The bridge to possible

Taking Authentication to the Next Level with Cisco Secure Access by Duo

Stefan Dürnberger
Technical Solutions Architect
CCIE Security #16458

Session Objectives

We are all looking for a secure and easy way to authenticate users when accessing applications. This session is about how Duo makes this process convenient and inherently secure. We will have a closer look at how Duo Passwordless works, explore new product enhancements like OIDC (OpenID Connect) and risk-based authentication to name just a few. This intermediate session is targeted at Security Architects and Security Admins that want to get a deeper understanding of various AuthN flows supported by Duo Security.

Agenda

- Authentication methods
  - FIDO2
- OpenID Connect & Duo CloudSSO
- Recent, major Duo enhancements
  - Risk-based Authentication
  - User Attribute Transformation
- Wrap Up

Cisco Webex App

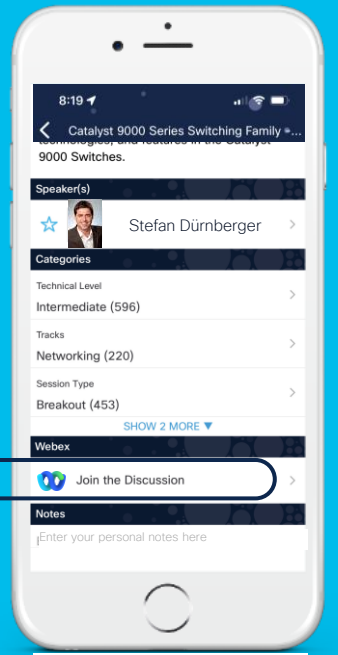
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2748

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

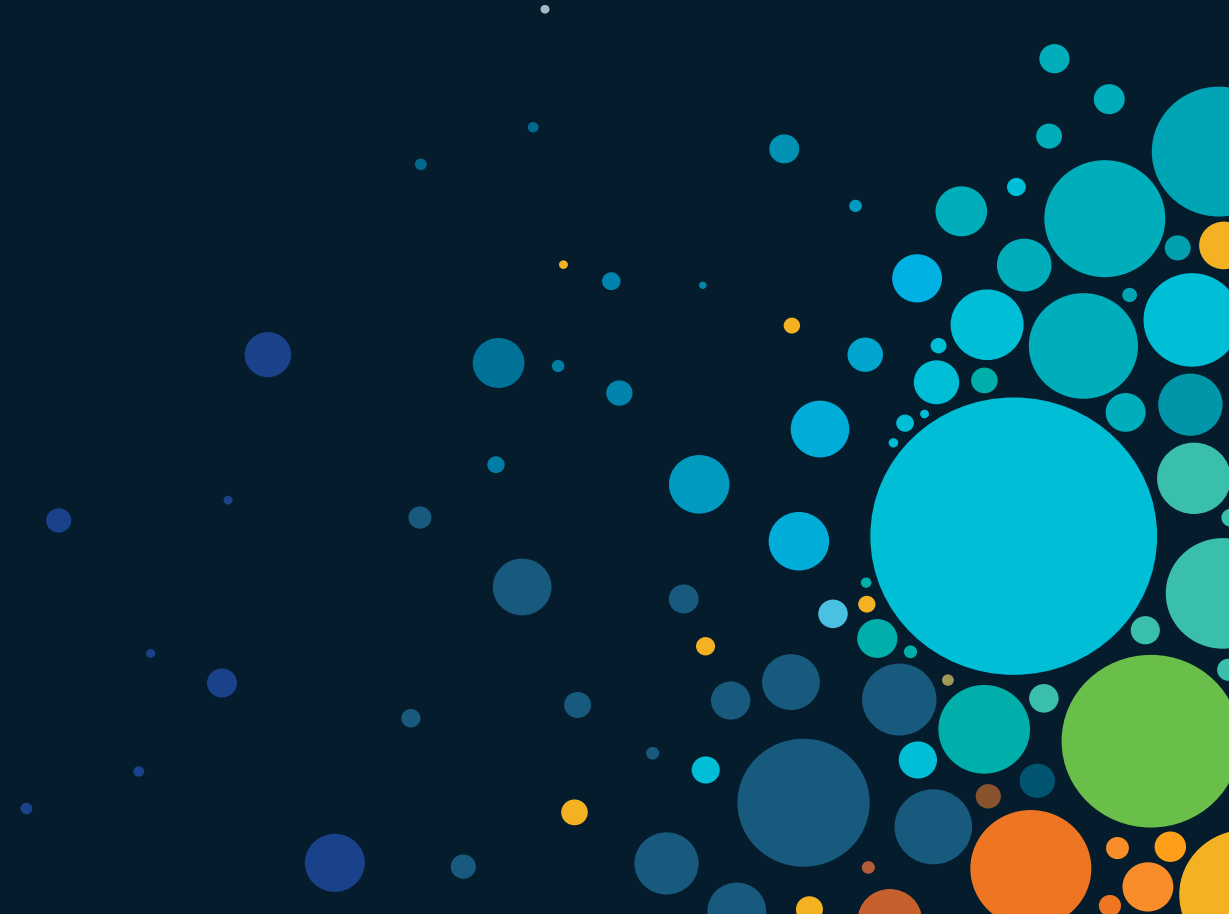


Webex spaces will be moderated until February 24, 2023.

About me

- Stefan Dürnberger – sduernbe@cisco.com
  - 23 years in IT, 18 years in IT Security
  - 15+ years at Cisco
- A so and so football player & coach, love rock music, like to be outside, craftsman (not qualified but ambitious), being a poor programmer

Introduction



Graphic: https://danielmiessler.com

MFA Methods

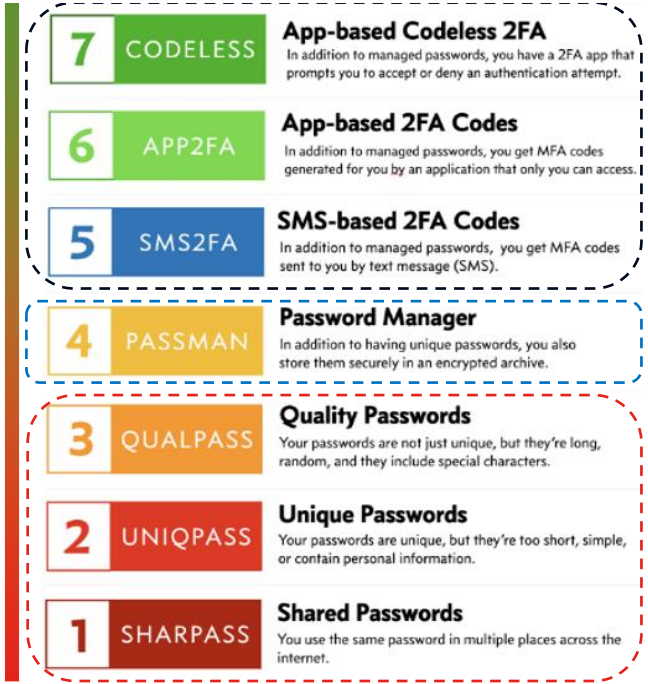
- Phishing is a low-skill, low-cost attack You just order a service
- Regardless what you do, you share a secret
- Password reset cost ~70$

Graphic: https://danielmiessler.com

MFA Methods

- Risk based Auth
- Step Up
- Verified Push

- Phishing is a low-skill, low-cost attack You just order a service
- Regardless what you do, you share a secret
- Password reset cost ~70$



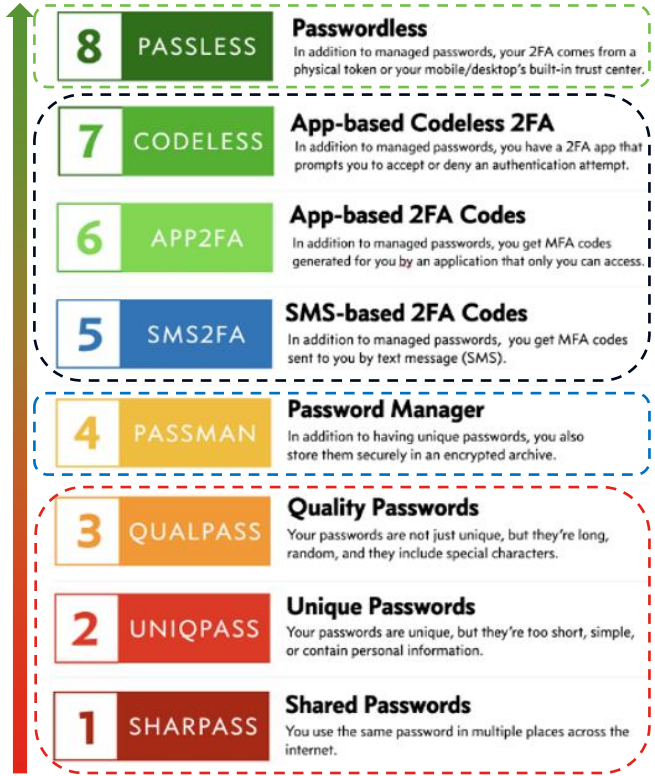
Evilproxy is a Proxy as a Service for phishing

Graphic: https://danielmiessler.com

MFA Methods

- Risk based Auth
- Step Up
- Verified Push

- Phishing is a low-skill, low-cost attack You just order a service
- Regardless what you do, you share a secret
- Password reset cost ~70$



Take care of backup authentication method. Think about a single, lost authenticator.

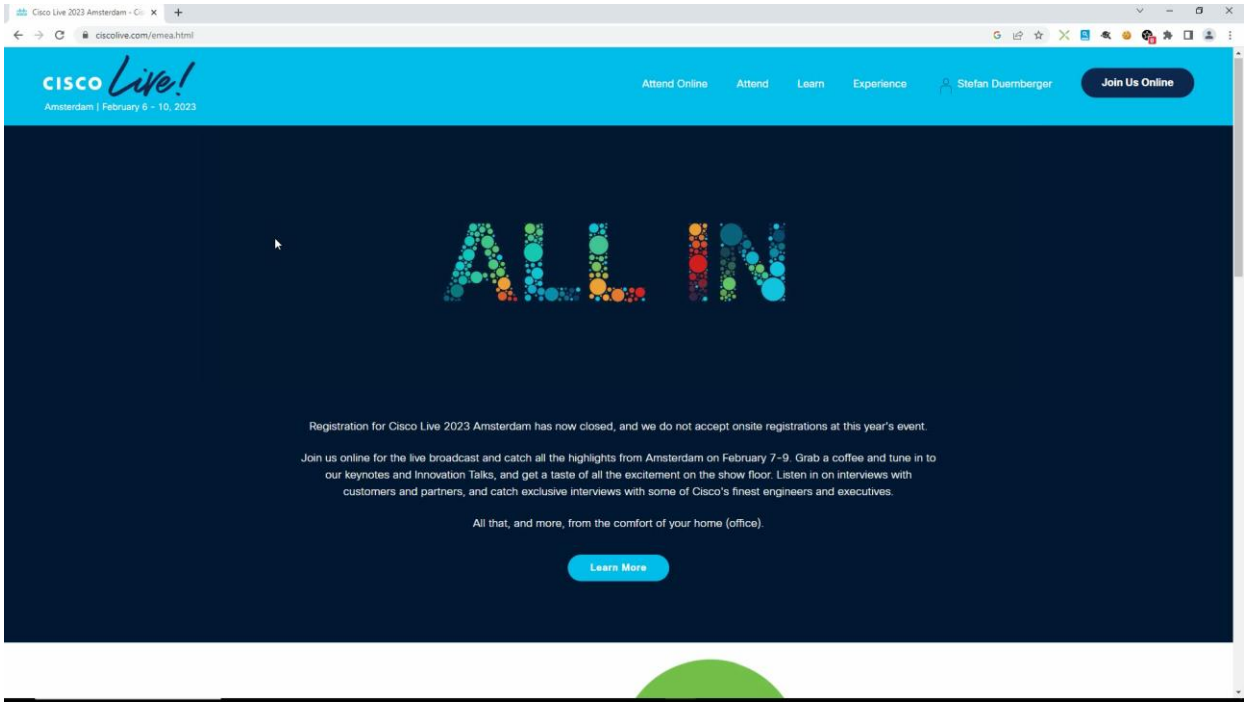
Evilproxy is a Proxy as a Service for phishing

FIDO2 & Duo

Fast IDentity Online (FIDO2)

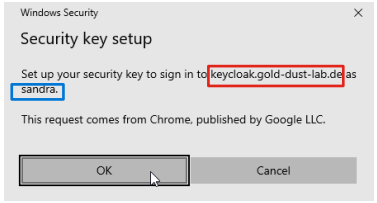
Overview

- FIDO2 provides secure, phishing resistant and convenient way of authentication to web services supporting the standard.
  - CISA urges to implement phishing resistant authentication like FIDO2: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- The goal is to have an open authentication standard which offers something you have & something you know and/or something you are.
  - FIDO2 authentication can be used as a 2nd factor, or being used for passwordless, or name & passwordless authentication



Fast IDentity Online (FIDO2)

Registration Ceremony (simplified)



Initial User Authentication

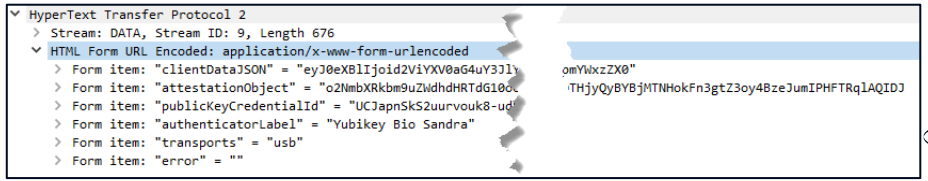
HEADERS[5]: POST /realms/Cisco_Live/login-actions/registrati… …d=Nextcloud&tab…
DATA[5] (application/x-www-form-urlencoded)

Challenge: User Info, RP_ID, Attestation optional: Authenticator Selection

```
// mandatory parameters\n
let challenge = "OtWB3eHAQf2nhQx8BCXAHQ";\n
let userid = "ZDc4OGExN2QtYjJmZi00NmJjLWJkYTEtNzgzMWIyNzQ2MmZ]";\n
let username = "sandra";\n
```

Make Cred Call: RP_ID, UserID, Options + originID

POST HTTP1.1 Signed Challenge

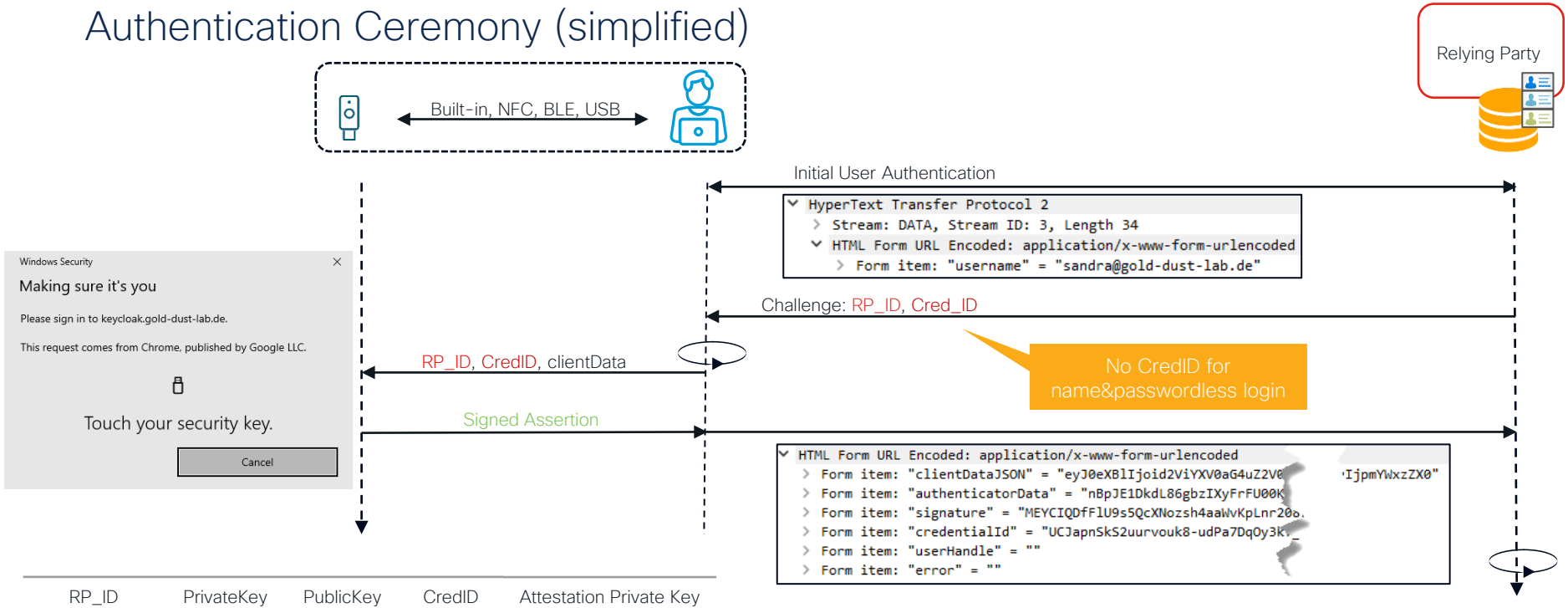


RP_ID	PrivateKey	PublicKey	CredID	Attestation Private Key
example.com	ABCDEF	12345	XYZ	AEI89AG

UserName	UserID	PublicKey	CredID
Stefan	AG87AR	12345	XYZ

Fast IDentity Online (FIDO2)

Authentication Ceremony (simplified)

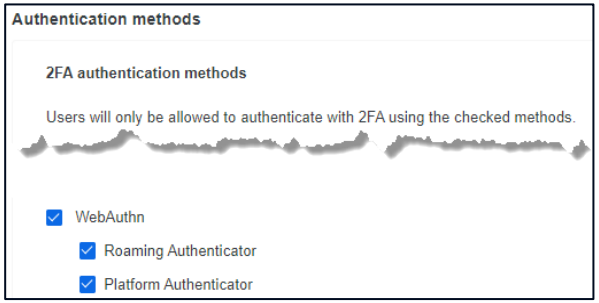


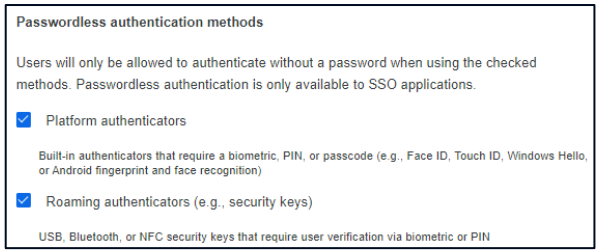
RP_ID	PrivateKey	PublicKey	CredID	Attestation Private Key
example.com	ABCDEF	12345	XYZ	AEI89AG

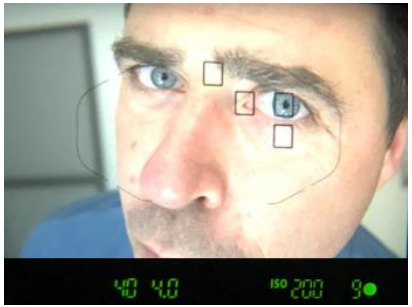
UserName	UserID	PublicKey	CredID
Stefan	AG87AR	12345	XYZ

Fast IDentity Online (FIDO2)

- Duo supports FIDO2 authentication for Passwordless and 2FA
  - Platform & Roaming authenticators
  - No Attestation Certificate validation, nor Enterprise Attestation validation
- User Presence vs User Verification

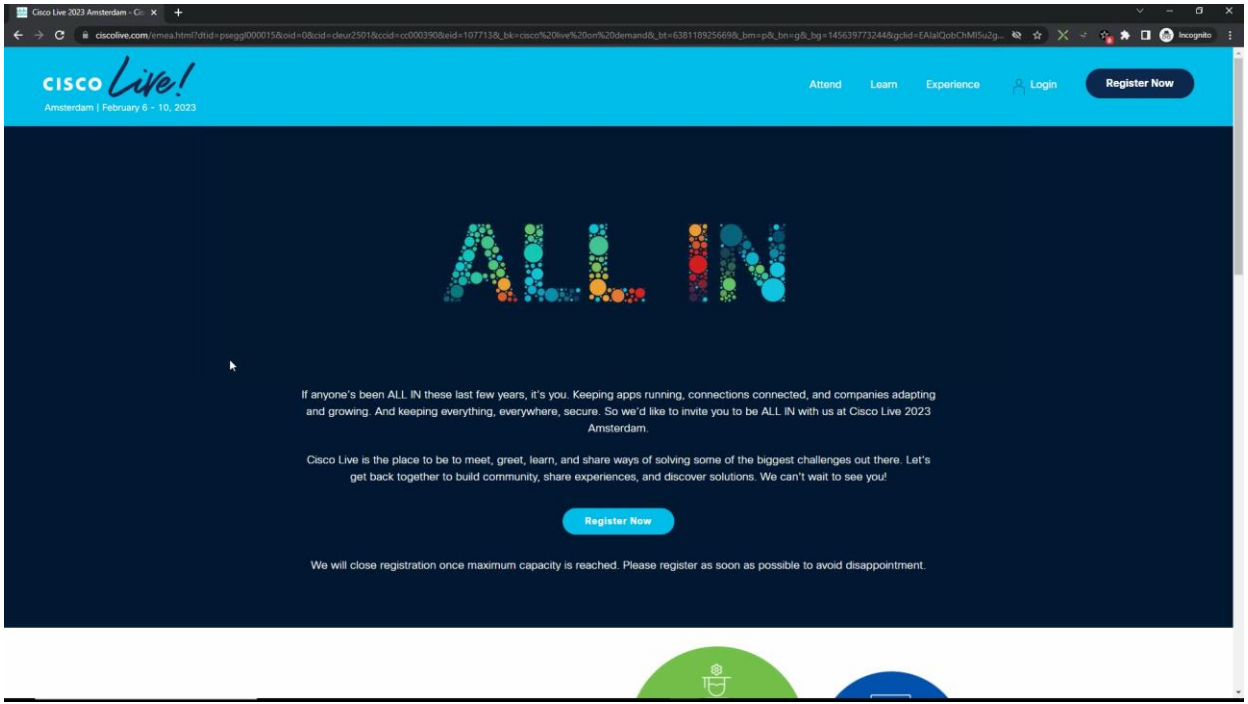






FIDO2 authentication – use cases

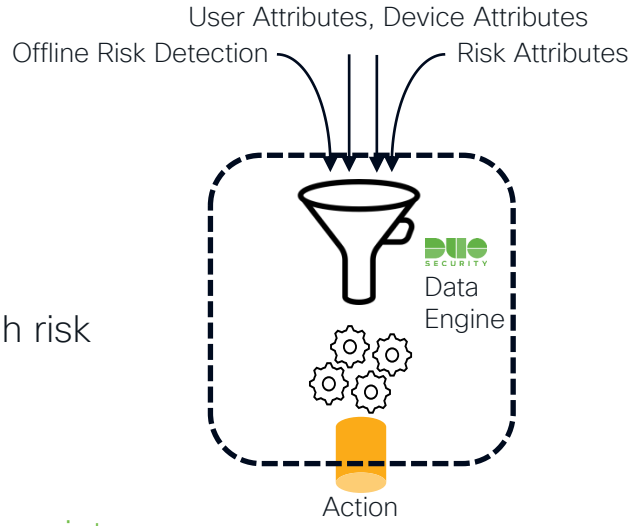
cisco Live!

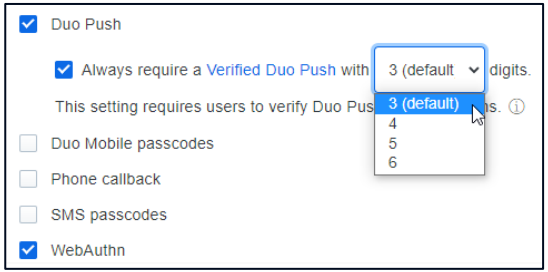


Risk-Based Authentication

Risk-Based Authentication

- Detects known attack patterns
  - Push harassment, Push fatigue, Push spray as well as high risk login location
- Processes historical statistics
  - Device IP, Browser Agent String, Time of Day, Wi-Fi Fingerprint
- Risk-Based Remembered Device & Factor Selection





Risk-Based Authentication

Push Harassment

✓ Granted Push answered with correct verification code	key	Less trusted	› Windows 10, version 21H2 (19044.2251) As reported by Device Health	› Verified Duo Push Sankt Wendel, SL, Germany ⚠ Step-up 2FA
✕ Denied No response	whiskey	Normal	› Windows 10, version 21H2 (19044.2251) As reported by Device Health	› Duo Push Location Unknown
✕ Denied No response	whiskey	Normal	› Windows 10, version 21H2 (19044.2251) As reported by Device Health	› Duo Push Location Unknown
✕ Denied No response	whiskey	Normal	› Windows 10, version 21H2 (19044.2251) As reported by Device Health	› Duo Push Location Unknown
✕ Denied No response	whiskey	Normal	› Windows 10, version 21H2 (19044.2251) As reported by Device Health	› Duo Push Location Unknown

Less trusted

Reasons

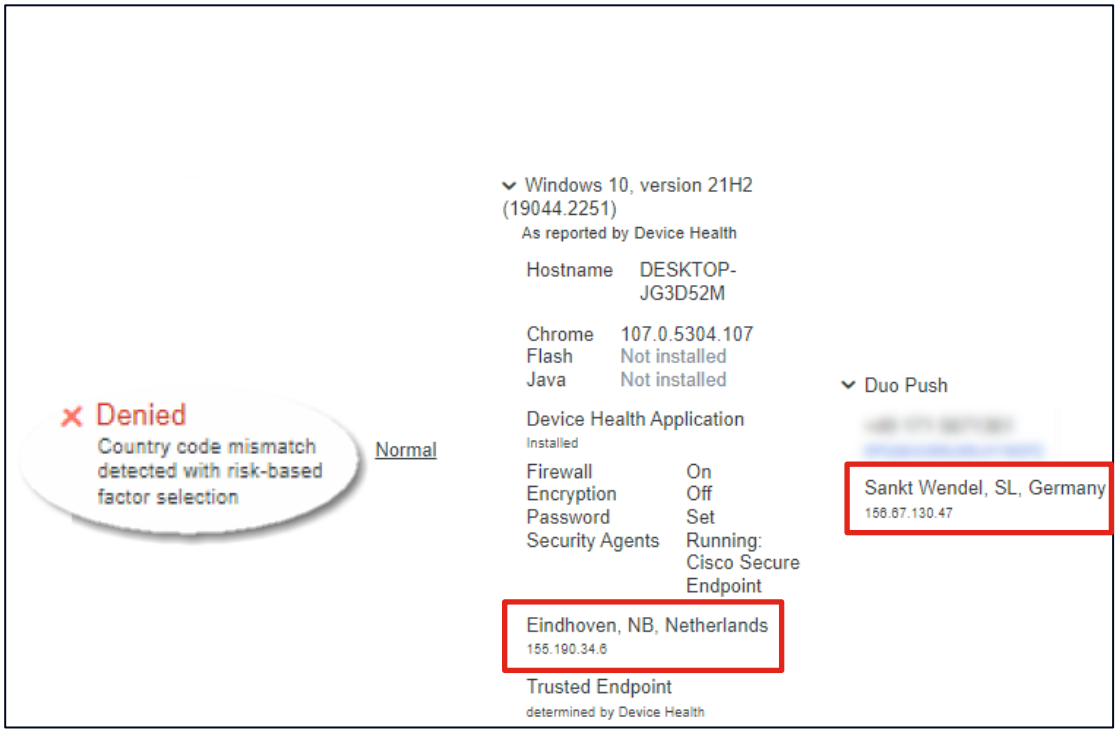
Authentication methods were limited due to the detection of consecutive failed authentication attempts.

Policies

Risk-based factor selection policy was enforced.

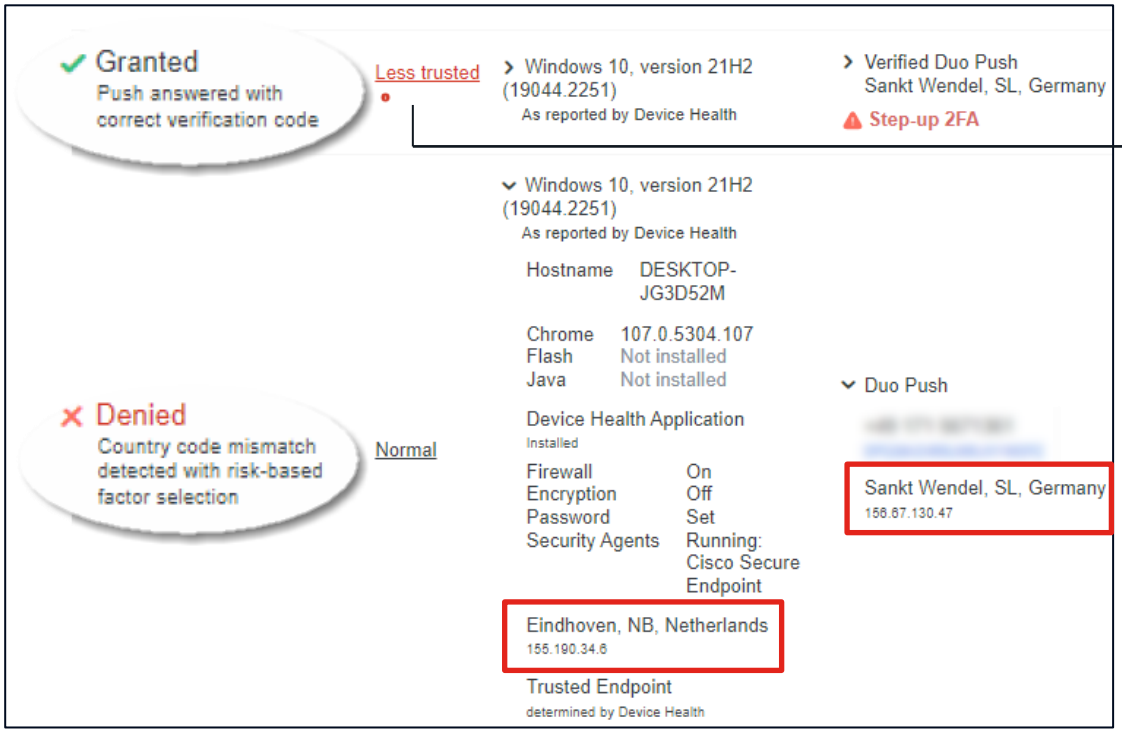
Risk-Based Authentication

Country code mismatch detection



Risk-Based Authentication

Country code mismatch detection



Less trusted

Reasons

Authentication methods were limited due to the detection of a country code mismatch (mismatch in country codes of the access and authentication device).

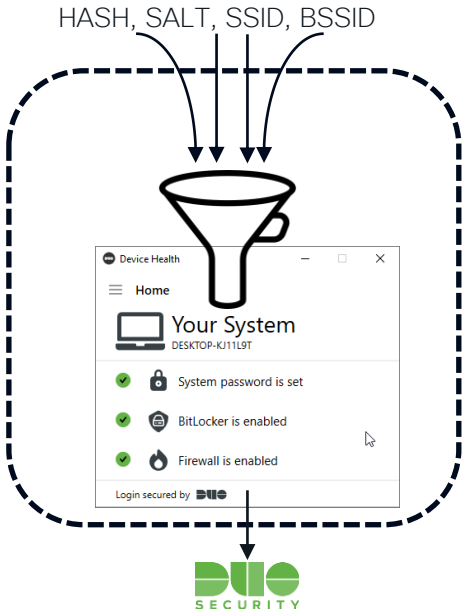
Policies

Risk-based factor selection policy was enforced.

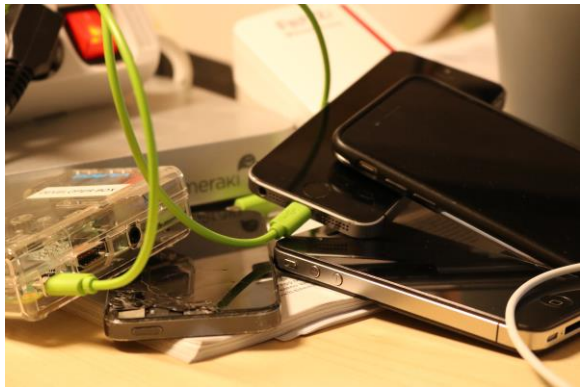
Risk-Based Authentication

Wi-Fi Fingerprint

- Anonymized Wi-Fi network data provides a strong signal of novel location. Takes advantage of Duo Device Health Application (DHA)
  - Client-side hashing
  - Unique key eliminates reply-attacks
- A deviation from the familiar/usual working location towards an unfamiliar location triggers a step-up in the sense of using only “more secure AuthC factors”
  - Familiar Wi-Fi fingerprint reduce the step-ups, while unfamiliar Wi-Fi fingerprints increase them



During testing, I was certainly at a different place ☺

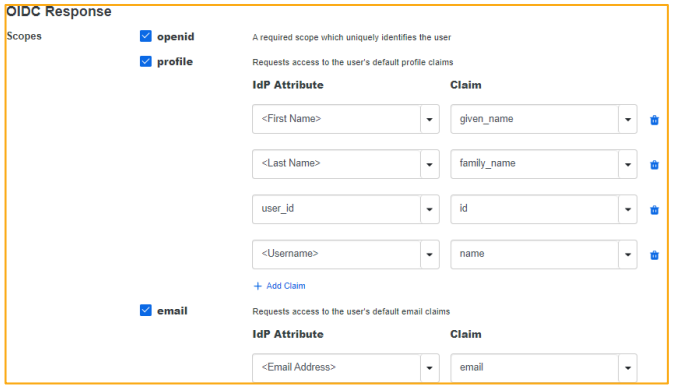


OpenID Connect (OIDC)

OIDC

Fundamentals

- Differences between SAML, OAuth
  - Filling missing gaps of OAuth2.0 (OAuth2)
- In OIDC, scopes are used by clients to authorize access to user´s resources
  - Claims are attributes about the identity itself
- OIDC uses access tokens and ID tokens (JSON web token, JWT)
- OIDC flows support a variety of use cases
  - Identifies users from mobile applications, SPA. Support for Machine to Machine Authentication & Authorization. Duo supports Authorization Code flow & Client Credentials in Early Access Mode



OIDC

Roles

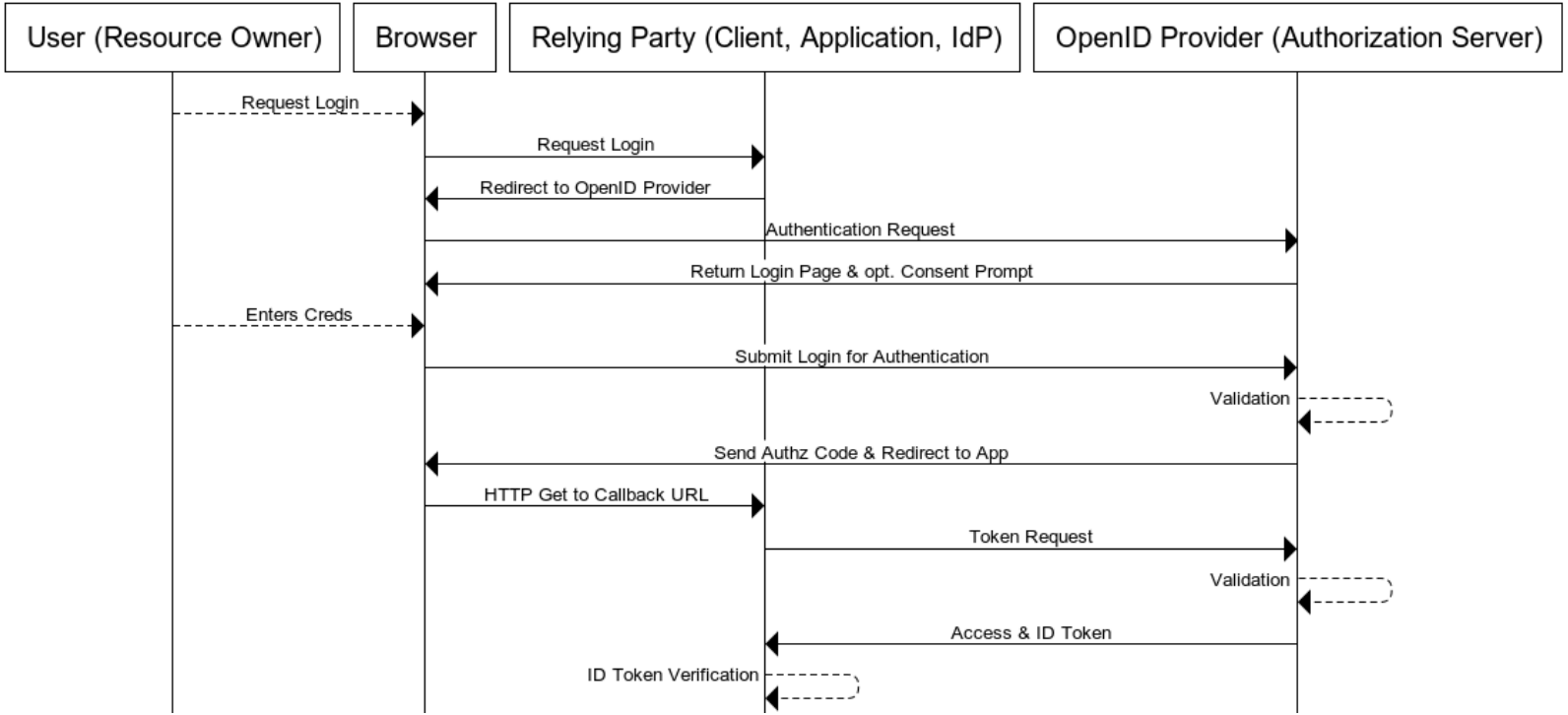
- Resource Owner
  - That´s you!

- Client/Relying Party
  - Application i.e., Browser, App

- OpenID Provider/Authorization Server
  - Duo CloudSSO

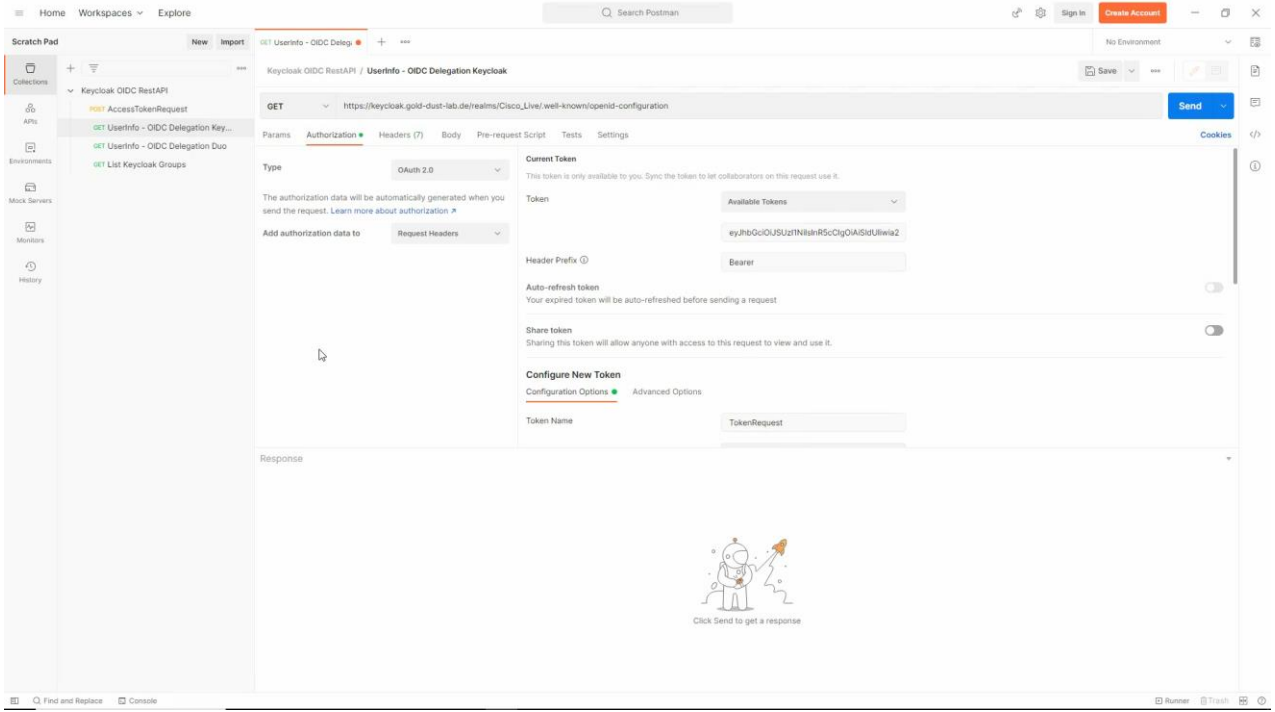
Actors in an OIDC dance

Authorization Code Flow

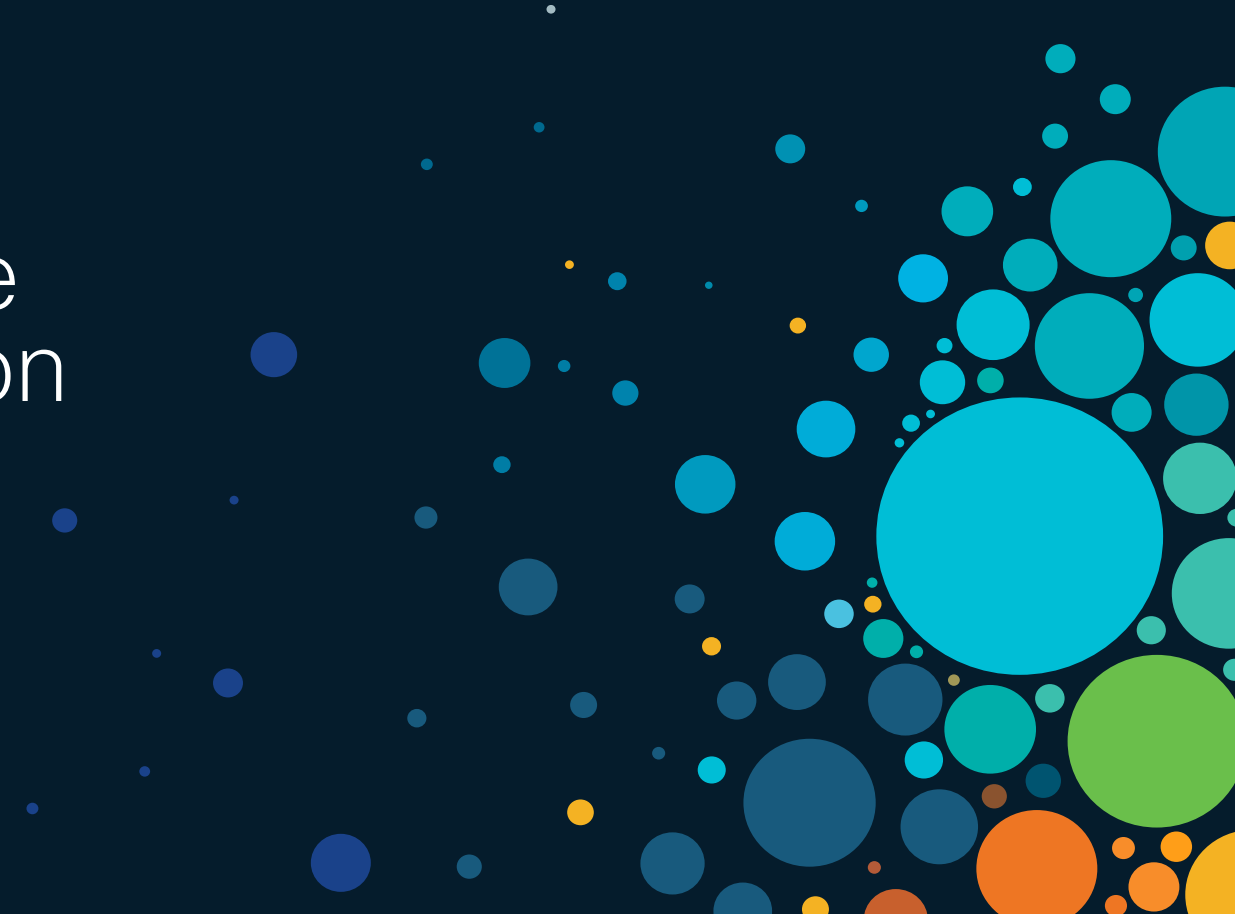


OIDC Demo

Postman



User Attribute Transformation



User Attribute Transformation

- User Attribute Transformation is a Duo CloudSSO feature
  - Available for Generic SAML SP applications
- Performs attribute modification before SAML assertion gets send out
- Using an expression language
  - $RULE_NAME $OPTION="$OPTION_VALUE"
  - Processing a list of rules from top to bottom

User Attribute Transformation

Use-Cases

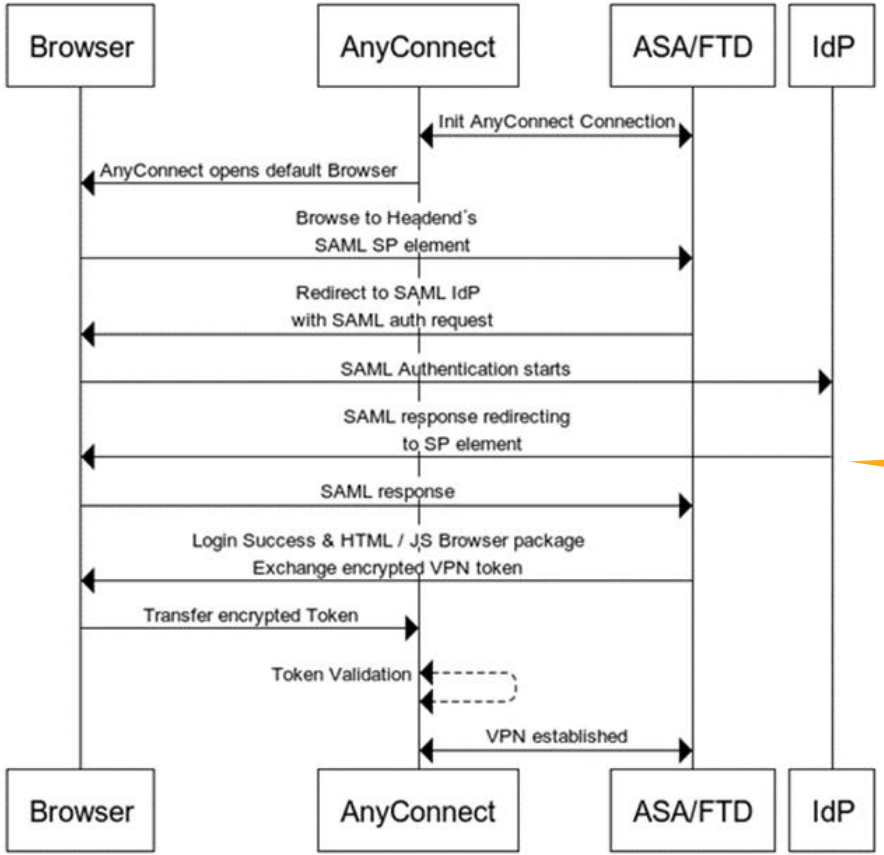
- Appending/Prepending a suffix to a username, mapping it to a SAML SP role
- Character transformation
  - Uppercase, Lowercase
- Cisco Anyconnect RAVPN group-policy can be specified by a SAML assertion attribute
  - When an attribute "cisco_group_policy" is received by the Secure Firewall, the corresponding value is used to select the connection group-policy
  - Optional: Can be used as part of Dynamic Access Policy

Cisco Anyconnect & User Attribute Transformation

Group-Policies & Dynamic Access Policies (DAP)

- A group policy is a set of user-oriented attribute/value pairs for RAVPN connections
  - Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user
- DAP allows granular access control to resources based on authentication method & authentication parameters
- Users can be assigned to a single Group-Policy but can use multiple DAP´s
  - DAP´s are aggregated

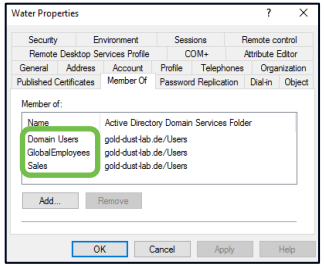
SAML Overview – Cisco Anyconnect ext. Browser



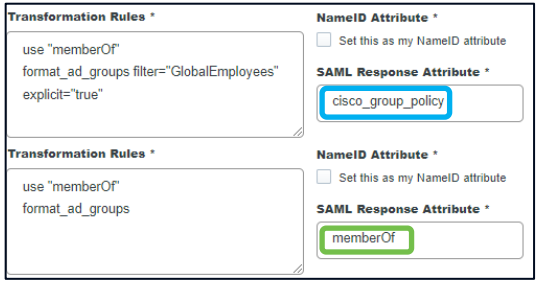
User Attribute Transformation happens at this stage!

SAML AuthZ

A practical use-case

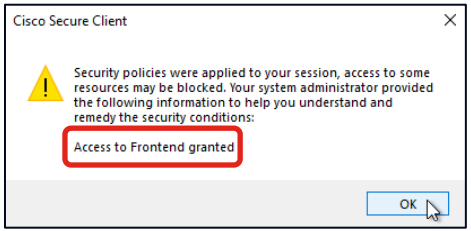


Duo CloudSSO




```
aaa["saml"]["memberOf"]["1"]="Sales"

aaa["saml"]["memberOf"]["2"]="GlobalEmployees"

aaa["saml"]["cisco_group_policy"]="GlobalEmployees"

aaa["saml"]["_cisco_saml_uid_"]=water@gold-dust-lab.de
water@gold-dust-lab.de, dap_concat_fcn: [Access to Frontend granted] 26 490
Classifying FrontendACL: priority=0, sense=0(White), Denies=0, Permits=1
```

```
FP2120# show vpn-sessiondb anyconnect

Username     : water@gold-dust-lab.de
Group Policy : GlobalEmployees
Tunnel Group : SAML_SingleCert_CloudSSO
```

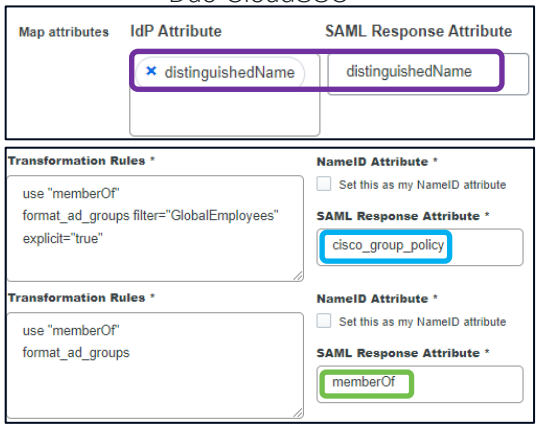


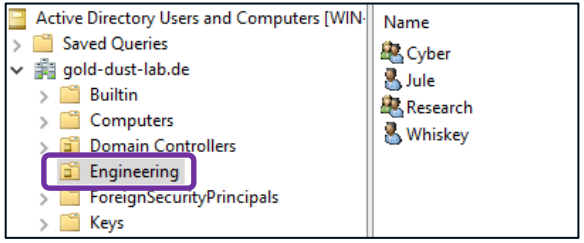

```
FP2120# show running-config dynamic-access-policy-record Frontend-Access
dynamic-access-policy-record Frontend-Access
 user-message "Access to Frontend granted"
 network-acl FrontendACL

FP2120# more disk0:/dap.xml
<dapRecordList>
  <dapRecord>
    <dapName>
      <value>Frontend-Access</value>
    </dapName>
    <dapViewsRelation>
      <value>and</value>
    </dapViewsRelation>
    <dapBasicView>
      <dapSelection>
        <dapPolicy>
          <value>match-all</value>
        </dapPolicy>
        <attr>
          <name>aaa.saml.cisco_group_policy</name>
          <operation>EQ</operation>
          <value>GlobalEmployees</value>
        </attr>
        <attr>
          <name>aaa.saml.memberOf</name>
          <operation>EQ</operation>
          <value>Sales</value>
        </attr>
```

SAML AuthZ

A practical use-case

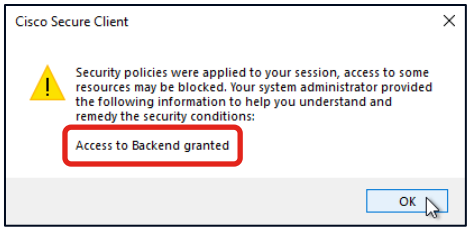
Duo CloudSSO






```
aaa["saml"]["distinguishedName"]="CN=Whiskey,OU=Engineering,DC=gold-dust-lab,DC=de"

aaa["saml"]["memberOf"]["1"]="SystemsEngineering"
aaa["saml"]["memberOf"]["2"]="GlobalEmployees"

aaa["saml"]["cisco_group_policy"]="GlobalEmployees"

aaa["saml"]["_cisco_saml_uid_"]="whiskey@gold-dust-lab.de"
whiskey@gold-dust-lab.de, dap_concat_fcn: [Access to Backend granted] 25 490
Classifying BackendACL: priority=10, sense=0(White), Denies=0, Permits=1
```

```
FP2120# show vpn-sessiondb anyconnect

Username     : whiskey@gold-dust-lab.de
Group Policy : GlobalEmployees
Tunnel Group : SAML_SingleCert_CloudSSO
```

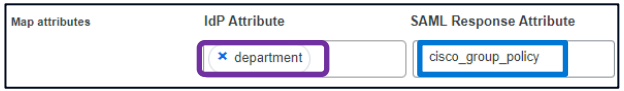


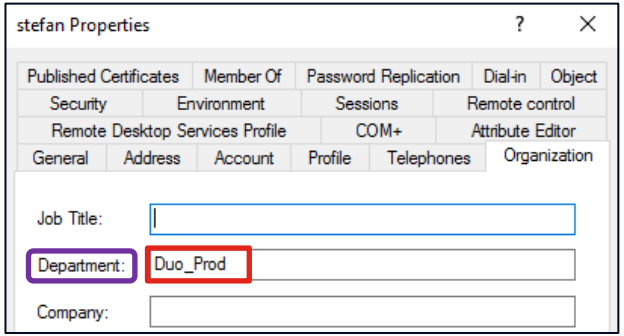

```
FP2120# show running-config dynamic-access-policy-record Backend-Access
dynamic-access-policy-record Backend-Access
 user-message "Access to Backend granted"
 network-acl BackendACL
 priority 10

FP2120# more disk0:/dap.xml
 <dapRecord>
    <dapName>
      <value>Backend-Access</value>
    </dapName>
    <dapViewsRelation>
      <value>and</value>
    </dapViewsRelation>
    <advancedView>
      <value>assert(function()&#13;
   if ( (type(aaa.saml.distinguishedName) ==
"string") and&#13;
        (string.find(aaa.saml.distinguishedName,
"OU=Engineering,DC=gold%-dust%-lab,DC=de$") ~= nil) )
then&#13;
       return true&#13;
   end&#13;
   return false&#13;
end)()</value>
    </advancedView>
    <dapBasicView>
      <dapSelection>
        <dapPolicy>
          <value>match-all</value>
        </dapPolicy>
        <attr>
          <name>aaa.saml.memberOf</name>
          <operation>EQ</operation>
          <value>SystemsEngineering</value>
        </attr>
```

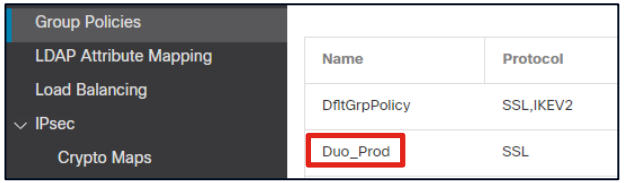
Expert Tip: % needs to be before the special character

Use-Case: Map Attributes

- Dynamic assignment of RAVPN group-policy based on directory attributes like department, city,...
  - Independent of Attribute Transformation!
- If an attribute with the name cisco_group_policy is received by the VPN headend, the corresponding value is used to select the connection group-policy
  - No match -> Default Group-Policy get´s assigned





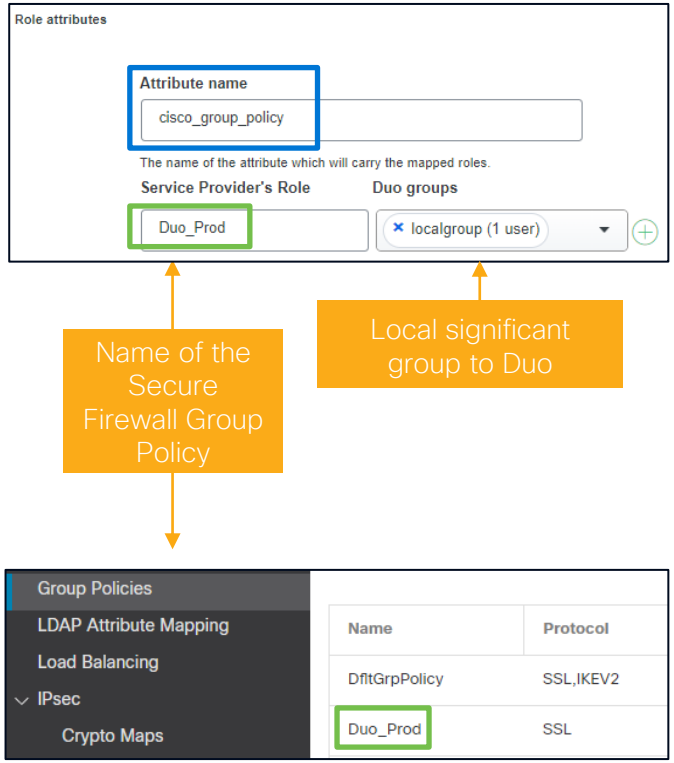


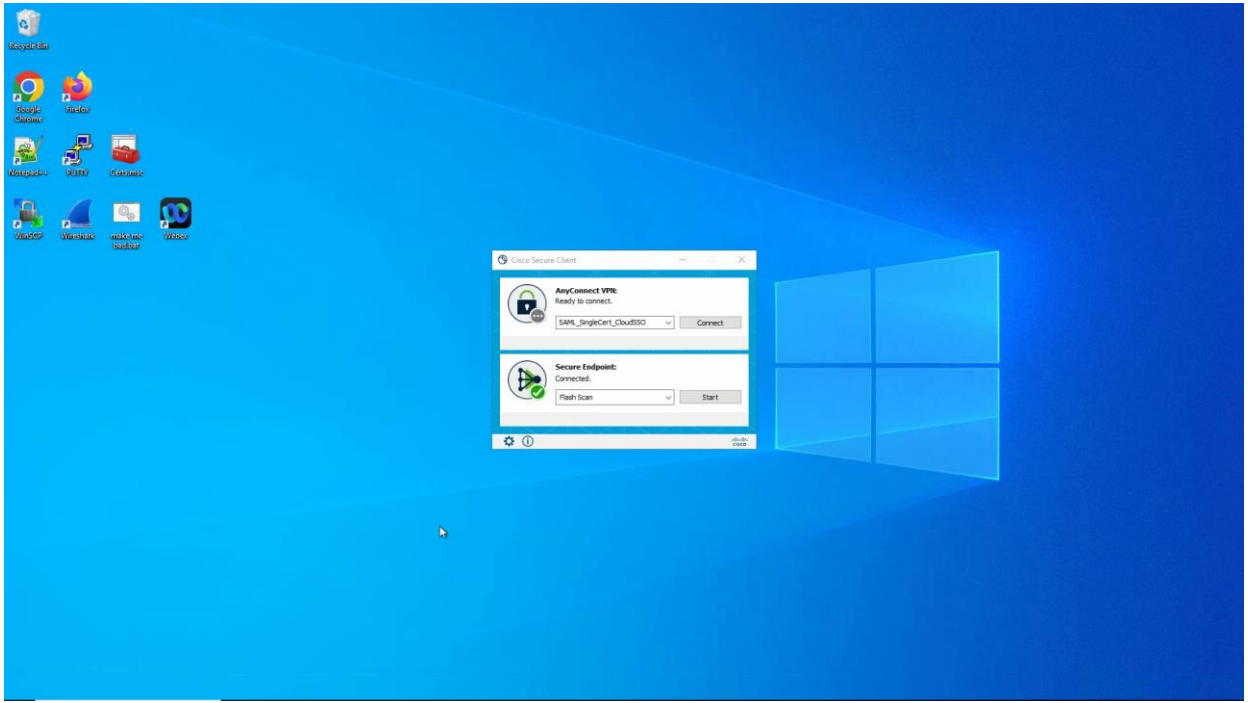

```
<saml:Attribute Name="cisco_group_policy" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" >
<saml:AttributeValue xsi:type="xs:string">Duo_Prod</saml:AttributeValue>
```

Role attributes

Use-Case

- Dynamic assignment of RAVPN group-policy w/o processing directory attributes
  - Independent of Attribute Transformation!
- If an attribute with the name cisco_group_policy is received by the VPN headend, the corresponding value is used to select the connection group-policy
- No match -> Default Group-Policy get´s assigned



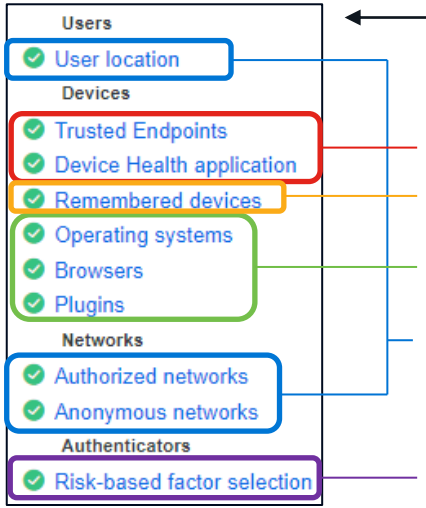


SAML Authentication

Anyconnect & Duo CloudSSO

- SAML authentication happens at an early stage
  - In case of Duo CloudSSO (IdP), this is where Duo policies gets processed, as well as where user attribute transformation happens

Note: Extraction of Duo´s Policy attributes but not limited to



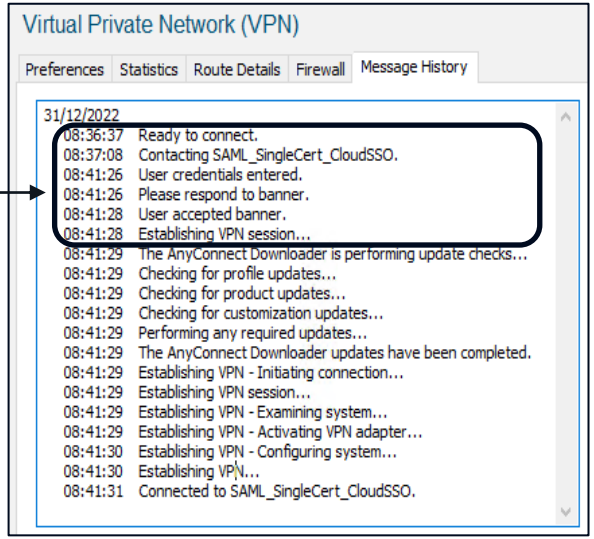
Device Compliancy (Posture, managed vs unmanaged)

Device Cookie

Client Device & Browser

L3 information (CIDR, Geo Info, Anonymizer, …)

Step-up Authentication



When processing high-value data, we have to have best in class security products for protection, a high-level assurance of who is accessing the data, continuously verifying the risk, and being able to control a session whenever a contextual change happens

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.
Meet the Speaker: Area 1 | 02/09/23 | 11:00 AM

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

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

A bit too early for beverages, but in case they serve later today in the World of Solutions, you can find me there!

Security Technologies

Zero Trust

Learn how Cisco will help you deploy a broad range of technologies in order to deploy your end to end Zero Trust strategy.

START.

Feb 5 | 16:00
LABSEC-2089
Multi-factor Authentication: Integration of DUO with ISE for MFA

Feb 6 | 08:45
TECSEC-2007
Find Your Zen with Cisco Secure Workload for Zero Trust Segmentation

Feb 6 | 08:45
TECSEC-3781
Zero Trust: From understanding the architecting a practical solution

Feb 6 | 15:20
PSOSEC-1210
A global view on Zero-Trust – mapping your business resilience requirements

Feb 7 | 08:45
BRKSEC-2445
The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 16:45
BRKSEC-2053
Zero Trust: Securing the Evolving Workplace

Feb 7 | 17:00
BRKSEC-1139
Application Security – The Final Frontier

Feb 8 | 10:45
BRKSEC-2096
Securing Industrial Networks: Where do I start?

Feb 8 | 13:30
BRKSEC-2748
Taking Authentication to the Next Level with Cisco Secure Access by Duo

Feb 8 | 17:00
BRKSEC-2123
Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

Feb 9 | 08:30
BRKSEC-2660
ISE Deployment Staging and Planning

Feb 9 | 13:45
BRKSEC-2834
Cisco's Unified Agent: Cisco Secure Client. Bringing AMP, AnyConnect, Orbital & Umbrella together

Feb 9 | 14:00
LTRSEC-2000 ISE
Deployments in the Cloud – Automate ISE Deployments in AWS and Integrate Them with Azure Active Directory

Feb 10 | 09:15
BRKSEC-2039
Secure Access with ISE in the Cloud

Feb 10 | 11:00
FINISH
BRKSEC-2773
How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload

If you are unable to attend a live session, you can watch it On Demand after the event

Feb 9 | 08:30

BRKSEC-2660

ISE Deployment Staging and Planning

Feb 9 | 13:45

BRKSEC-2834

Cisco's Unified Agent: Cisco Secure Client. Bringing AMP, AnyConnect, Orbital & Umbrella together

Feb 9 | 14:00

LTRSEC-2000 ISE

Deployments in the Cloud - Automate ISE Deployments in AWS and Integrate Them with Azure Active Directory

Feb 10 | 09:15

BRKSEC-2039

Secure Access with ISE in the Cloud

Feb 10 | 11:00

FINISH **BRKSEC-2773**

How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload

If you are unable to attend a live session, you can watch it On Demand after the event


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN