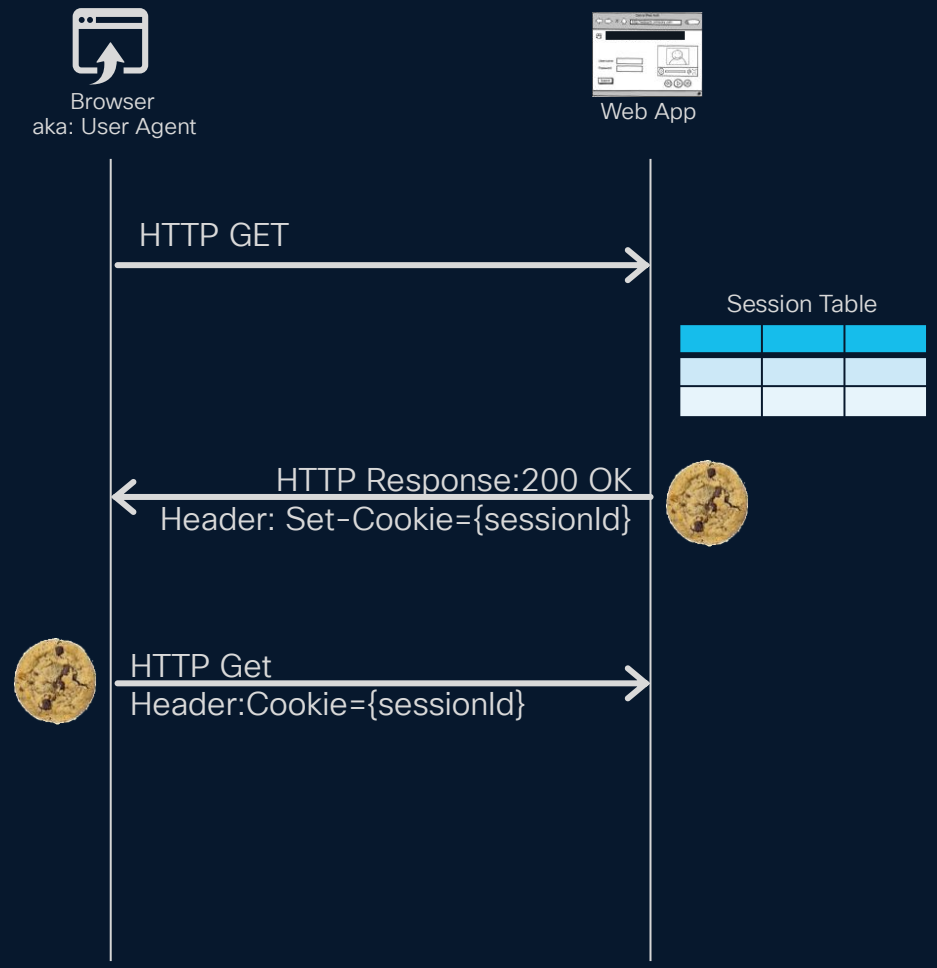
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Sessions & Cookies

For the non-Web Developer

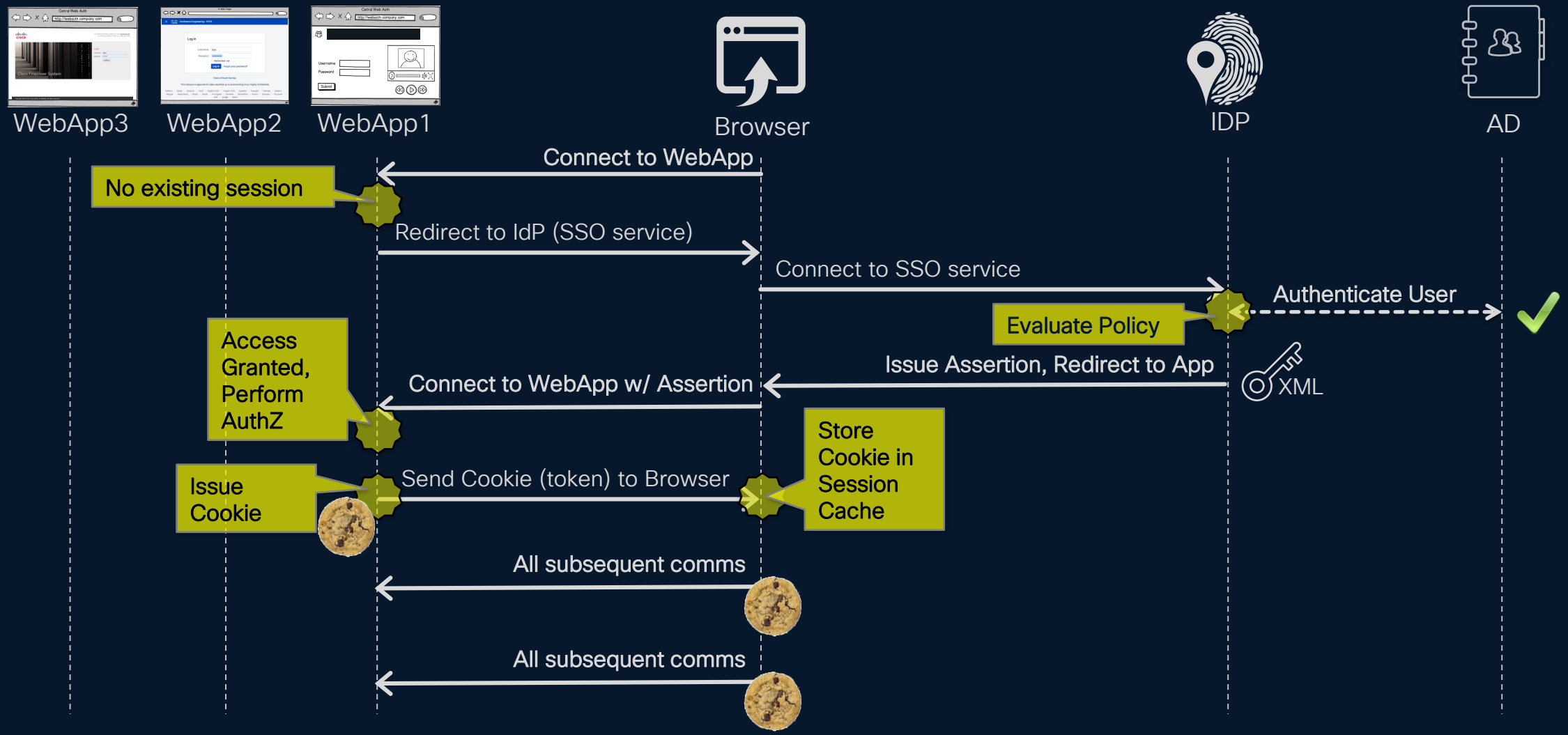
- Web Apps use HTTP
  - HTTP is transactional, but not stateful
  - An HTTP Request is made, response is sent, comm is over
- Cookies are used to maintain state
  - Session ID & other useful information for the website
  - Once the user clears their cache, the cookies are often deleted
- Each session is associated with a randomly generated unique ID
  - Website sends the cookie to the browser
  - Stored in the browser's local cache
  - Used in all future transactions to identify the state to the web app



Note: *The web service does not retain a copy. It does not compare the client's cookie to what the service sent.*

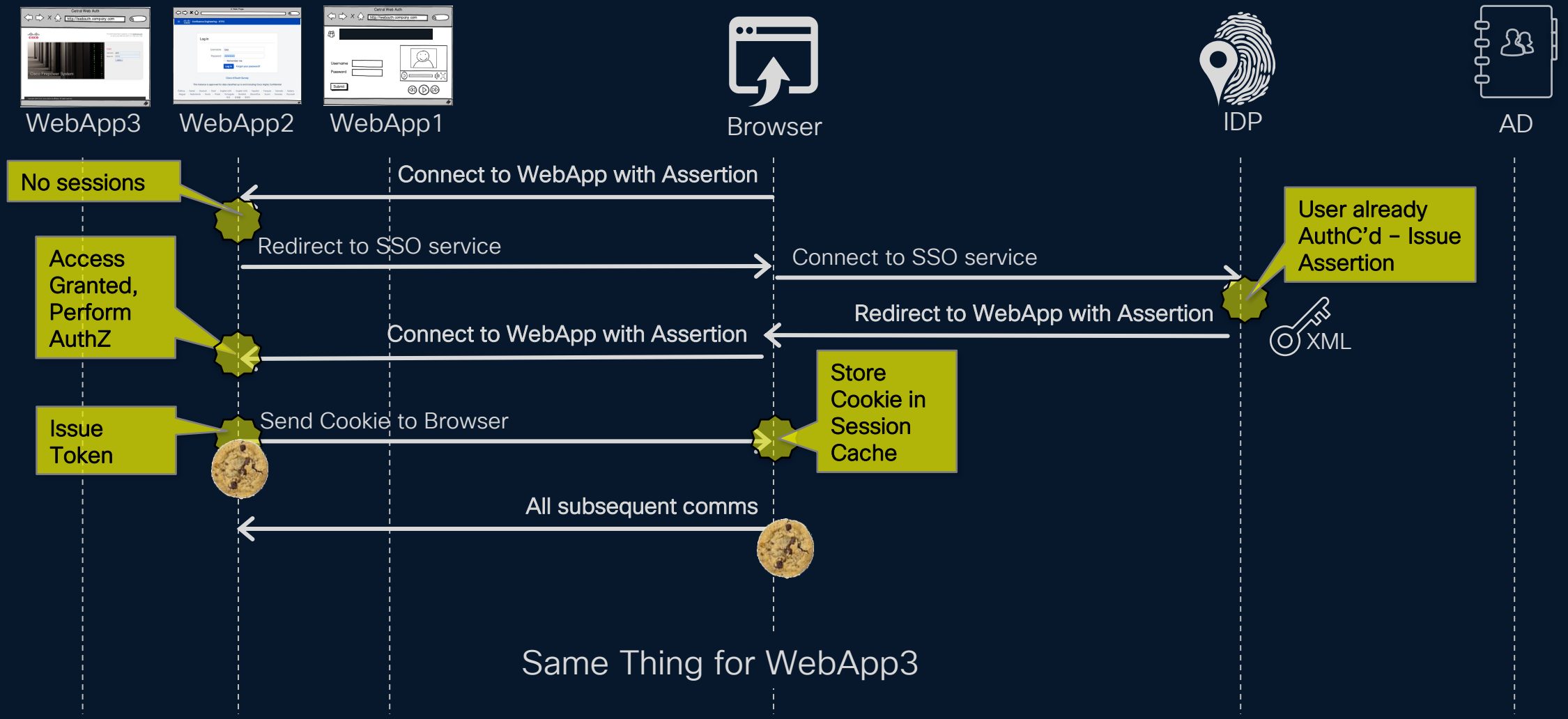
© 2025 Cisco and/or its affiliates. All rights reserved.

SAML for Single-Sign-On



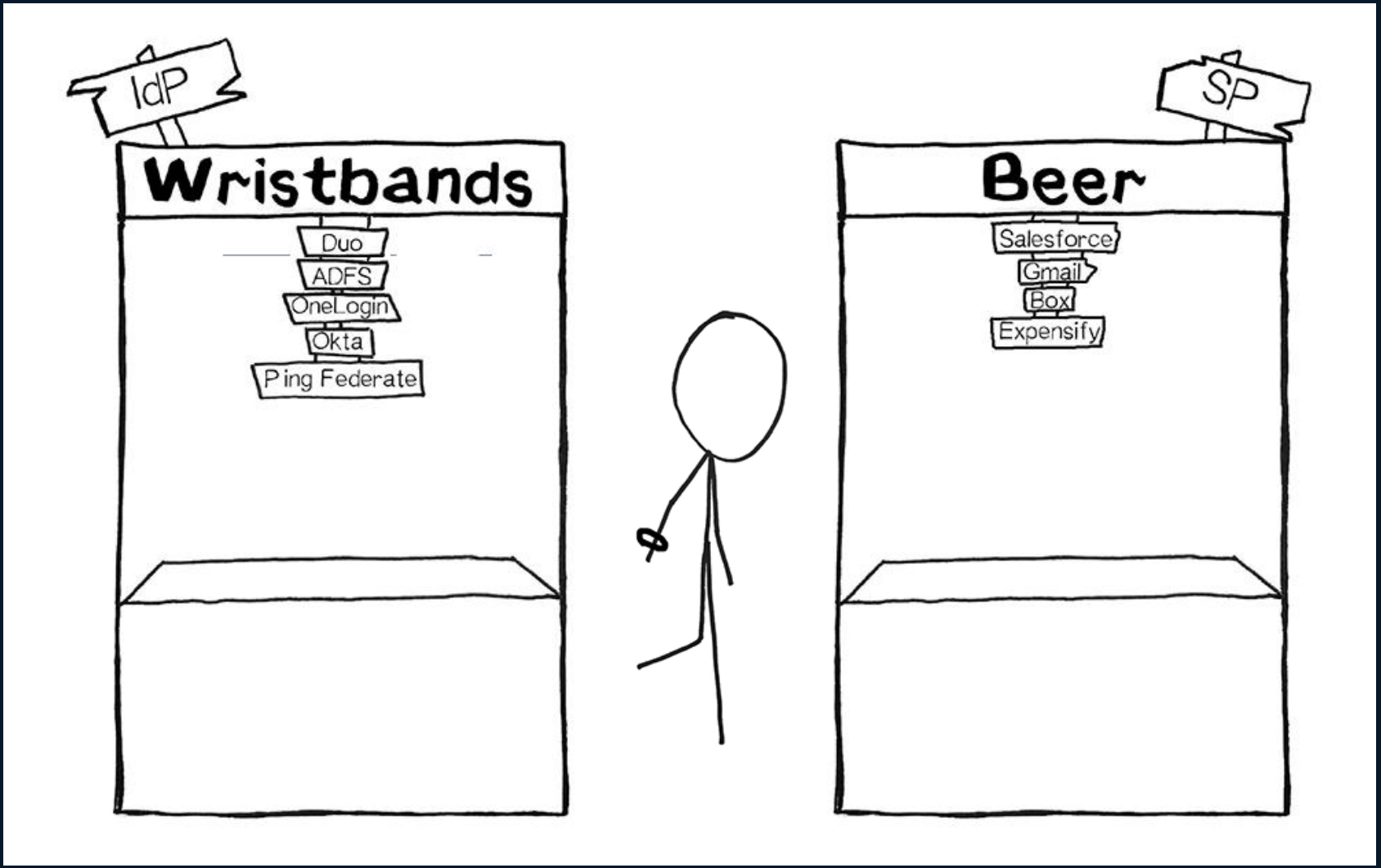
© 2025 Cisco and/or its affiliates. All rights reserved.

SAML for Single-Sign-On



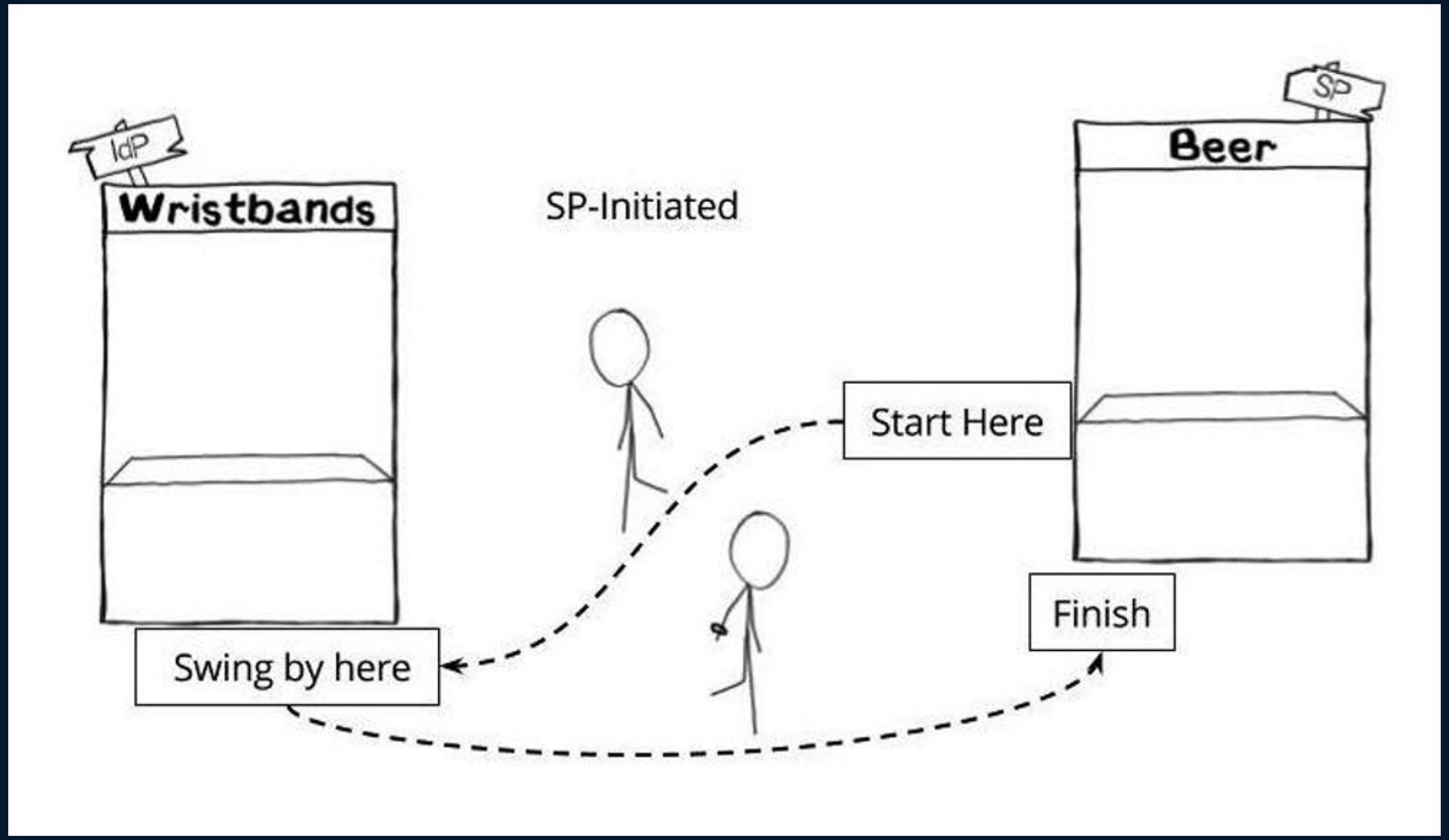
© 2025 Cisco and/or its affiliates. All rights reserved.

The Beer Drinker's Guide to SAML



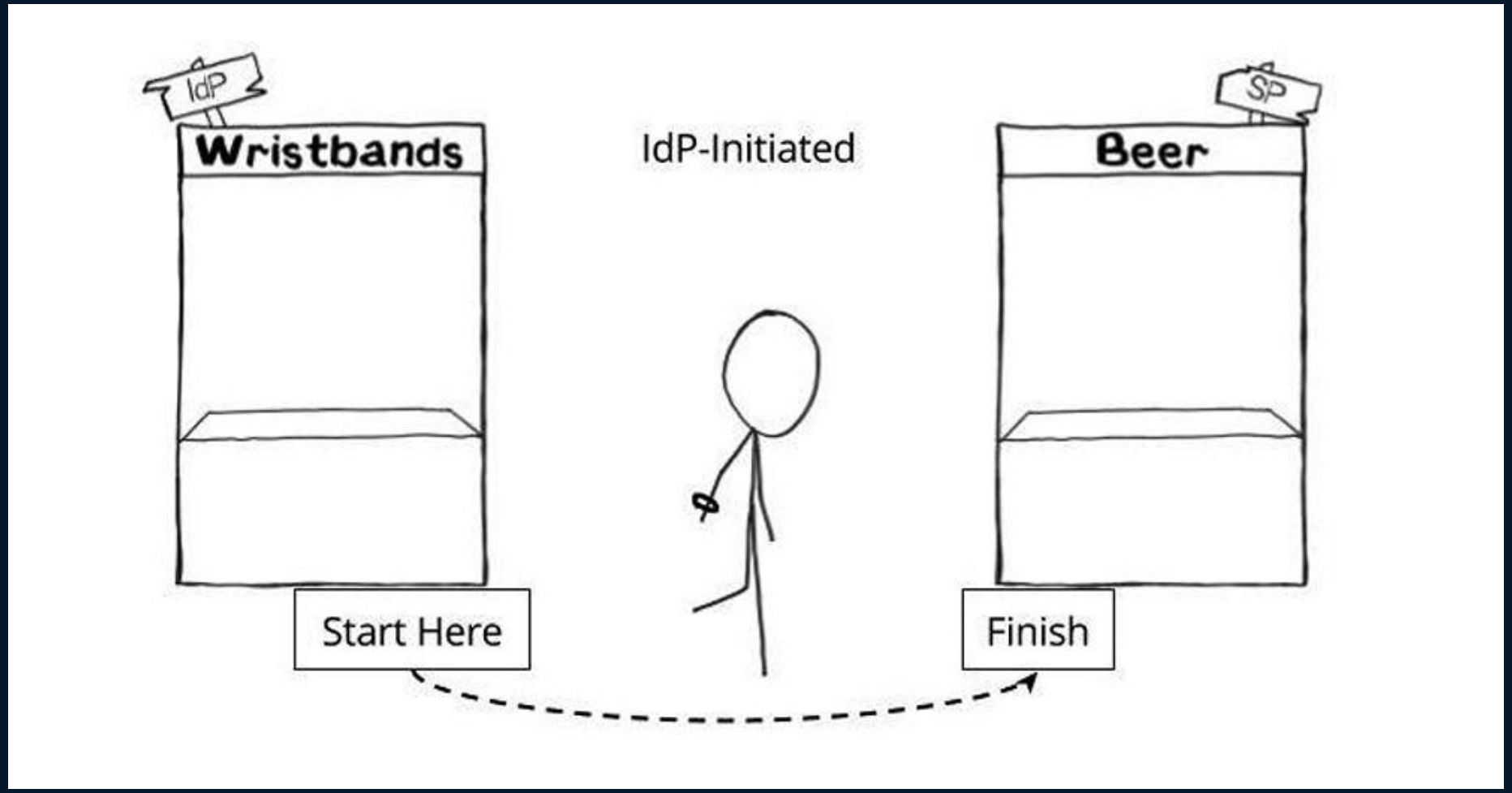
© 2025 Cisco and/or its affiliates. All rights reserved.

The Beer Drinker's Guide to SAML



© 2025 Cisco and/or its affiliates. All rights reserved.

The Beer Drinker's Guide to SAML



© 2025 Cisco and/or its affiliates. All rights reserved.

IDP vs. SP Initiated Login

IdP Initiated Login

Centralized App Launch Location – end–user logs in to the central portal with SSO.

Clicks one of the tiles & is directed to the SP (application) with the token ”in-hand”.

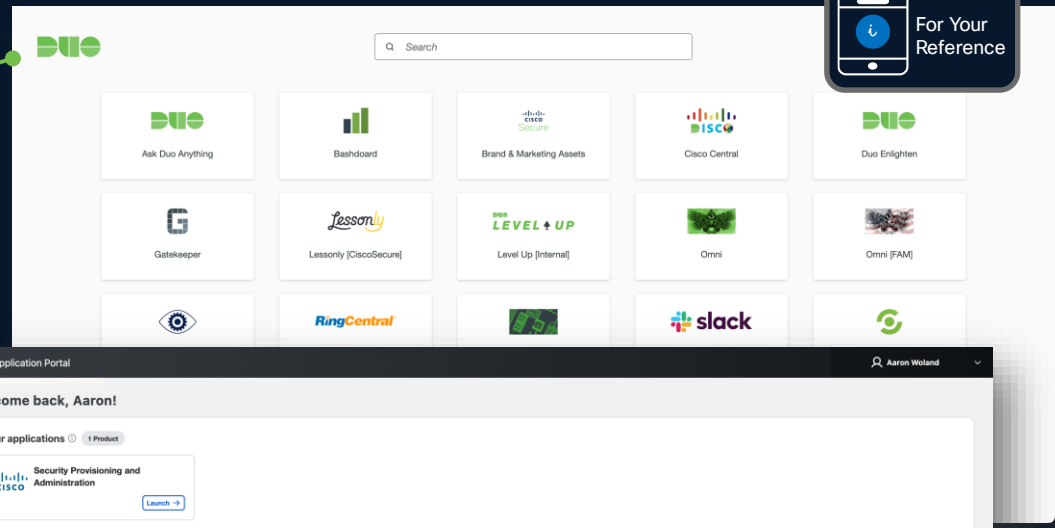
Preferred when a simplified user-experience is desired w/ a single place to access all the applications.

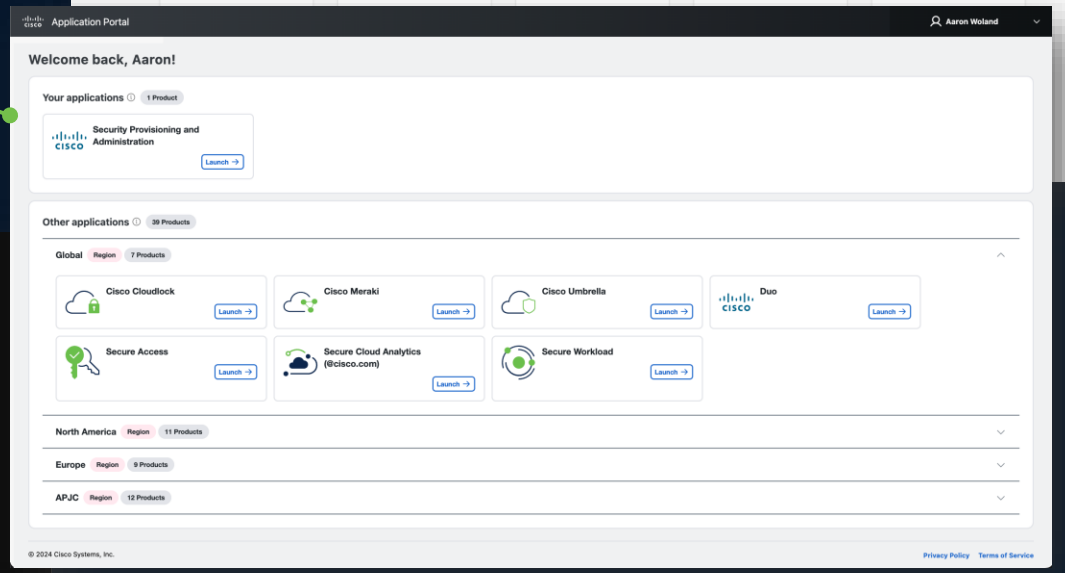
Examples: Security Cloud Sign-on & Duo Central

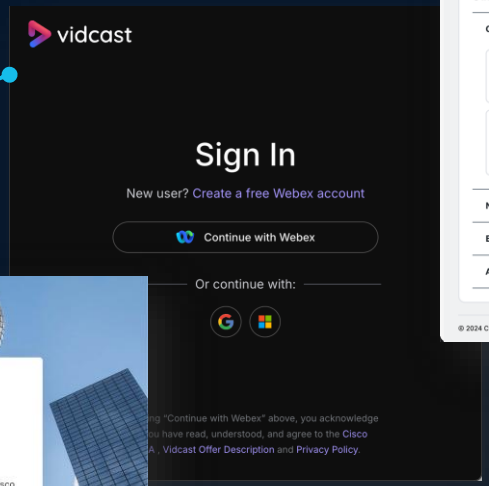
SP Initiated Login

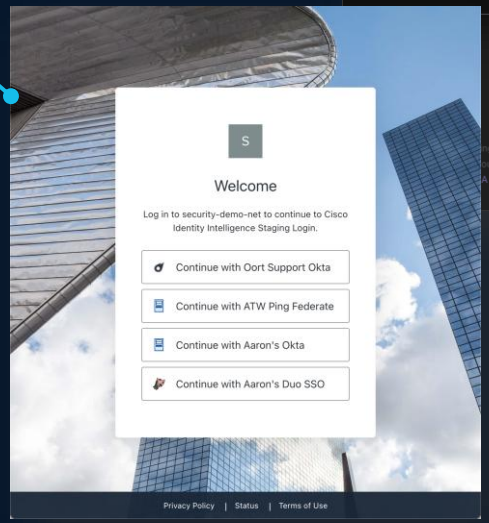
Application triggered login – when logging into the application itself, the end-user is redirected to the IdP for authentication.

Examples: CII & Webex









© 2025 Cisco and/or its affiliates. All rights reserved.

Configuring SAML

SAML requires copy/pasting values between the IDP and the SP

IDP Configuration

IDP Entity ID

The unique URL on the IDP to identify this configured app

Single Sign-On-URL

The unique URL for the SP to redirect the user-agent (browser) to for logins to this app to start SSO

Single-Log-Out-URL (optional)

If the IDP supports logout process, this is the URL to redirect clients to

Metadata URL (optional)

Sometimes the IDP will offer each of these fields within an XML document and publish it to make it easy for the SP to get these values instead of Copy/Paste

SP Configuration

SP Entity ID

The unique URL on the SP to identify the app

Assertion Consumer Service (ACS) URL

The unique URL for the sso-subsystem on the SP for the user-agent to send the IDPs assertion to.

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Configuring SAML

SAML requires copy/pasting values between the IDP and the SP

IDP Configuration	SP Configuration

They must also exchange their own X.509 certificate.

- Building Trust Relationship between IDP & SP
- Securing the Communications (*i.e: TLS)
- Signing the Assertions
- Encrypting SAML messages

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

Open Authorization (OAuth)

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

© 2025 Cisco and/or its affiliates. All rights reserved.

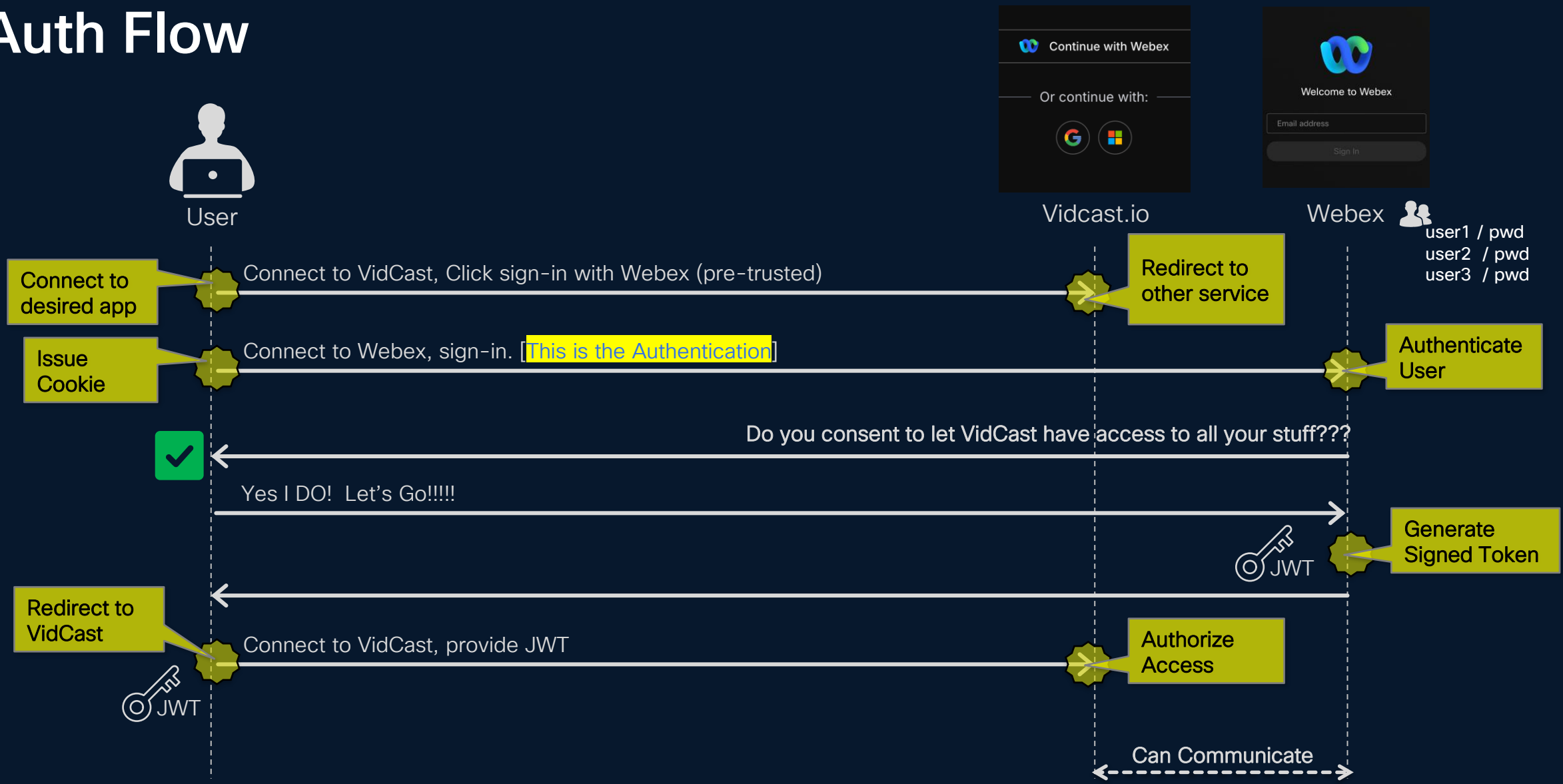
Open Authorization v2 (OAuth2)

- Open Standard
  - Token exchange protocol
  - Designed for **application to application**, **authorized by a user**.
  - User authorizes the application.
    - IdP issues a token (JSON Web Token [JWT]) to the app
    - Allows the app to make API calls on behalf of the user.

© 2025 Cisco and/or its affiliates. All rights reserved.

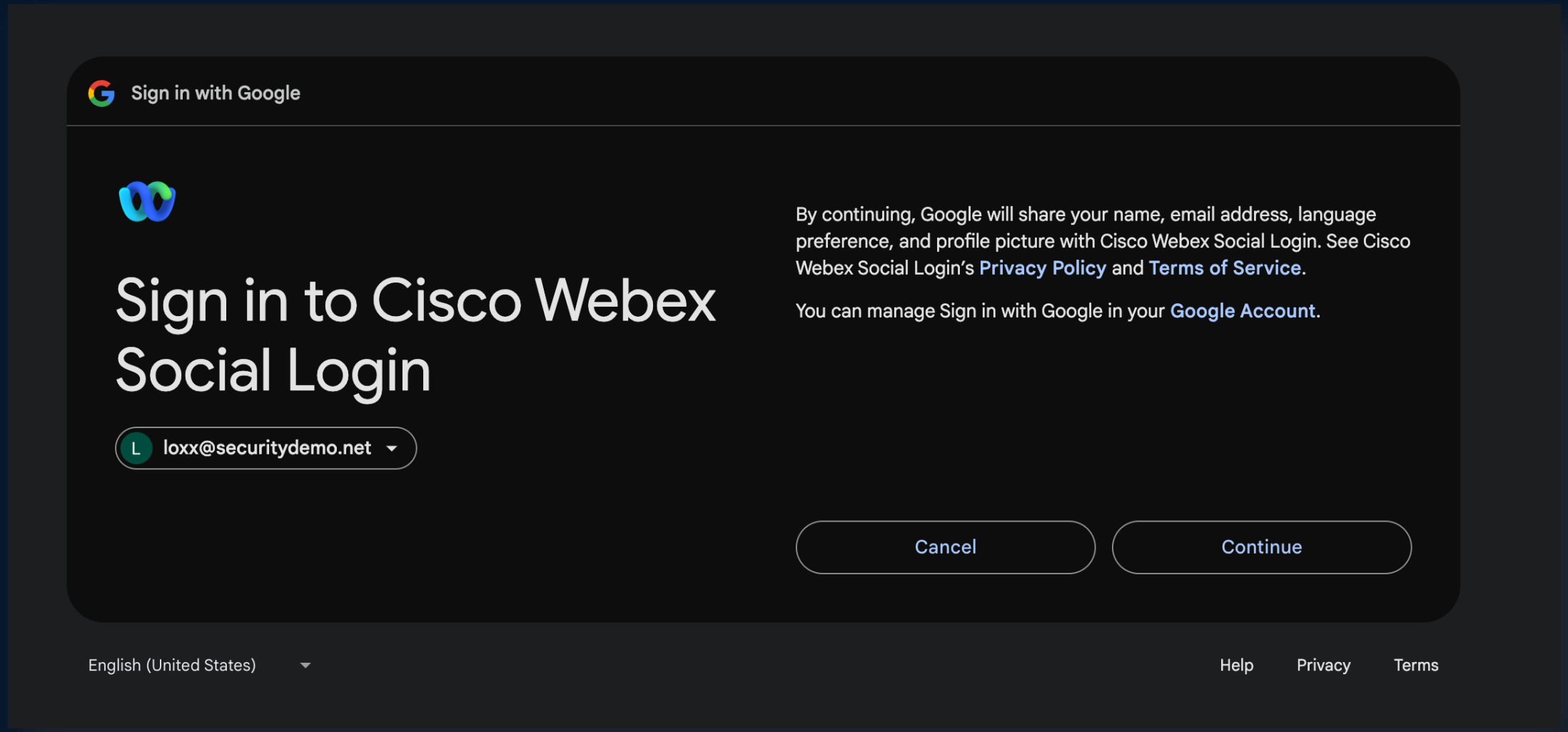
cisco

OAuth Flow



© 2025 Cisco and/or its affiliates. All rights reserved.

Example of Consent



© 2025 Cisco and/or its affiliates. All rights reserved.

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 add authentication to OAuth2's authorization!

© 2025 Cisco and/or its affiliates. All rights reserved.

OIDC is now an alternative to SAML for SSO.

OAuth is App to App AuthZ.

© 2025 Cisco and/or its affiliates. All rights reserved.

OIDC Glossary

- Relying Party (RP) – This is the application that Lee is logging into! It is the same as an SP in SAML.
- Resource Owner – This is authorizing user. They own their ID, data, and control actions performed on their account.
- Client – The technical component of the the application that wants to access data or perform actions on behalf of the Resource Owner. It is the public ID of the RP.
- IDP – Responsible for AuthN of users and issuing an ID Token providing the identity info to the Relying Party.
- Authorization Server – Very often this is also the IDP, but it can be separated. It is an application that knows the Resource Owner and where the Resource Owner already has an account. This is also called an OpenID Provider in OIDC
- Resource Server – An API or service that the client wants to use on behalf of the resource owner. This will sometimes be the same provider as the Authorization Server

© 2025 Cisco and/or its affiliates. All rights reserved.

Configuring OIDC

Minimum Fields

OIDC requires entering values from the IDP into the RP

Client ID
Unique ID created by the IDP. Is the identifier for the Relying Party & acts like a username for auth

Client Secret
A secret between the RP & the IDP, it acts like the password for the auth between the RP & IDP

Issuer
Like the Entity ID from SAML. The unique URL on the IDP to identify this configured app

Authorization URL
Specific URL on the IDP for AuthN/Z comms

Token URL
URL on the IDP for the RP to obtain an access token

JWKS URL
URL on the IDP containing the keys the RP uses to validate the IDPs signatures

UserInfo URL
The RP presents a token to this URL to retrieve claims

Token Introspection URL
RP uses this URL to validate access tokens. Kind of like an OCSP service in PKI.

Discovery URL
Like the MetaData URL in SAML. It's the openid-configuration JSON file with all these attributes in it

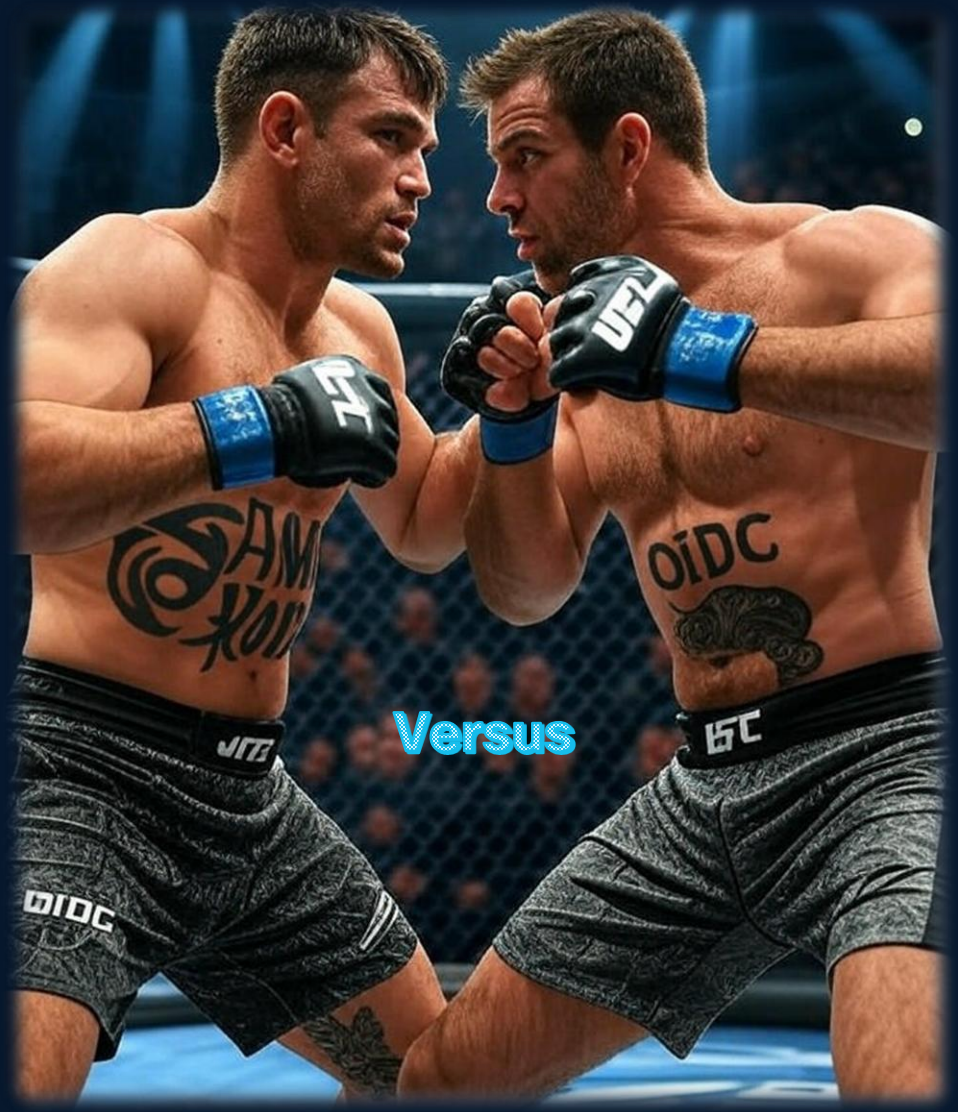
© 2025 Cisco and/or its affiliates. All rights reserved.

OIDC versus SAML

For Your Reference

- SAML is older than OIDC.
  - SAML transmits user attributes using XML format and browser redirects
  - While OIDC uses JSON format and communicates directly from the client application to the OpenID Provider.
- OIDC is considered to be more secure*
  - Enables complete machine-to-machine authentication.

- Which should you choose?
  - Often won't have a choice as not many application vendors implement both!
  - OIDC is being increasingly common for new integrations.



*Depending on which grant type is being used

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

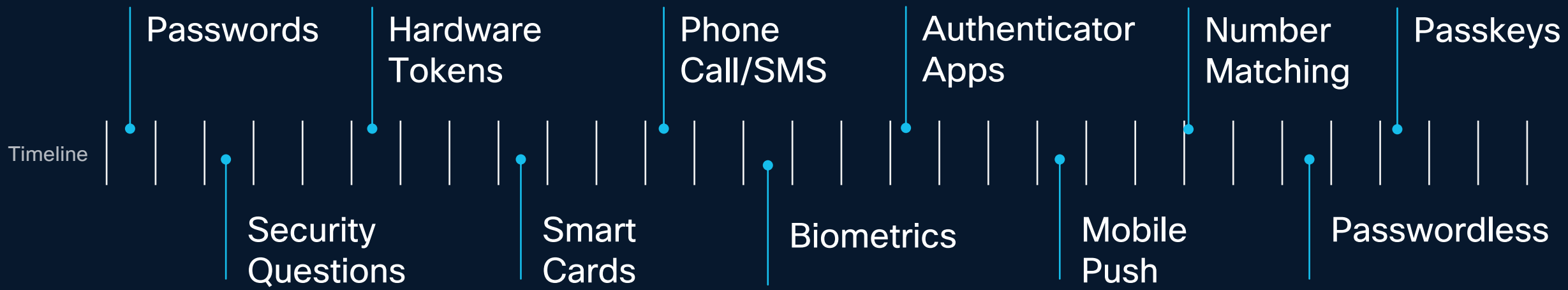
Authentication Factors

The Evolution

Authentication Factors:
- Something you Are
- Something you Know
- Something you have

Multi-Factor AuthN (MFA):
- Means more than One

Assurance Levels:
- How good is the AuthN?
- Is SMS as reliable and strong as a YubiKey?



© 2025 Cisco and/or its affiliates. All rights reserved.

Web Authentication (WebAuthN)

Web Authentication (WebAuthN)

This is what enables passkeys

- 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

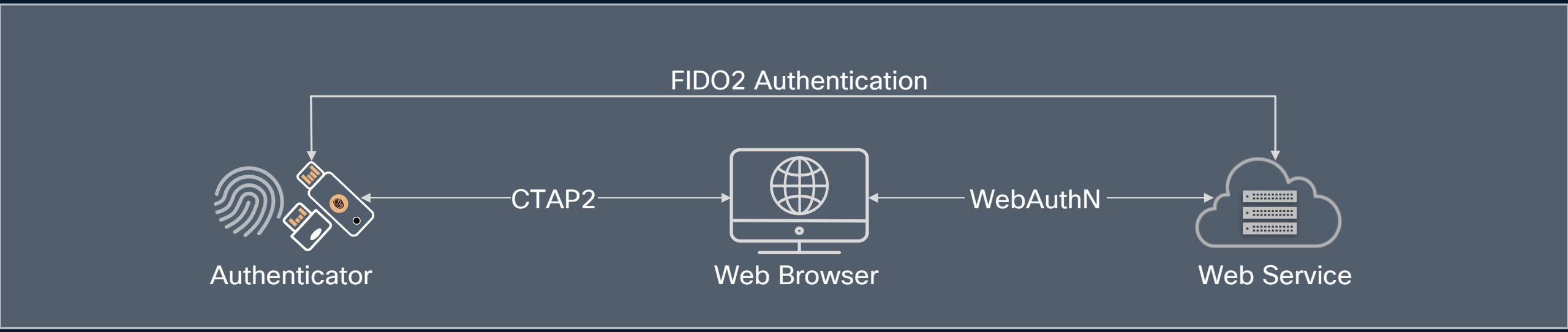
WebAuthn.io

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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



© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Authentication Refresher

Because this is SOO Similar

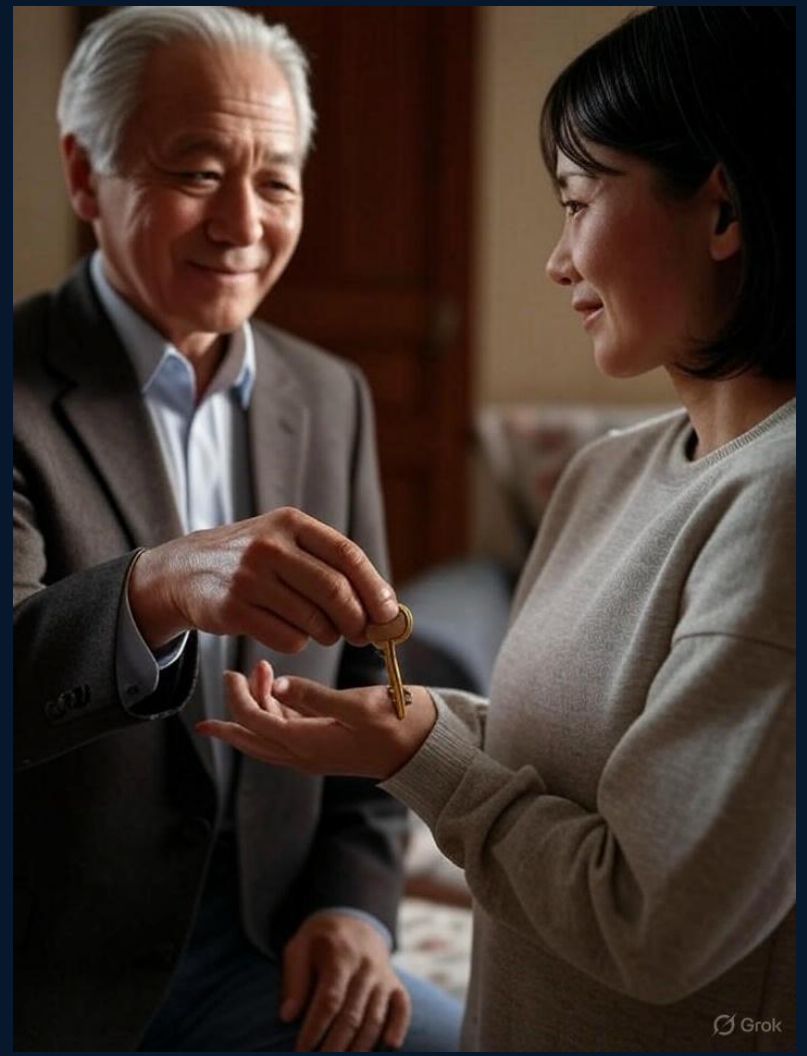
When the authentication server is presented with an identity certificate, it will perform the following tasks (at a minimum):

1. Has the Digital Certificate been issued and properly signed by a known and trusted certificate authority?
2. Is the Certificate Expired? – Must check both the issue and expiration dates!
3. Has the Certificate been revoked by the certificate authority?
4. Has the client provided proof of possession?

© 2025 Cisco and/or its affiliates. All rights reserved.

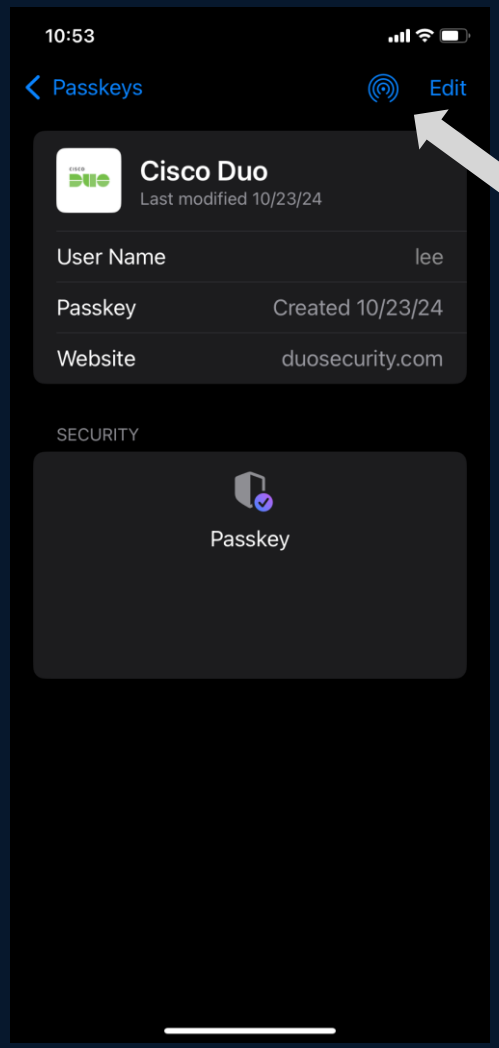
Passkeys

- 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…



© 2025 Cisco and/or its affiliates. All rights reserved.

Shared Passkeys



Airdrop!

To ANYONE!

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Back in My Day

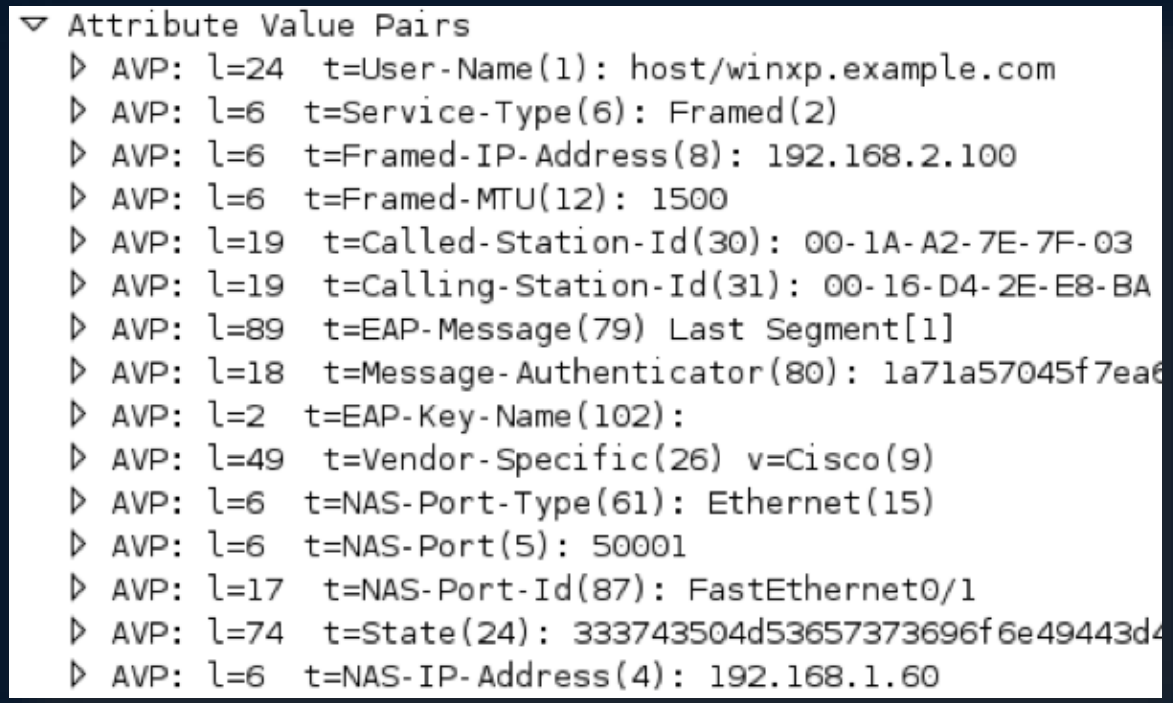
RADIUS Did it All!

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

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).



© 2025 Cisco and/or its affiliates. All rights reserved.

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
  - Defined in the metadata

```
! - 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",
! - SNIP
    "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
}
```

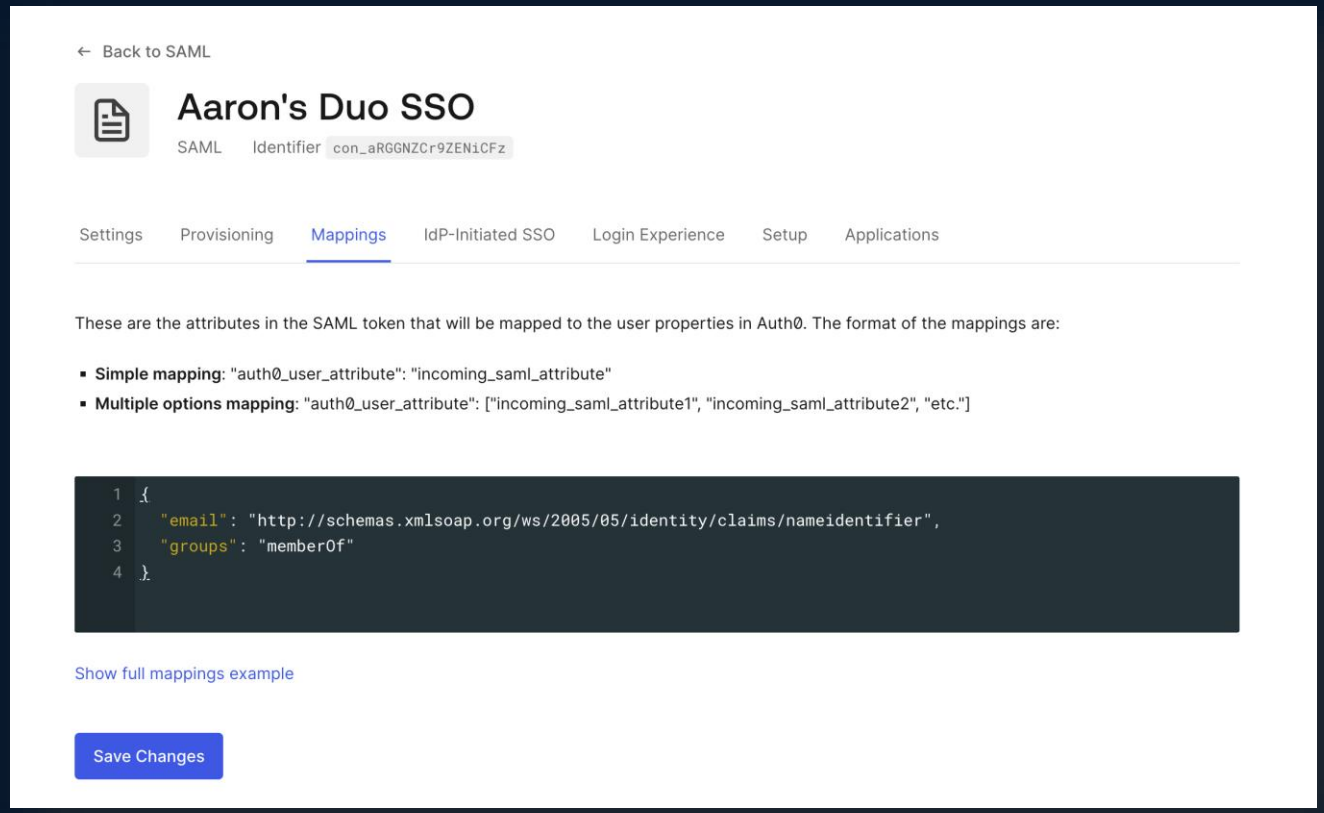
© 2025 Cisco and/or its affiliates. All rights reserved.

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.



© 2025 Cisco and/or its affiliates. All rights reserved.

Lack of Standards / Easy Behaviors

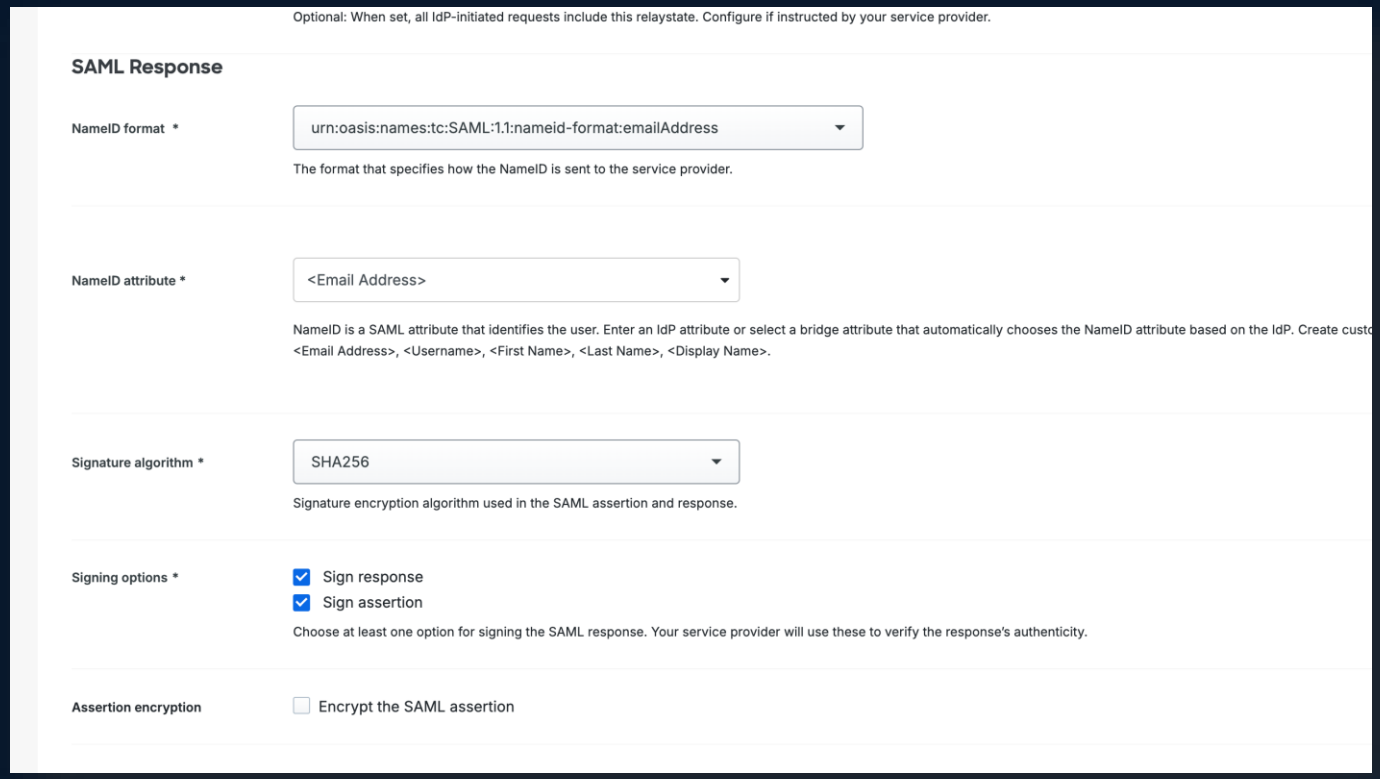
- Can get REALLY complex
  - This shows a powerful, but complex IDP
    - Each & everything is customizable
    - There aren't really any preconfigured drop downs, etc..

© 2025 Cisco and/or its affiliates. All rights reserved.

Lack of Standards / Easy Behaviors

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

- Supported schemas are selectable via a drop down.
- Change our UI to represent the naming convention on the integrated app

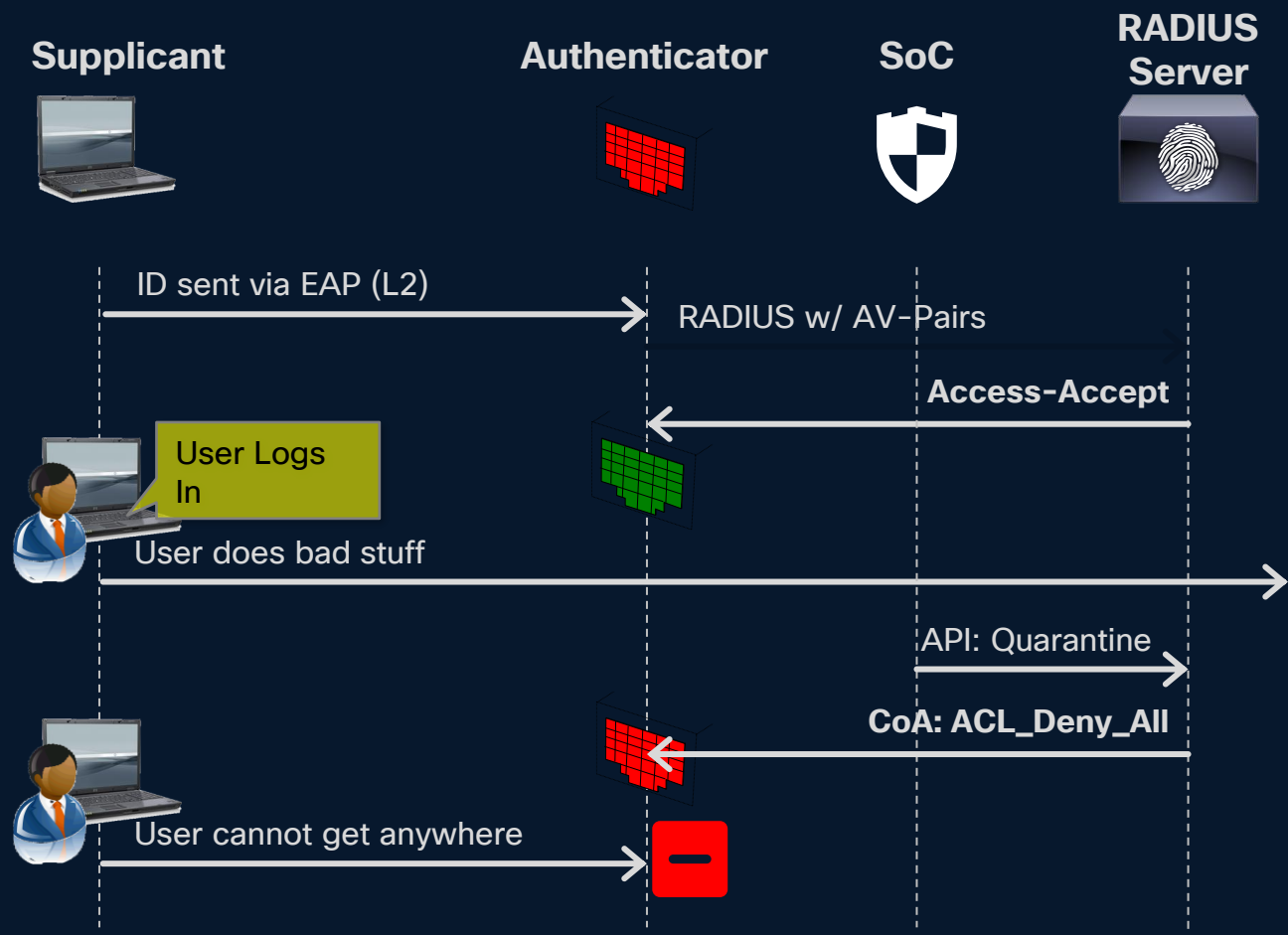


© 2025 Cisco and/or its affiliates. All rights reserved.

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



© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

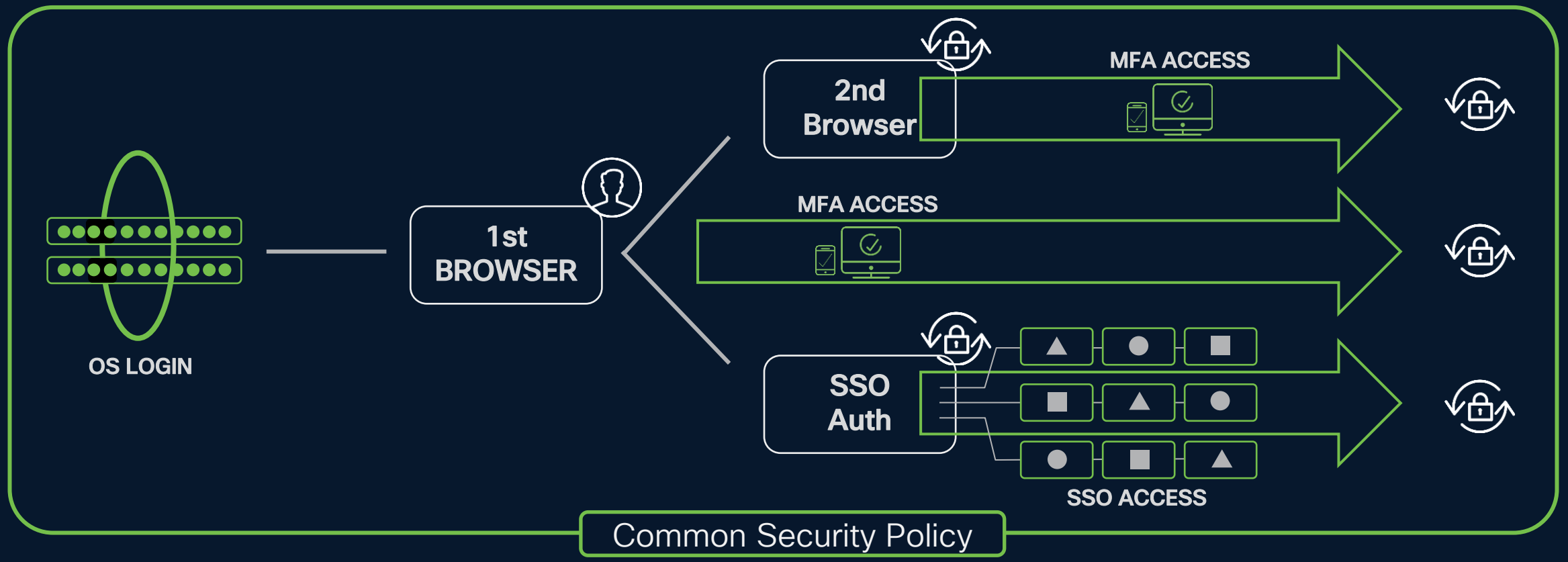
Requires Human Interaction

- 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?

© 2025 Cisco and/or its affiliates. All rights reserved.

Last piece of the puzzle

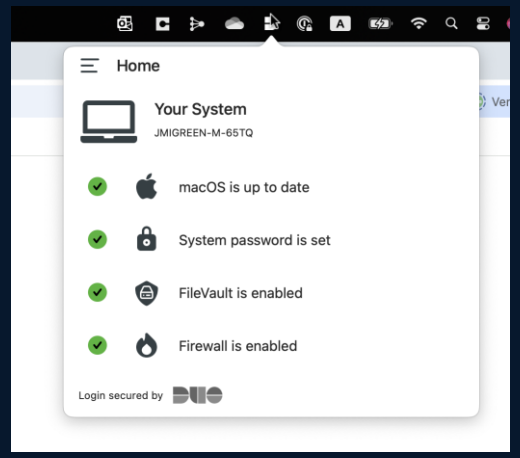
Login Once, Access Everything Securely

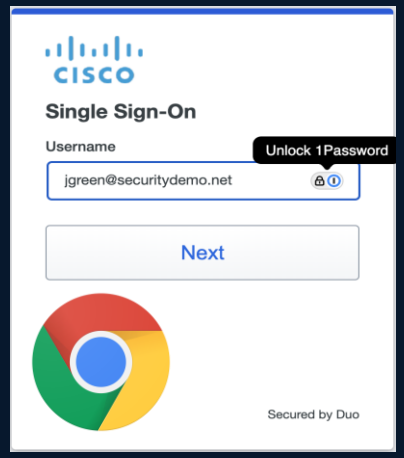


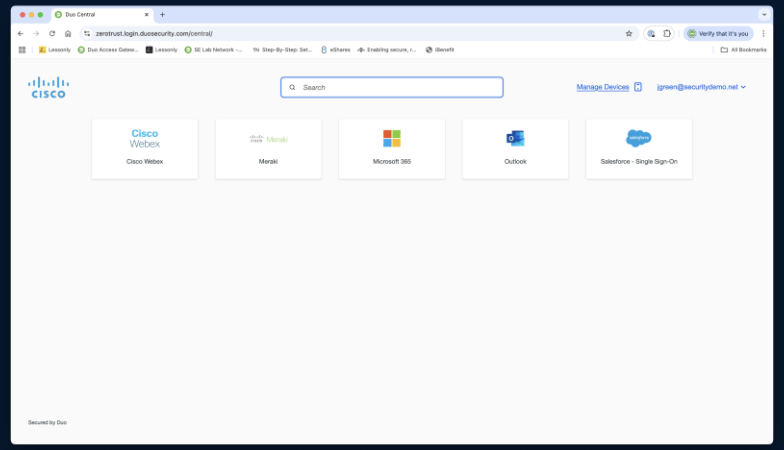
	Interactive authentication - end user friction
	Authentication brokered through device, Duo, and Duo Desktop

© 2025 Cisco and/or its affiliates. All rights reserved.

Duo Passport – True SSO







Endpoint

Duo Desktop sends signed user and device profile to Duo Cloud

User accesses a Duo-protected application via any browser

Duo Desktop sends an updated profile to the cloud

User is logged in to the application

Timeline

Duo Cloud

Duo Cloud records this profile.

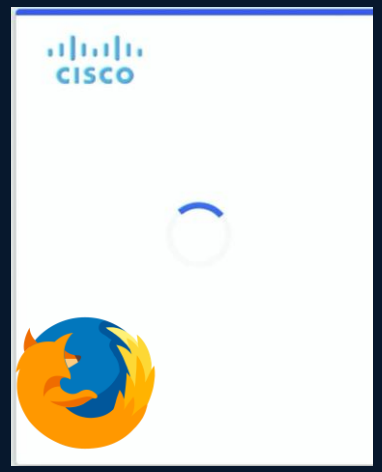
Duo requests a fresh user & device profile from the device

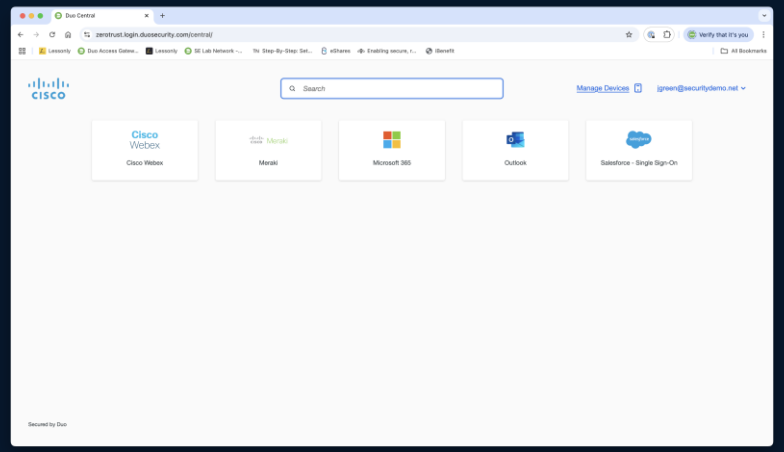
Does the new profile match the original profile?

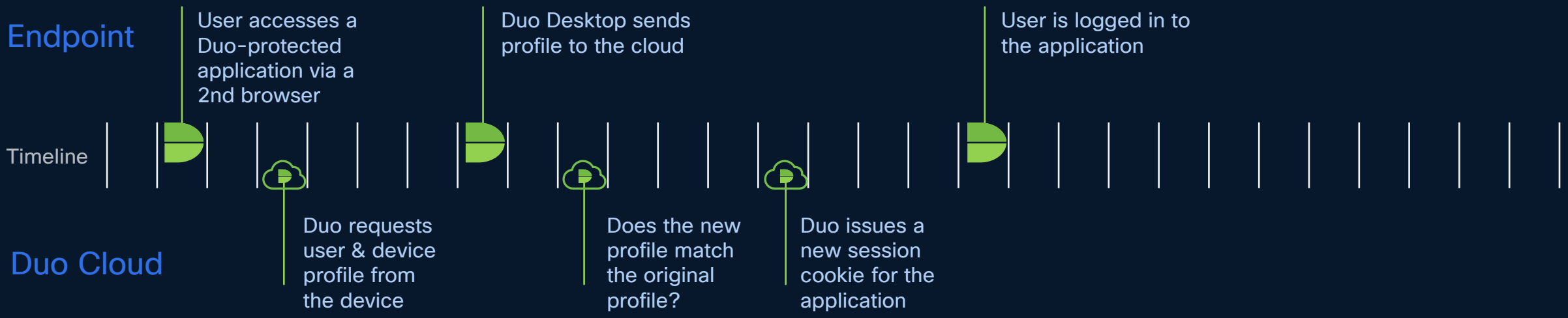
Duo issues a new session for the application

© 2025 Cisco and/or its affiliates. All rights reserved.

Duo Passport – True SSO

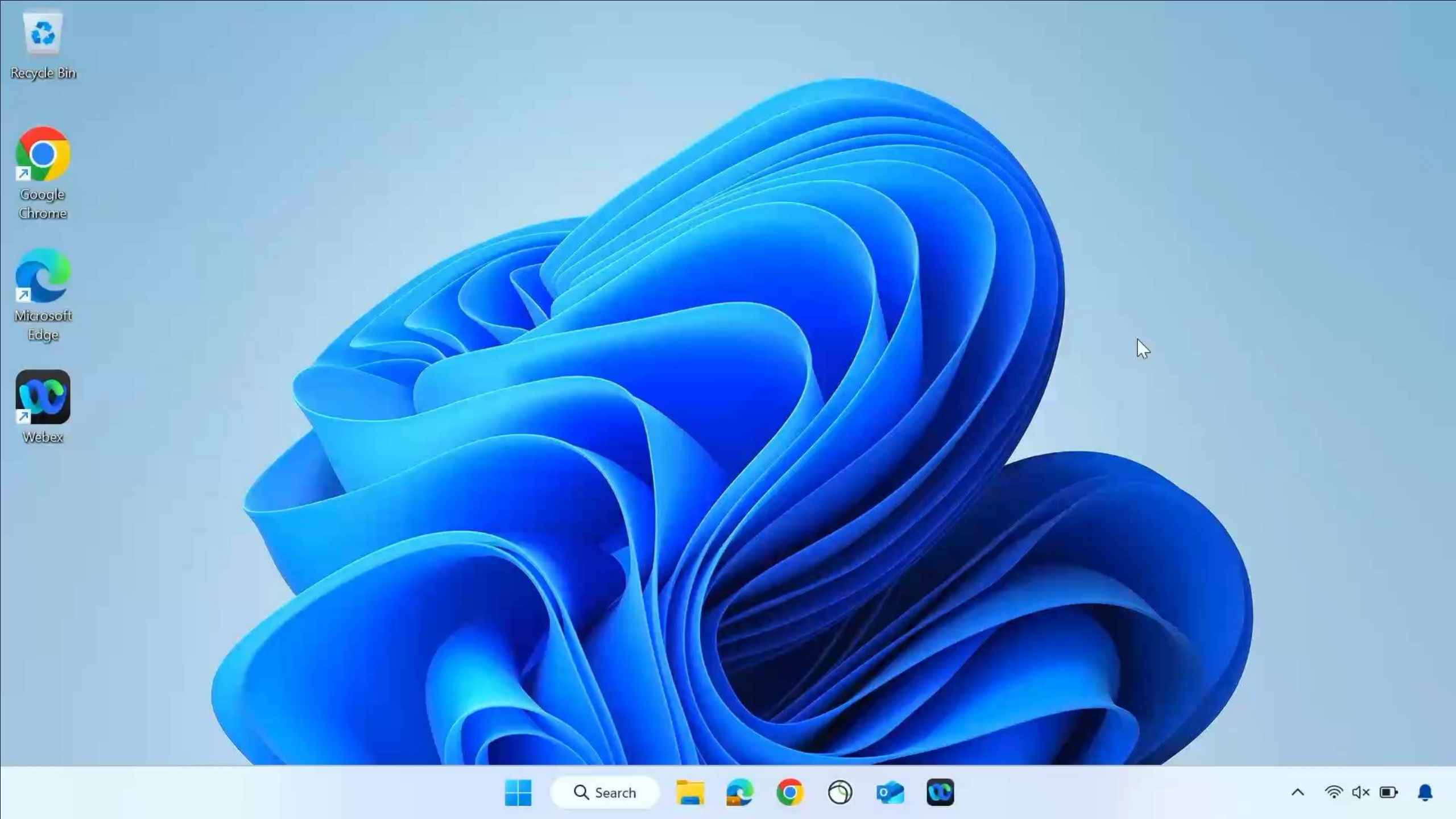






© 2025 Cisco and/or its affiliates. All rights reserved.

cisco


Recycle Bin
Google Chrome
Microsoft Edge
Webex
Search

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

“Future is so bright, I gotta wear shades”

Verifiable Credentials – Why?

“The electric light did not come from the continuous improvement of candles.”

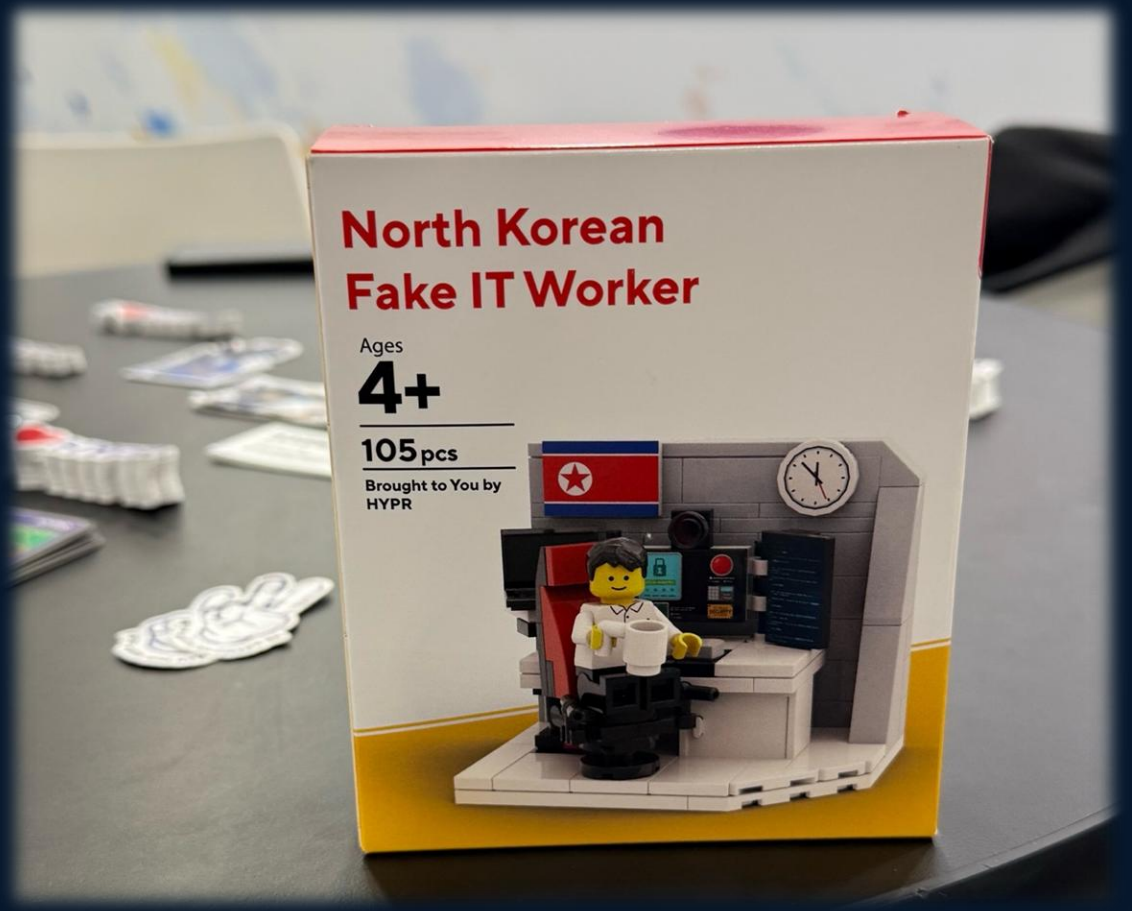
Oren Harari

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Is your new hire who they say they are?

- Issuing credentials to the bad-actors is a GREAT way for them to gain access to your data
  - *"Why hack in when I can log in?"*
- Helpdesk impersonation attacks
  - Successful Phishing Attack:
    - Stolen office session cookie
    - Password harvested off the dark-web
    - Bad guy has access to your email
  - Call into the helpdesk, need to add a new MFA device
  - Now the bad-guy has his own authenticator for valid MFA
- This happens ALL THE TIME



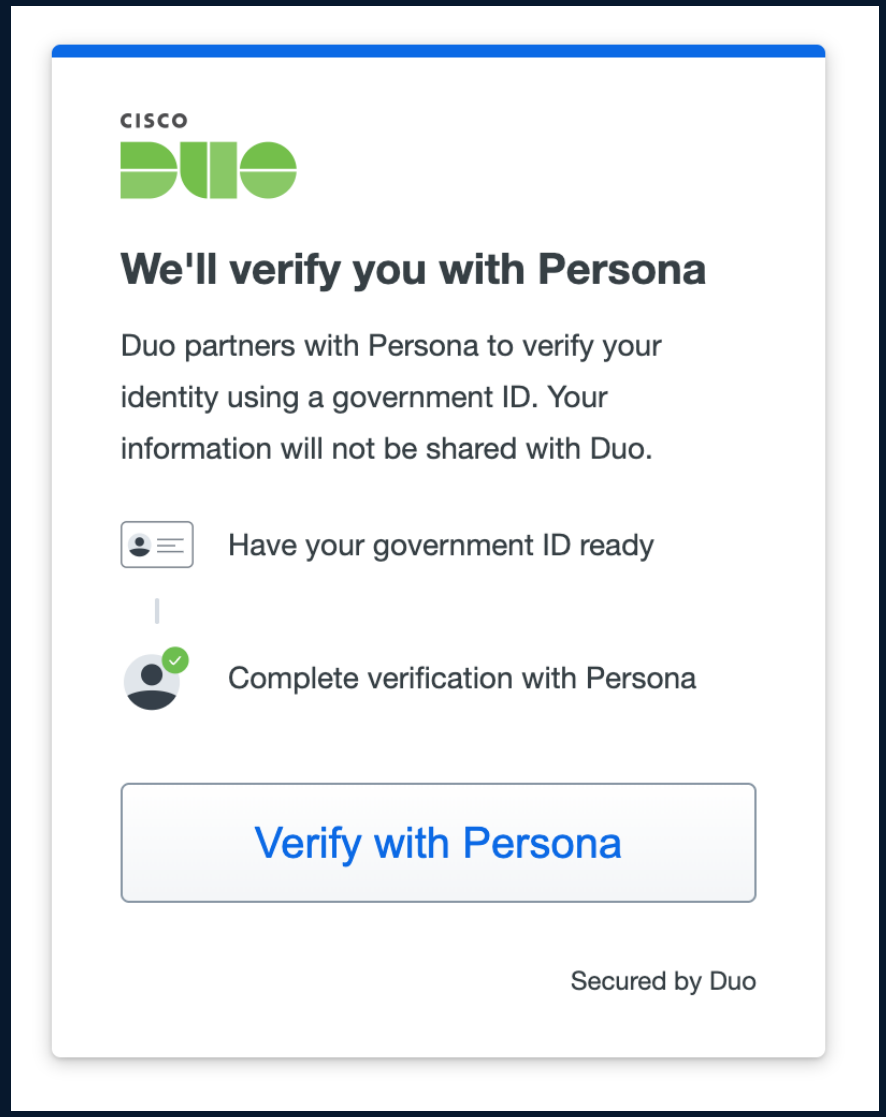
© 2025 Cisco and/or its affiliates. All rights reserved.

Duo Identity Verification integration

- Introducing IDV workflows during critical moments in the workforce user's lifecycle

- First phase is a partnership with Persona. This partner was chosen for:
  - Flexibility and broad options
  - Global support
  - Strategic alignment with Cisco & Duo

- Key workflows:
  - Help Desk Verification
  - Remote Onboarding
  - Self-Service



To establish trust, users must match information that has been stored in Duo – then provide government ID and a selfie.

© 2025 Cisco and/or its affiliates. All rights reserved.

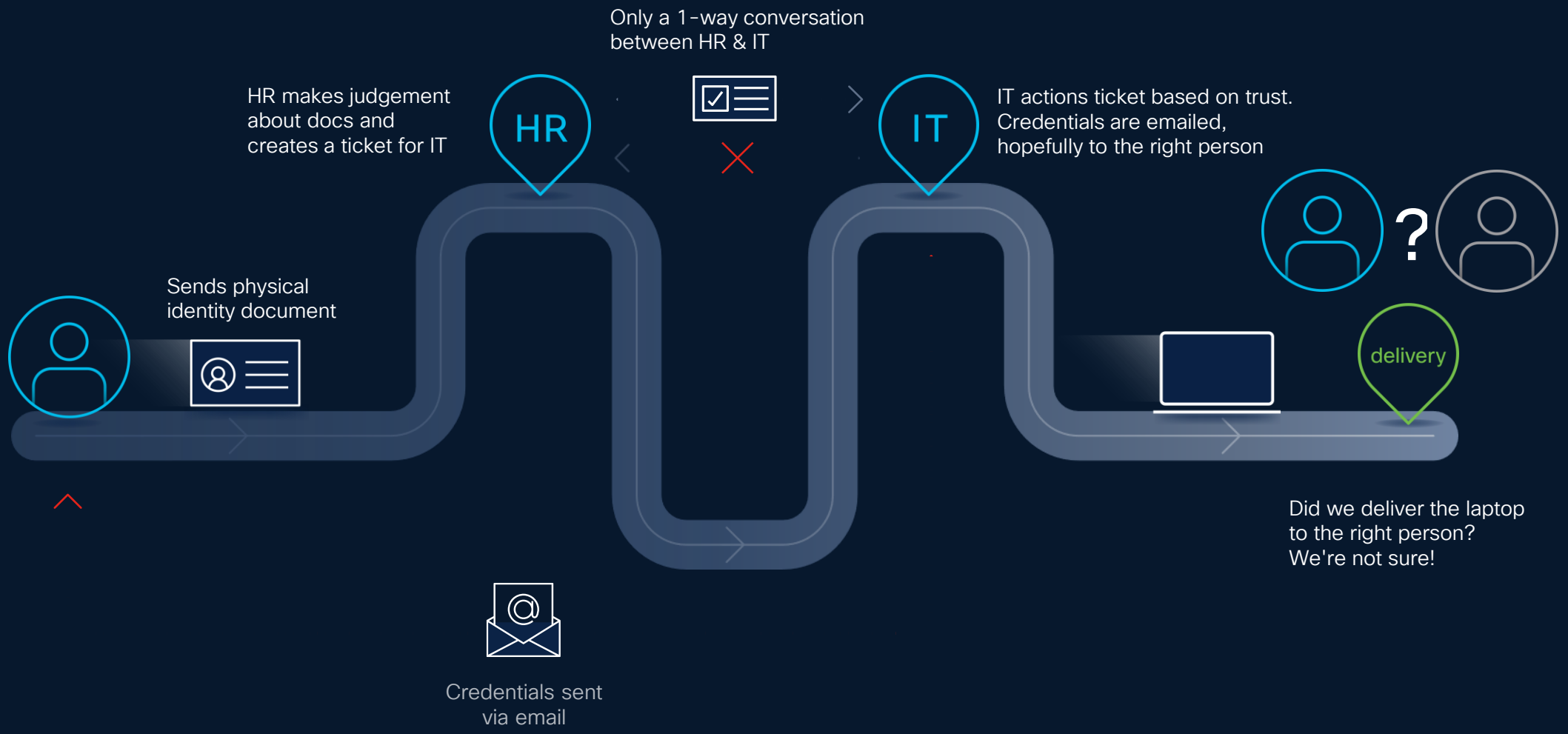
Helpdesk Identity Verification

That was Identity Verification (IDV).

Coming soon is Verifiable Credentials with Digital ID’s

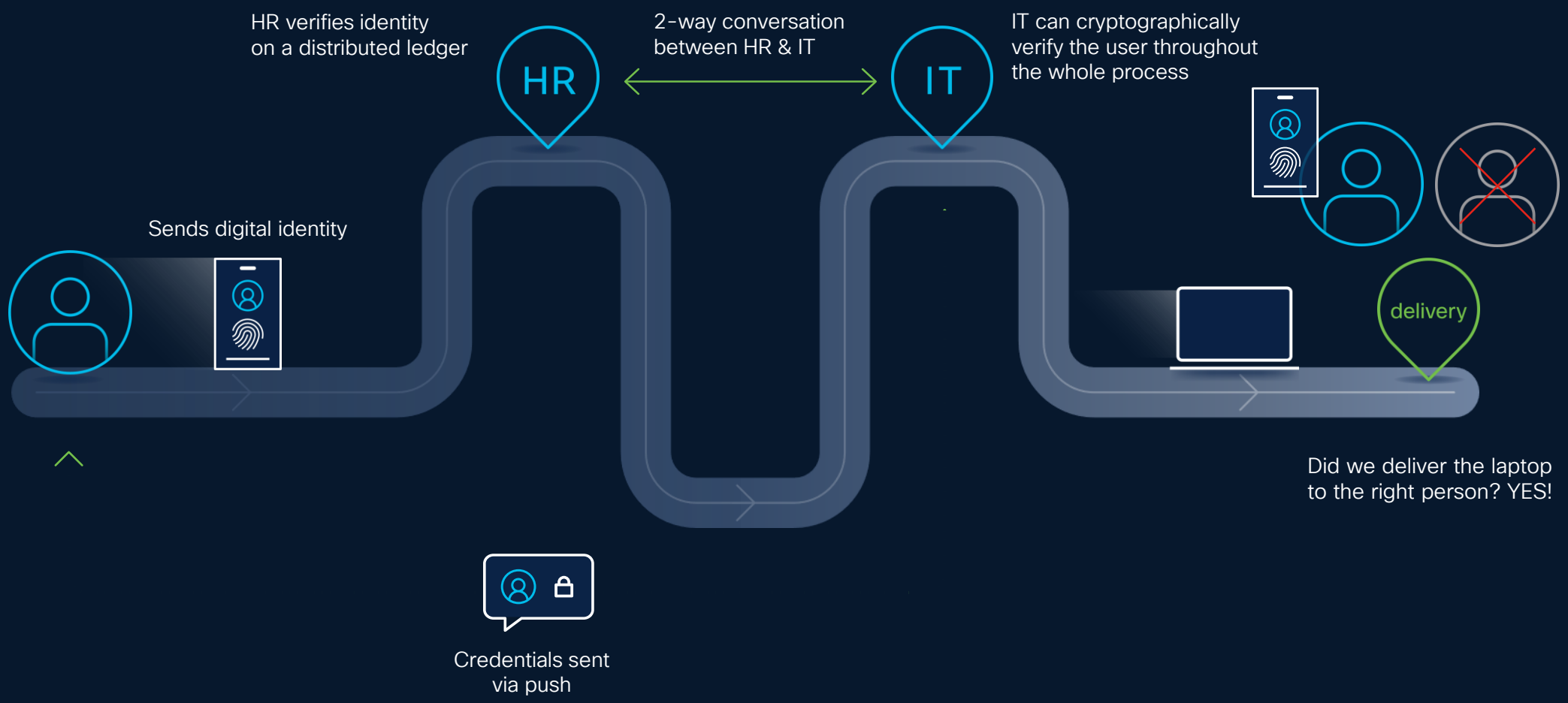
© 2025 Cisco and/or its affiliates. All rights reserved.

Jill onboards at ACME - Today



© 2025 Cisco and/or its affiliates. All rights reserved.

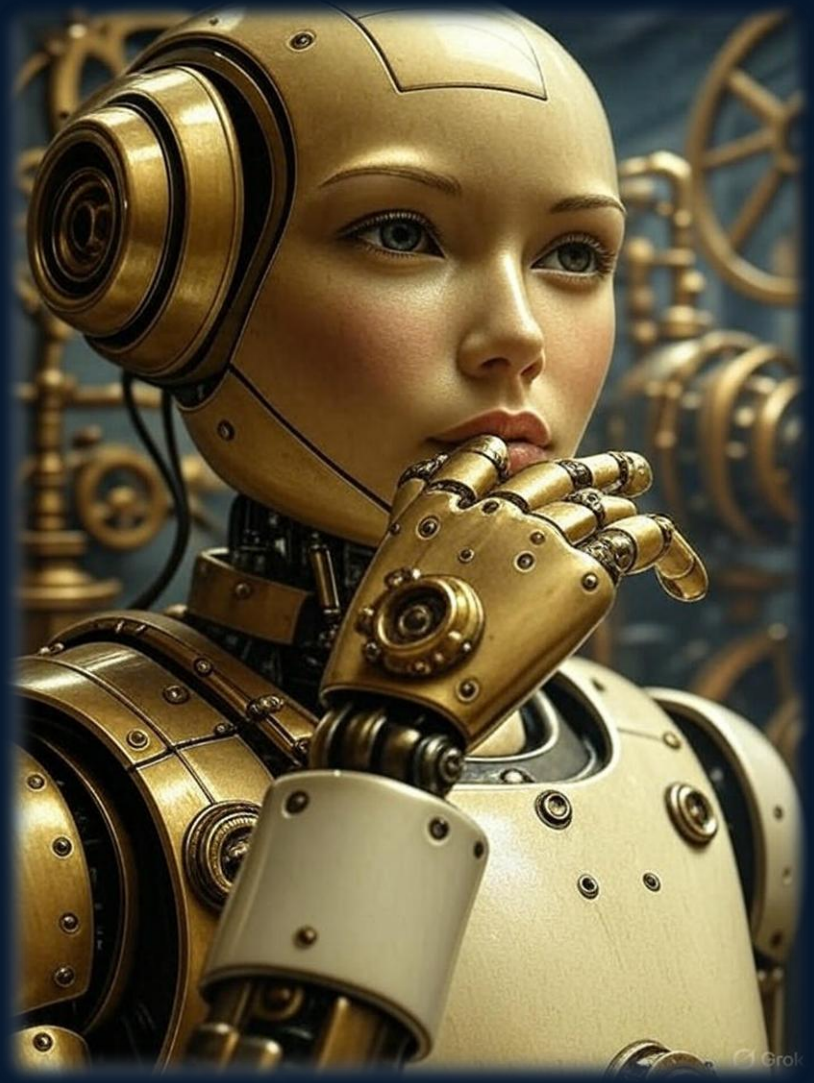
Jill onboards at ACME - Tomorrow



© 2025 Cisco and/or its affiliates. All rights reserved.

More Future Goodness

Non-Human Identity (NHI)



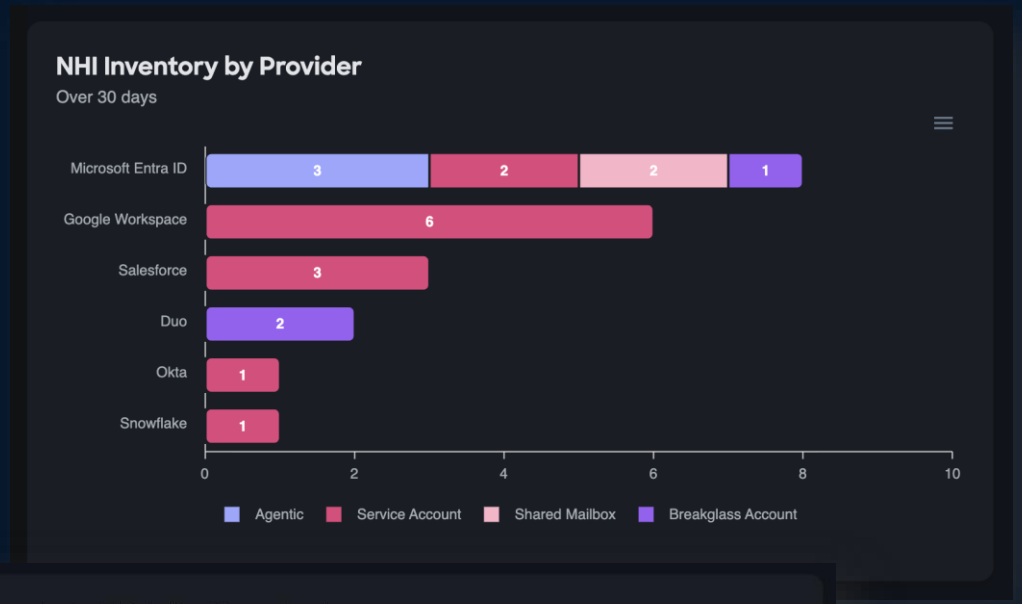
This is NOT NEW! Seems that the industry just woke-up to it!

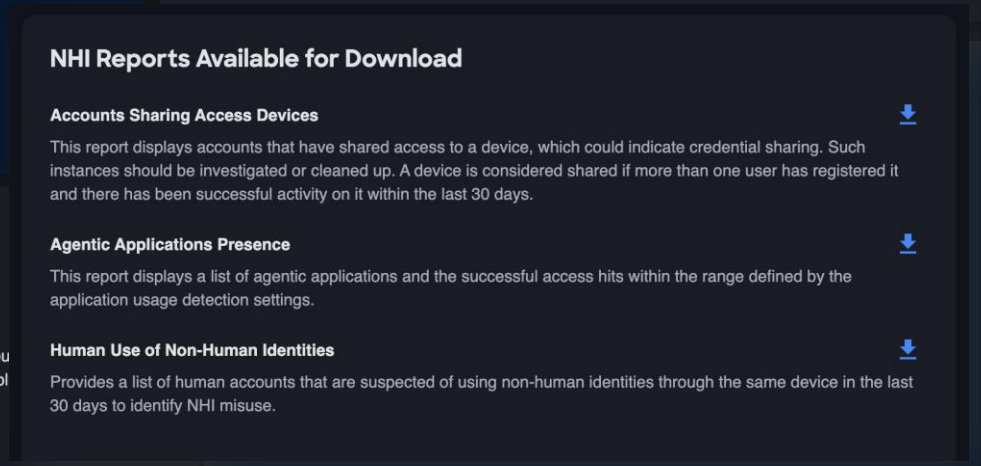
- Humans aren't the only entities with identities
  - Machine Identities.
  - Workload Identities.
- For example, look at the Webex rooms & do they have "LoxxBot" in them?
- Is an agent/bot that acts with API keys tied to me as a human.
- Like services accounts.
  - They have so many permissions – do we know which human to tie those service accounts to?

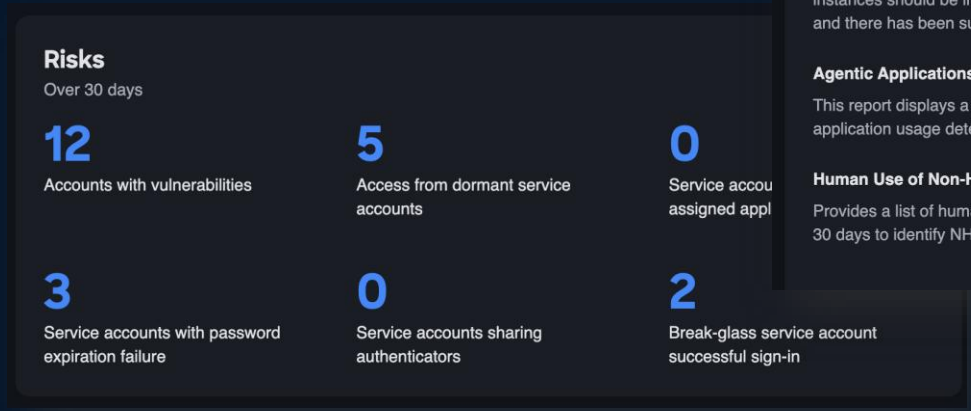
© 2025 Cisco and/or its affiliates. All rights reserved.

NHI Dashboard

- CII Identifies Non-Human Identities
  - Service Accounts (where possible)
  - Attempts to Identify Risks
- Offers direct download of reports related to NHI's from the Dashboard
  - These require deeper queries into the system & are then offered as CSV Exports

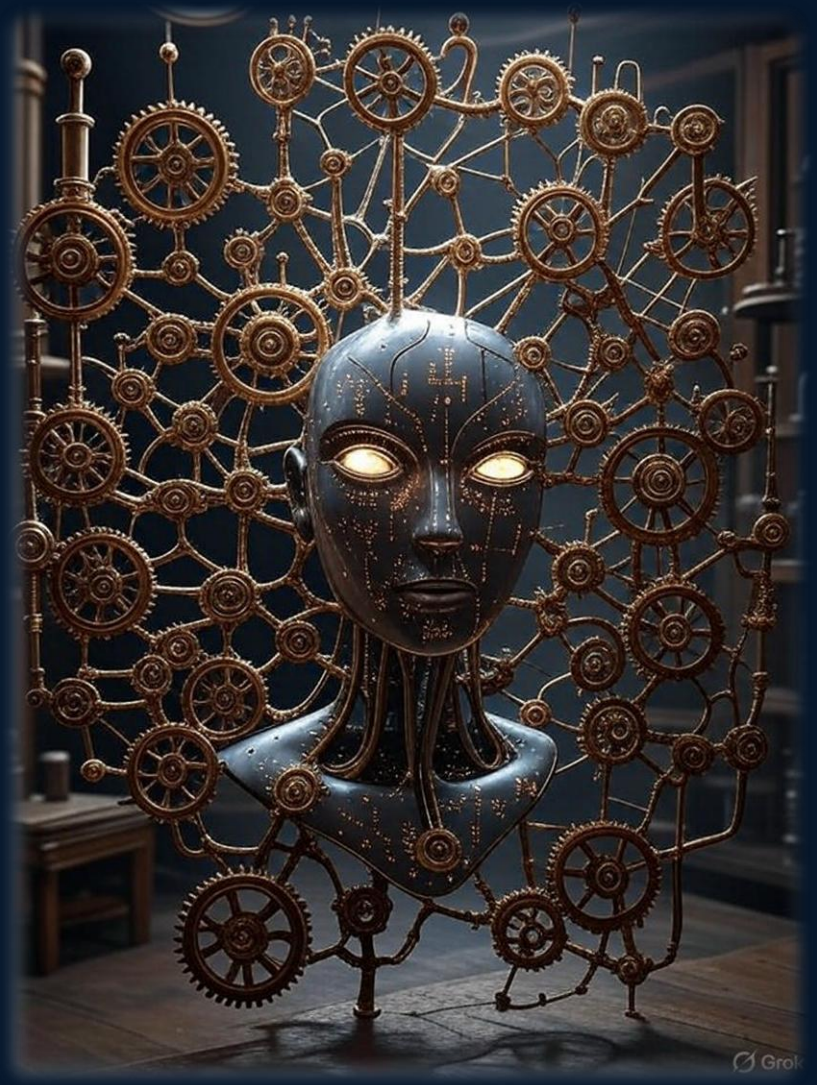






© 2025 Cisco and/or its affiliates. All rights reserved.

Cannot have a preso today without mentioning “AI” ☺



Agentic AI – where AI agents are acting on behalf of humans.

- Think about OAuth. A human can authorize an agent to act, with their level of permissions and rights.
- How do I know if Aaron did this, or if an Agent did this on behalf of Aaron.

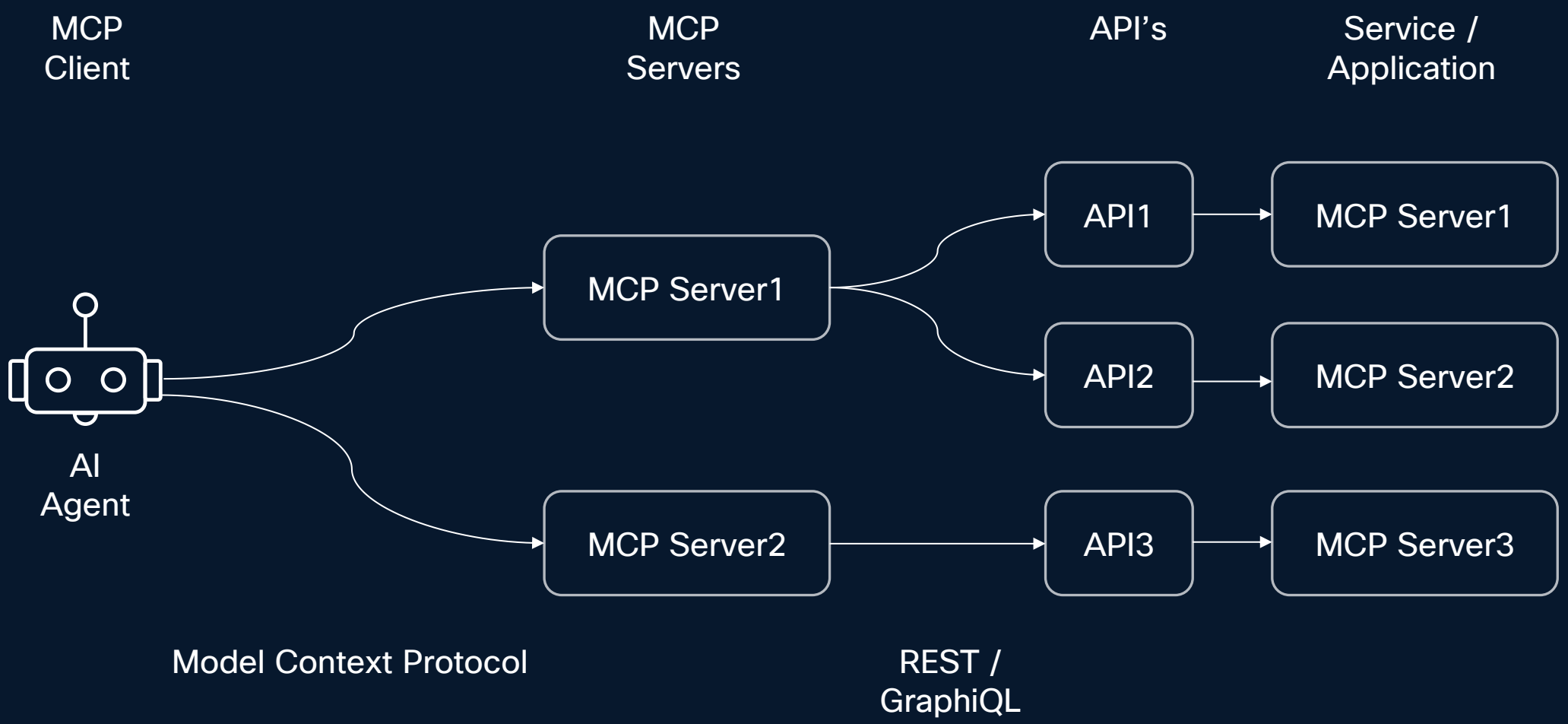
© 2025 Cisco and/or its affiliates. All rights reserved.

New Vocabulary Terms for AI

- MCP – Model Context Protocol
  - The MCP Server knows about the APIs or other resources it is programmed for.
  - When an MCP Client (agent) is looking for information / answers, it can look into any of the LLMs it is connected to but also can query the MCP Servers for the types of information they can answer.
  - Connects AI to the outside world: It allows AI models to access things like databases, APIs (Application Programming Interfaces), file systems, and other applications.
  - Enables AI to perform actions: This means AI agents can do more than just generate text; they can retrieve specific data, send emails, create calendar events, manage code, or even control network devices.

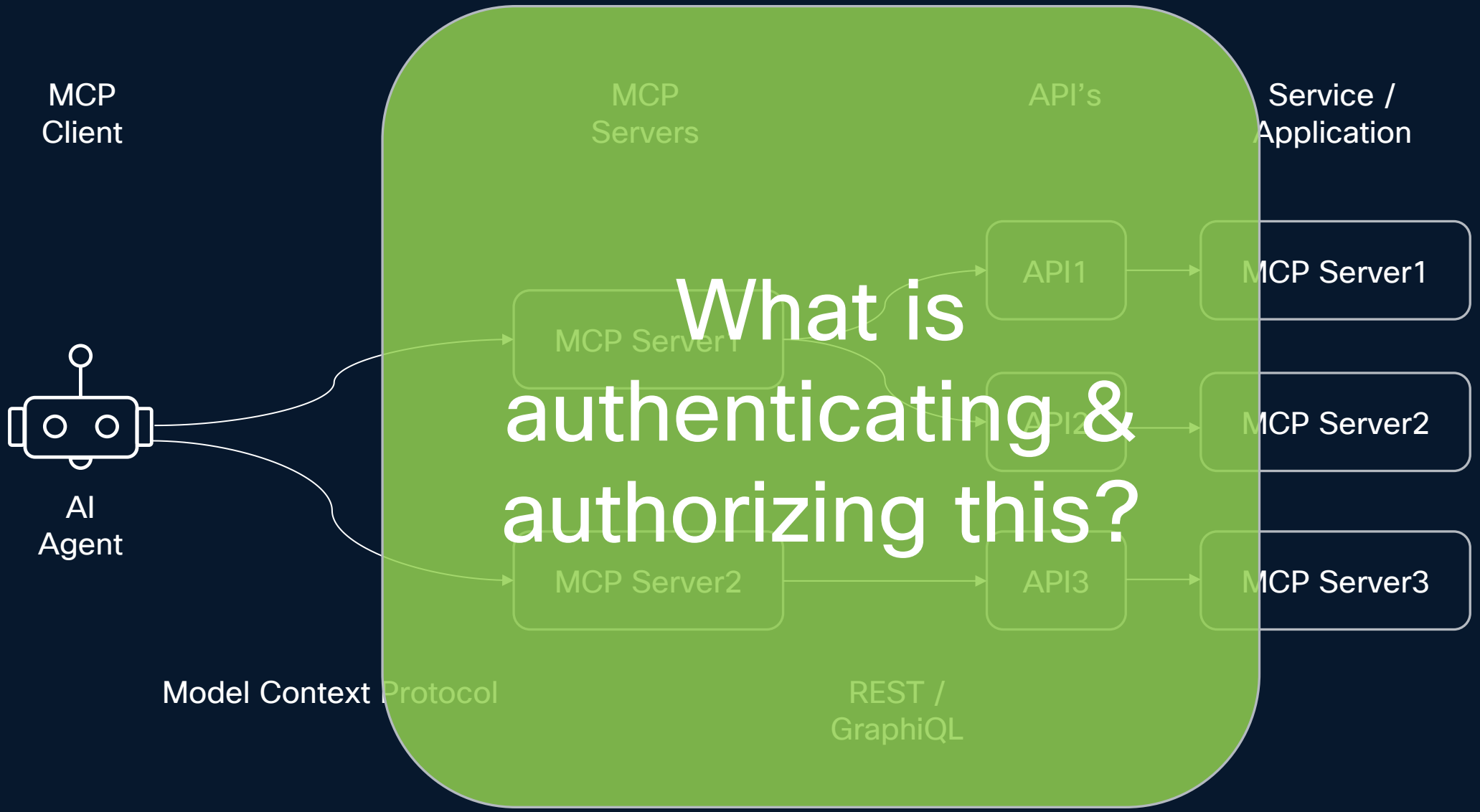
© 2025 Cisco and/or its affiliates. All rights reserved.

MCP Comms & Components in a Nutshell



© 2025 Cisco and/or its affiliates. All rights reserved.

MCP Comms & Components in a Nutshell



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Extending Authorization for an Agentic AI World

- OAuth 2.1 Enhances Security for Agentic AI
  - Removes insecure Grant Types
  - Mandates PKCE (Proof Key for Code Exchange) - ensuring only the client that initiated the request can exchange the code for a token
  - Requires exact matching of redirect URIs (no wildcards or partial matches) to prevent attacks where malicious URIs are used
  - Removes Long-Lived Token Support, pushing for Refresh Token Rotation after every use
  - Used for centralized authorization
- SPIFFE (Secure Production Identity Framework for Everyone)
  - Each workload gets a unique Cryptographic ID (Certificate or JWT)
  - A SPIFFE ID is a standardized format for identifying workloads. It looks like: spiffe://trust-domain/workload-path.
    - The “trust domain” defines a group of workloads that trust each other (e.g., a company’s infrastructure).
  - Meant for workload-to-workload distributed auth
- SPIRE (SPIFFE Runtime Environment)
  - Reference implementation of SPIFFE

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Agenda

01 Introduction
02 History & AAA
03 Enter: Single-Sign-On
04 SAML
05 OAuth & OIDC
06 WebAuthN & Passkeys
07 Gotcha's
08 Identity Security's Bright Future
09 Conclusion(s)

© 2025 Cisco and/or its affiliates. All rights reserved.

Conclusion(s)

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, but keep an eye to the future w/ Verifiable Credentials
- Duo makes Identity Easy and Secure
- You had fun in this session, even though the topic is boring

© 2025 Cisco and/or its affiliates. All rights reserved.

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
- How Certificate Authentication Works: https://blog.woland.com/2014/03/03/how-does-certificate-based-authentication-actually-work/

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

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

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education

Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: Insert preferred comms method

© 2025 Cisco and/or its affiliates. All rights reserved.

Please fill out the Survey

If there is anything we can improve, please let us know!

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

CISCO