



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

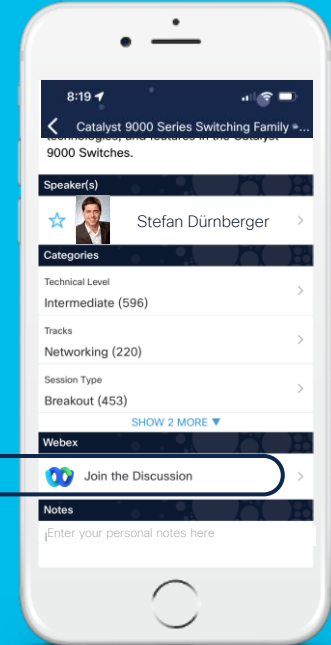
Questions?

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

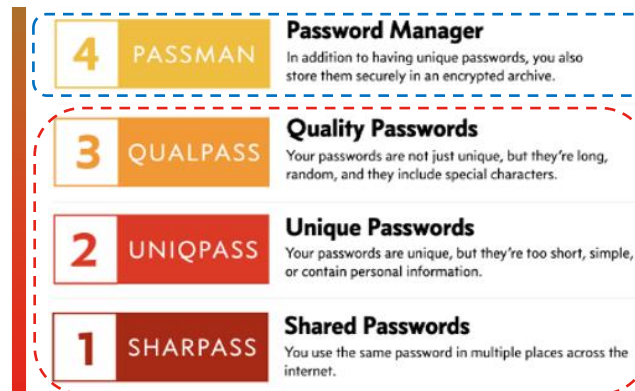
- Stefan Dürnberger –
sduernbe@cisco.com
 - 23 years in IT, 18 years in IT Security
 - 15+ years at Cisco
- A so and so football player & coach, love rock music, like to be outside, craftsman (not qualified but ambitious), being a poor programmer



Introduction

MFA Methods

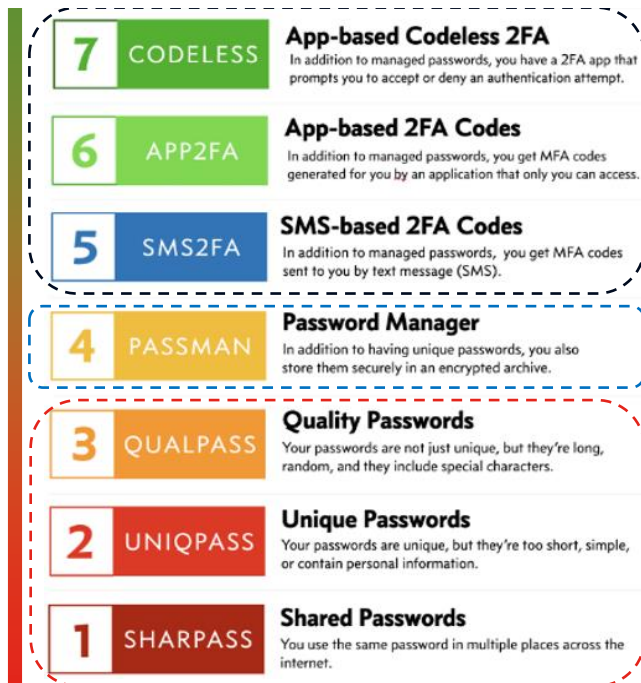
- Phishing is a low-skill, low-cost attack You just order a service
- Regardless what you do, you share a secret
- Password reset cost ~70\$



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\$

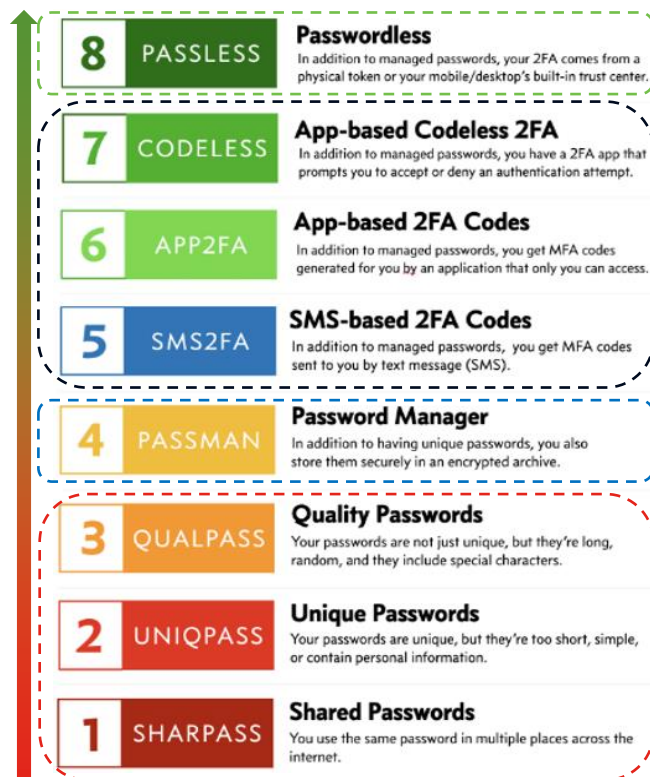


Evilproxy is a Proxy
as a Service for
phishing

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

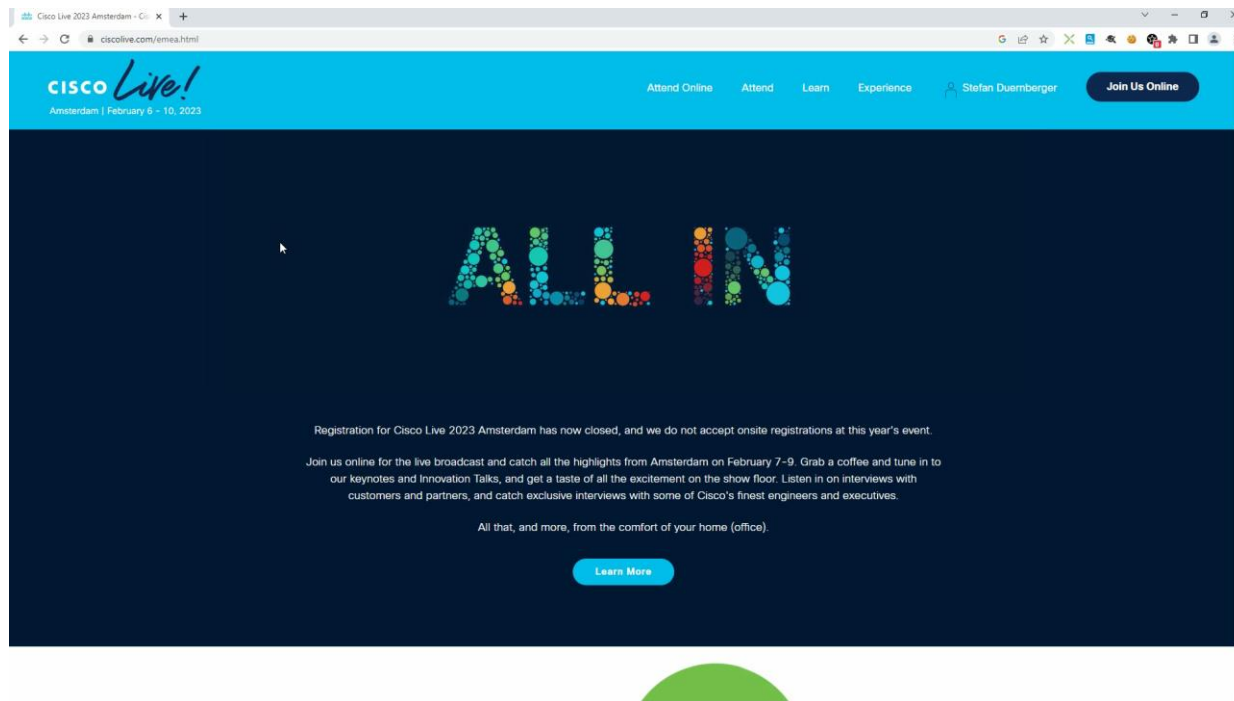
FIDO2 & Duo

Fast Identity Online (FIDO2)

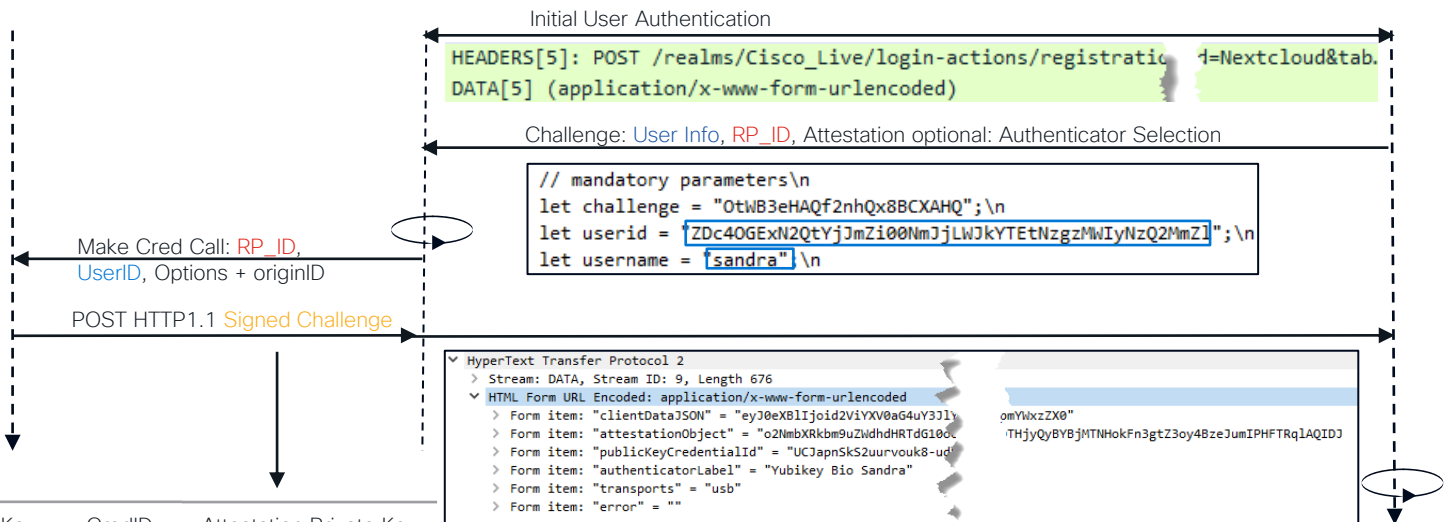
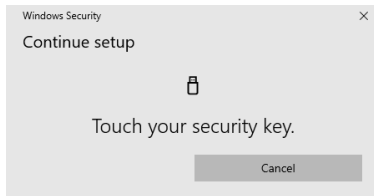
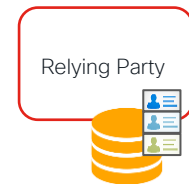
Overview

- 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





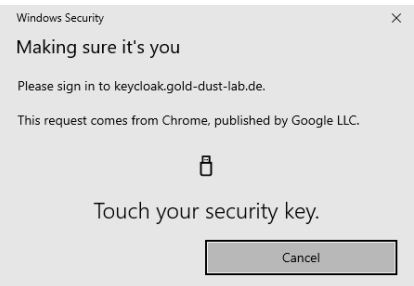
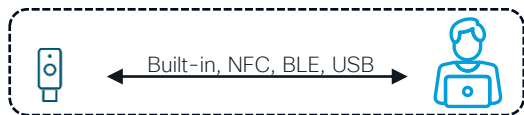
Registration Ceremony (simplified)



UserName	UserID	PublicKey	CredID
Stefan	AG87AR	12345	XYZ

Fast Identity Online (FIDO2)

Authentication Ceremony (simplified)



Initial User Authentication

```
HyperText Transfer Protocol 2
  > Stream: DATA, Stream ID: 3, Length 34
  > HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "sandra@gold-dust-lab.de"
```

Challenge: RP_ID, CredID

RP_ID, CredID, clientData

No CredID for
name&passwordless login

Signed Assertion

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "clientDataJSON" = "eyJ0eXB1Ijoid2ViYXV0aG4uZ2V0eX0iLCJ1aWxzZX0"
  > Form item: "authenticatorData" = "nBpJE1DkdL86gbzIXyFrFU00K"
  > Form item: "signature" = "MEYCIQDfF1U9s5QcXNozsh4aakvKpLnr20o."
  > Form item: "credentialId" = "UCJapnSkS2uurvouk8-udPa7Dq0y3K"
  > Form item: "userHandle" = ""
  > Form item: "error" = ""
```

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



Authentication methods

2FA authentication methods

Users will only be allowed to authenticate with 2FA using the checked methods.

- ☒ WebAuthn
- ☒ Roaming Authenticator
- ☒ Platform Authenticator

Passwordless authentication methods

Users will only be allowed to authenticate without a password when using the checked methods. Passwordless authentication is only available to SSO applications.

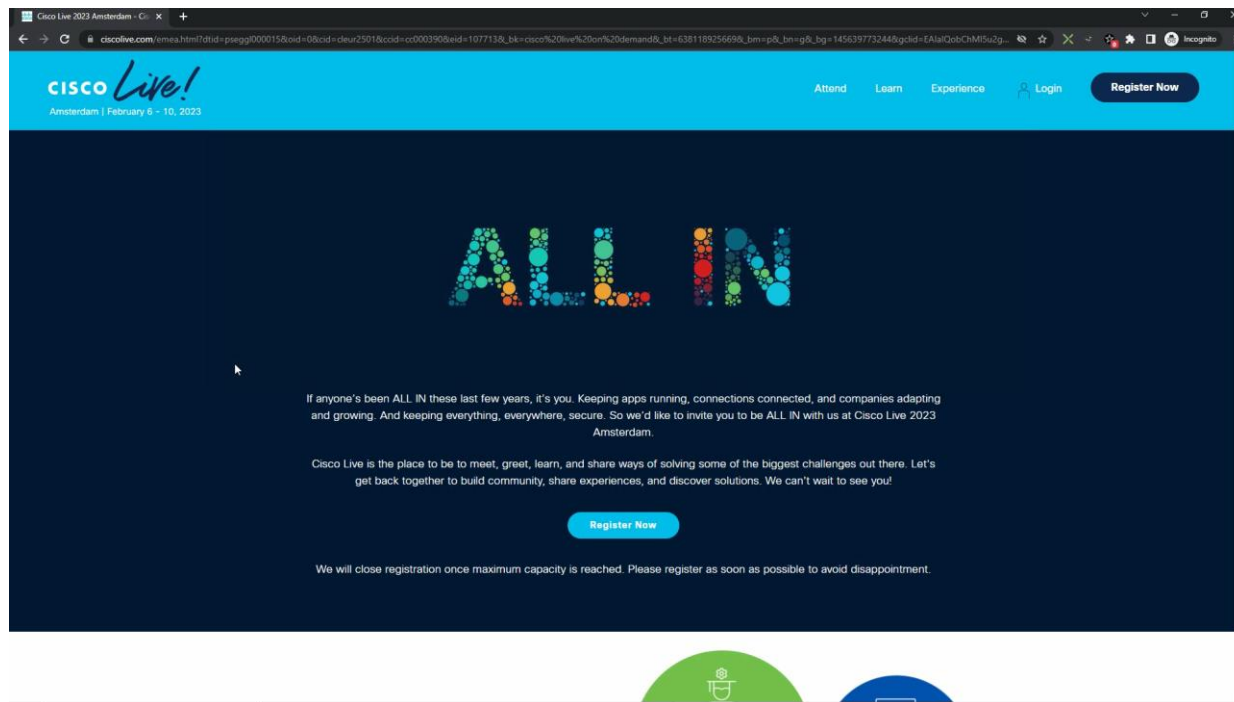
- ☒ Platform authenticators
- ☒ Roaming authenticators (e.g., security keys)

Built-in authenticators that require a biometric, PIN, or passcode (e.g., Face ID, Touch ID, Windows Hello, or Android fingerprint and face recognition)

USB, Bluetooth, or NFC security keys that require user verification via biometric or PIN

FIDO2 authentication – use cases

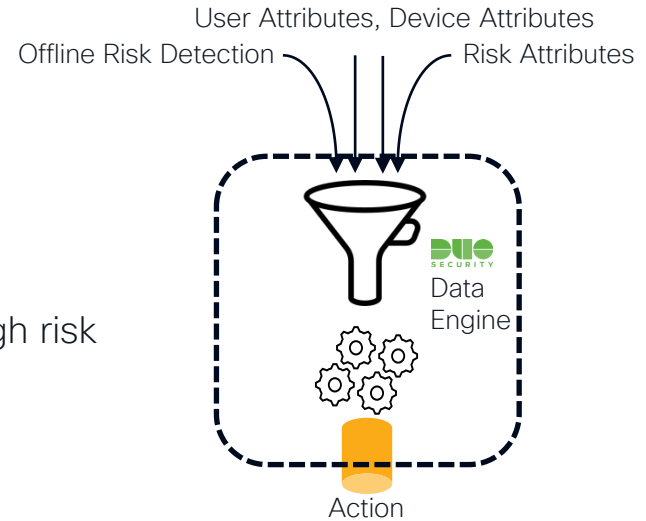




Risk-Based Authentication

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



A screenshot of the Duo Push settings interface. The 'Duo Push' checkbox is checked. Below it, the 'Always require a Verified Duo Push with' dropdown menu is open, showing options: '3 (default)' (selected), '4', '5', and '6'. The text 'This setting requires users to verify Duo Push' is visible. Other settings include 'Duo Mobile passcodes' (unchecked), 'Phone callback' (unchecked), 'SMS passcodes' (unchecked), and 'WebAuthn' (checked).

18:42:57
10. JAN. 2023

✓ **Granted**
Authentication trusted by
Risk-based remembered
devices

stefan AWS

› Windows 10, version 21H2
(19044.2364)
As reported by Device Health

› Remembered Device
(passwordless)

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

The screenshot displays a Duo Push notification interface. On the left, a red 'x' icon is next to the word 'Denied'. Below it, a message states: 'Country code mismatch detected with risk-based factor selection'. To the right of this message is the word 'Normal' in blue. The main body of the notification lists system information: 'Windows 10, version 21H2 (19044.2251)' and 'As reported by Device Health'. Below this, the 'Hostname' is 'DESKTOP-JG3D52M'. Further down, it lists 'Chrome 107.0.5304.107', 'Flash Not installed', and 'Java Not installed'. A section titled 'Device Health Application' shows it is 'Installed'. Below this, it lists 'Firewall On', 'Encryption Off', 'Password Set', and 'Security Agents Running: Cisco Secure Endpoint'. At the bottom, it says 'Trusted Endpoint determined by Device Health'. On the right side of the notification, there is a 'Duo Push' section with a blurred image of a phone screen. Below the image, the text 'Sankt Wendel, SL, Germany' and the IP address '156.67.130.47' are displayed. At the bottom left of the notification, the text 'Eindhoven, NB, Netherlands' and the IP address '155.190.34.6' are displayed. Both the IP address and location information at the bottom are enclosed in red rectangular boxes.

✗ Denied
Country code mismatch detected with risk-based factor selection

Normal

Windows 10, version 21H2 (19044.2251)
As reported by Device Health

Hostname DESKTOP-JG3D52M

Chrome 107.0.5304.107
Flash Not installed
Java Not installed

Device Health Application
Installed

Firewall On
Encryption Off
Password Set
Security Agents Running: Cisco Secure Endpoint

Trusted Endpoint
determined by Device Health

Sankt Wendel, SL, Germany
156.67.130.47

Eindhoven, NB, Netherlands
155.190.34.6

Risk-Based Authentication

Country code mismatch detection

✔ **Granted**
Push answered with
correct verification code

✗ **Denied**
Country code mismatch
detected with risk-based
factor selection

Less trusted

Windows 10, version 21H2
(19044.2251)
As reported by Device Health

Verified Duo Push
Sankt Wendel, SL, Germany
⚠ **Step-up 2FA**

Windows 10, version 21H2
(19044.2251)
As reported by Device Health

Hostname DESKTOP-
JG3D52M

Chrome 107.0.5304.107
Flash Not installed
Java Not installed

Device Health Application
Installed

Firewall On
Encryption Off
Password Set
Security Agents Running:
Cisco Secure
Endpoint

Eindhoven, NB, Netherlands
155.190.34.6

Trusted Endpoint
determined by Device Health

Normal

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).**

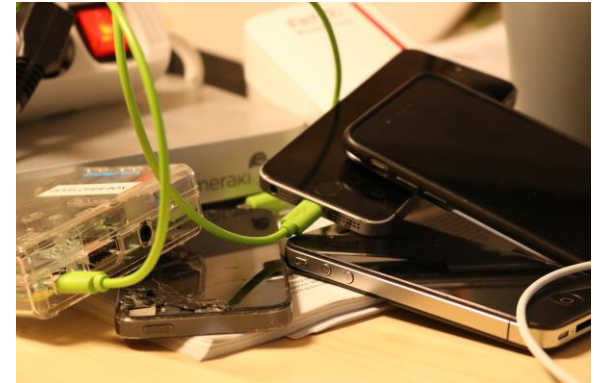
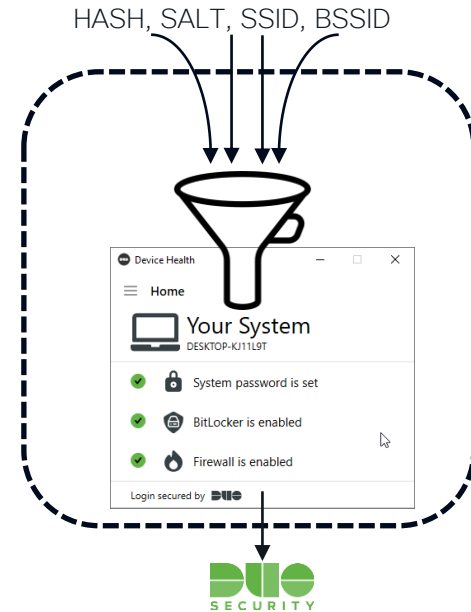
Policies
Risk-based factor selection policy was enforced.

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

The screenshot displays the 'OIDC Response' configuration page. On the left, under the 'Scopes' section, the 'openid' and 'profile' scopes are selected with checkboxes. The 'email' scope is also present but not selected. The main area shows the configuration for the 'profile' scope, which is described as 'Requests access to the user's default profile claims'. Below this, there are two columns: 'IdP Attribute' and 'Claim'. The 'IdP Attribute' column contains dropdown menus for '<First Name>', '<Last Name>', 'user_id', and '<Username>'. The 'Claim' column contains corresponding dropdown menus for 'given_name', 'family_name', 'id', and 'name'. Each pair of dropdowns is accompanied by a small blue icon. At the bottom of the 'profile' section, there is a '+ Add Claim' link. Below this, the 'email' scope is shown with a description 'Requests access to the user's default email claims' and a single dropdown pair for '<Email Address>' and 'email'.

OIDC

Roles

- Resource Owner

- That's you!



- Client/Relying Party





- Application i.e., Browser, App



- OpenID Provider/Authorization Server

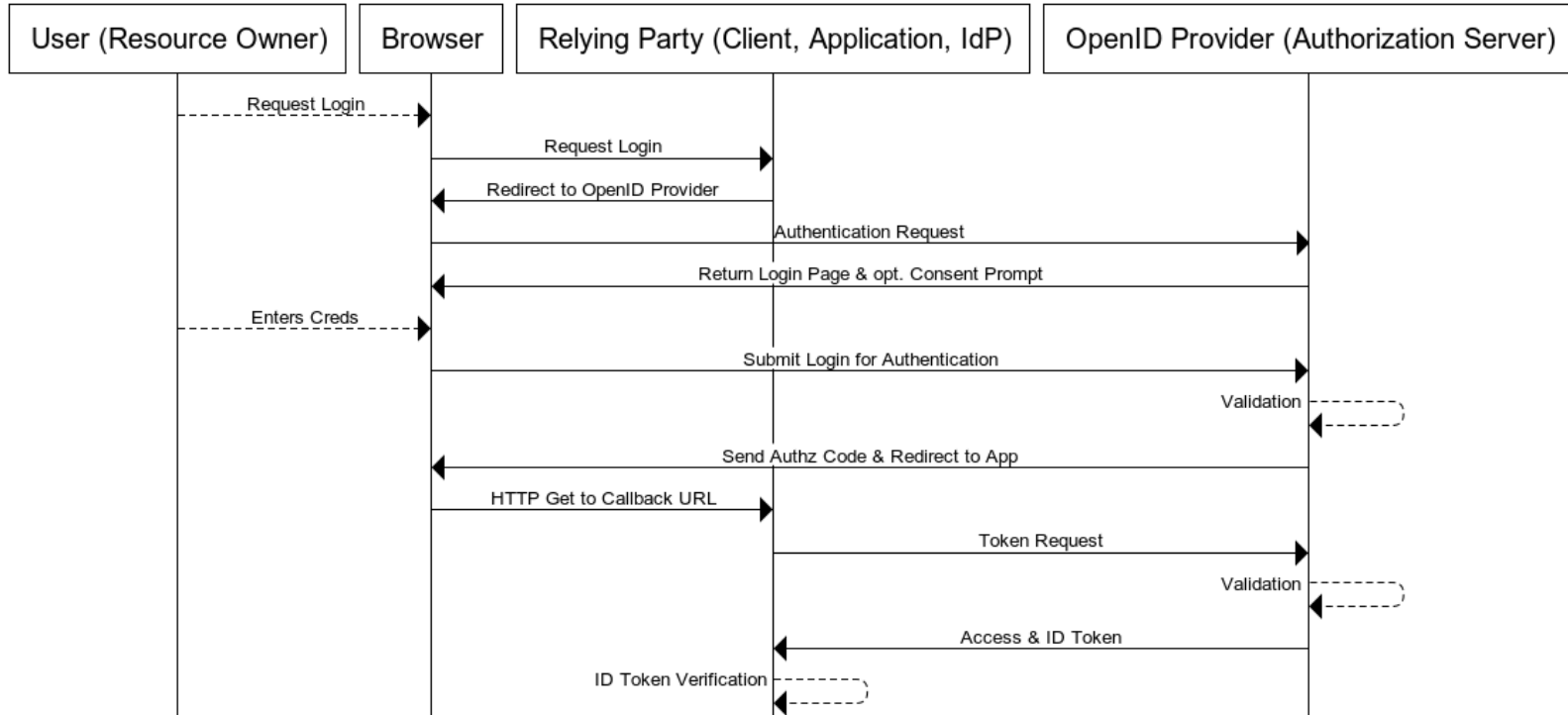
- Duo CloudSSO



	Generic OIDC Relying Party	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
	 Early Access			
	OAuth 2.0 Client Credentials	2FA with SSO hosted by Duo (Single Sign-On)	Documentation	Protect
	 Early Access			

Actors in an OIDC dance

Authorization Code Flow



CISCO *Live!*



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



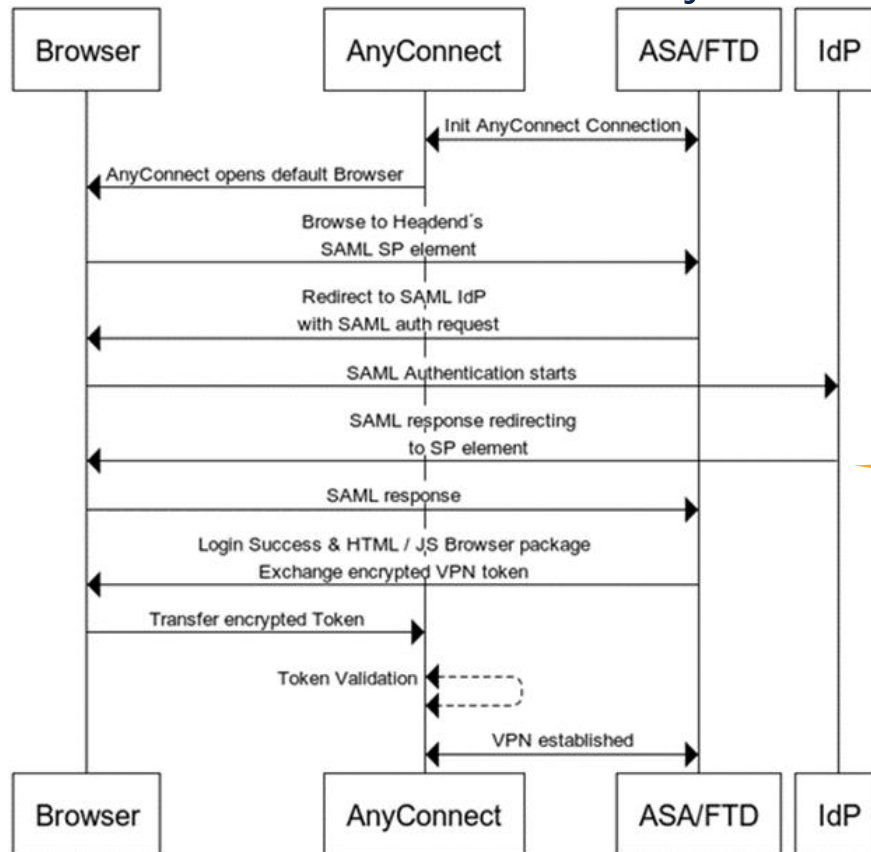
Cisco Anyconnect & User Attribute Transformation

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



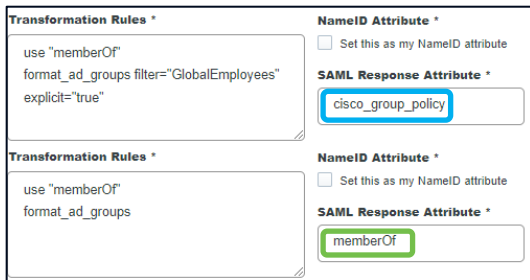
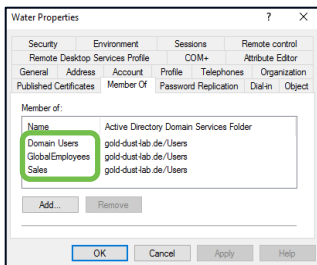
SAML Overview – Cisco Anyconnect ext. Browser



User Attribute Transformation happens at this stage!

SAML AuthZ

A practical use-case



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

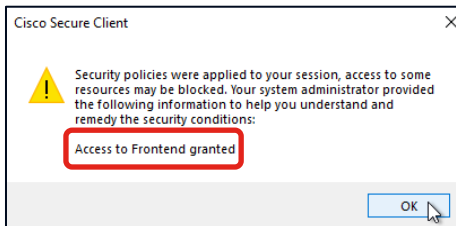
```
aaa["saml"]["memberOf"]["2"]="GlobalEmployees"
```

```
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
```

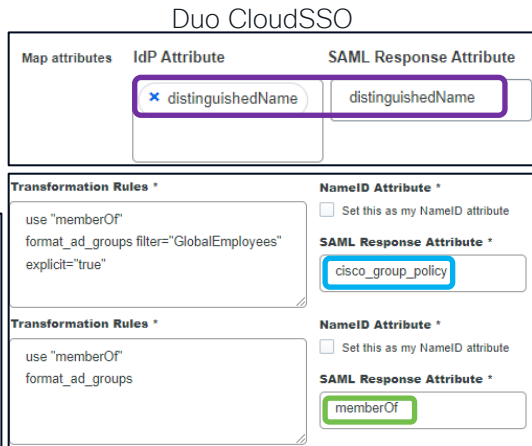
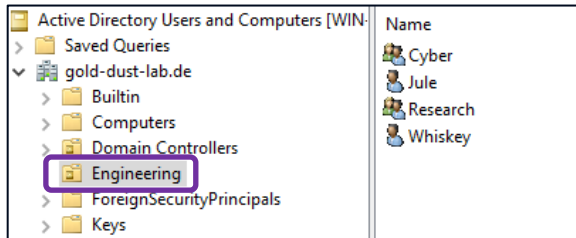


```
FP2120# show running-config dynamic-access-policy-
record Frontend-Access
dynamic-access-policy-record Frontend-Access
  user-message "Access to Frontend granted"
  network-acl FrontendACL
```

```
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>
      </dapSelection>
    </dapBasicView>
  </dapRecord>
</dapRecordList>
```

SAML AuthZ

A practical use-case



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

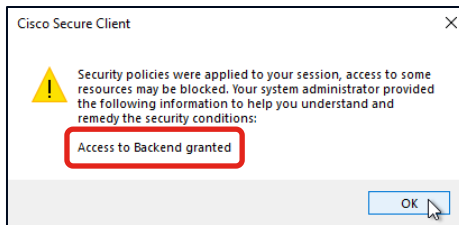
```
aaa["saml"]["memberOf"]["1"]="SystemsEngineering"
aaa["saml"]["memberOf"]["2"]="GlobalEmployees"
```

```
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

Map attributes	IdP Attribute	SAML Response Attribute
	<code>department</code>	<code>cisco_group_policy</code>

stefan Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
		Organization		

Job Title:

Department: `Duo_Prod`

Company:

Group Policies	
LDAP Attribute Mapping	
Load Balancing	
IPsec	
Crypto Maps	

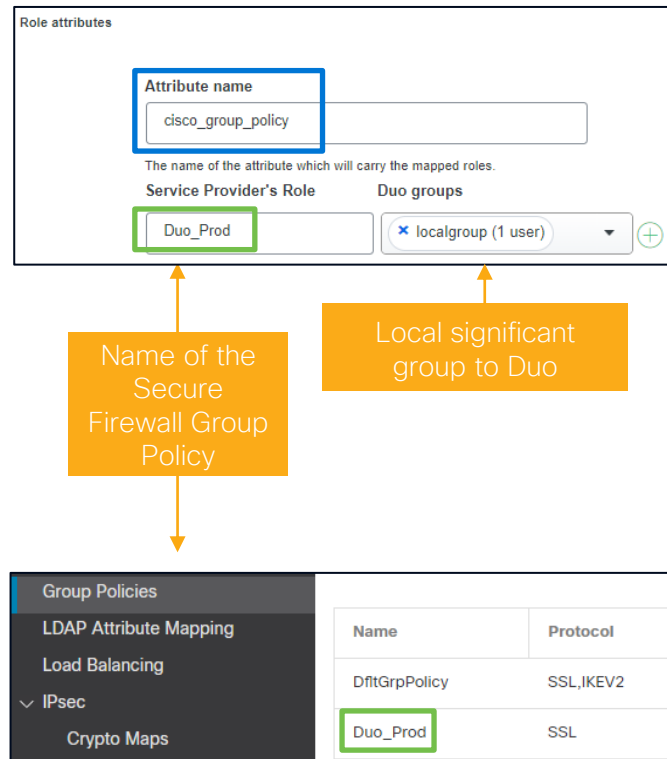
Name	Protocol
DfltGrpPolicy	SSL_IKEV2
<code>Duo_Prod</code>	SSL

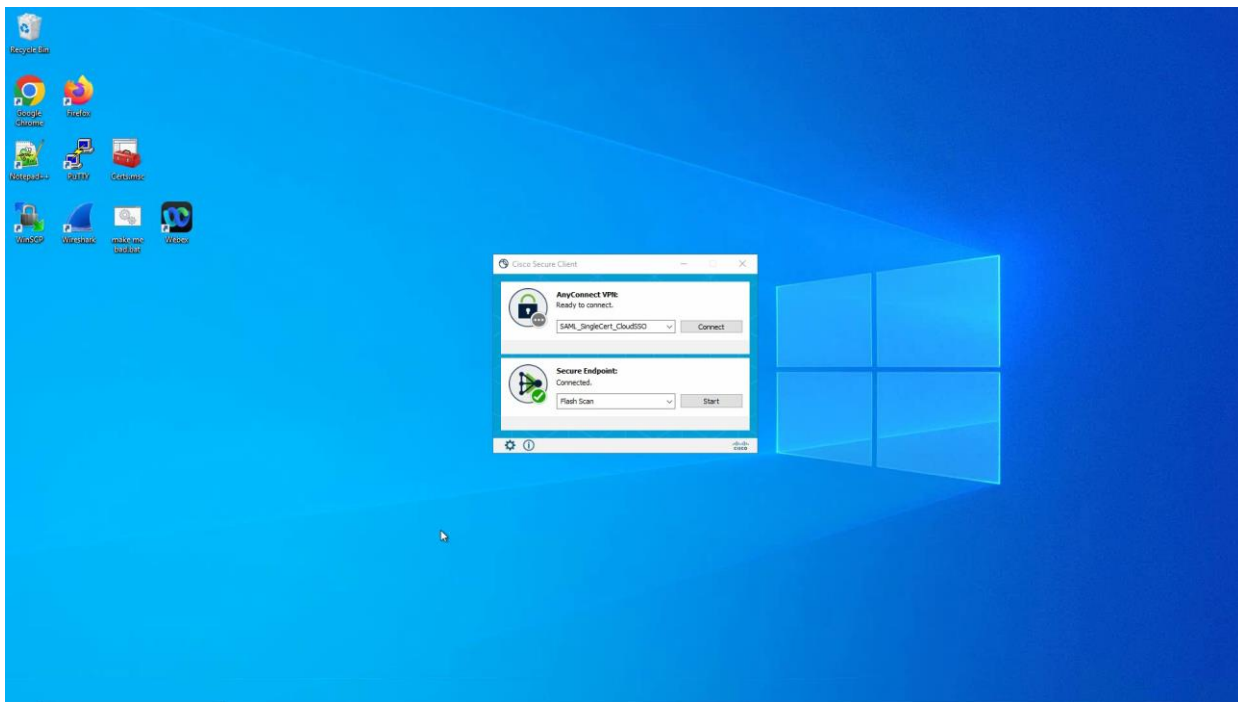
```
<saml:Attribute Name="cisco_group_policy" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic" >
<saml:AttributeValue xsi:type="xs:string">Duo_Prod</saml:AttributeValue>
```

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



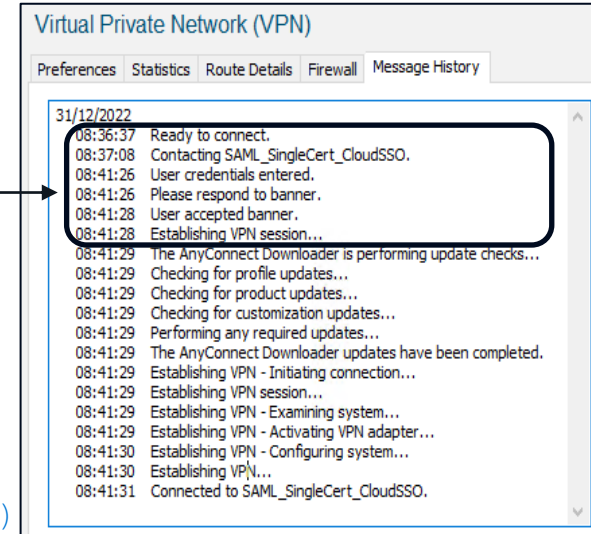
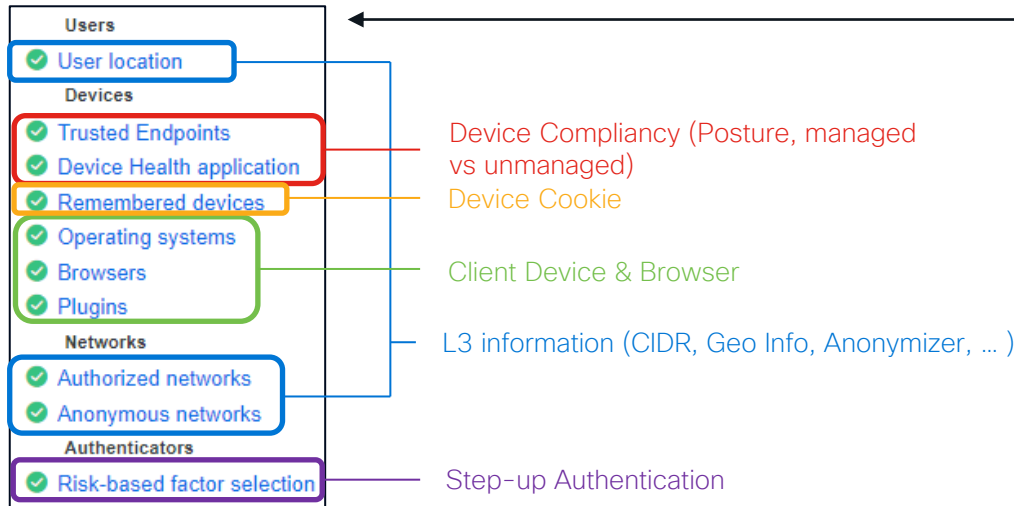



SAML Authentication

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





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-781

3781st: 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

BRKSEC-2773

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

FINISH

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 *Live!*



The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN