

TURN IT UP

CISCO *Live!*



#CiscoLive



The bridge to possible

Application and User-centric Protection with Duo Security

Stefan Dörnberger, Technical Solutions Architect, Duo Security
sduernbe@cisco.com

BRKSEC-2104

CCIE Security #16458

CISCO *Live!*

#CiscoLive



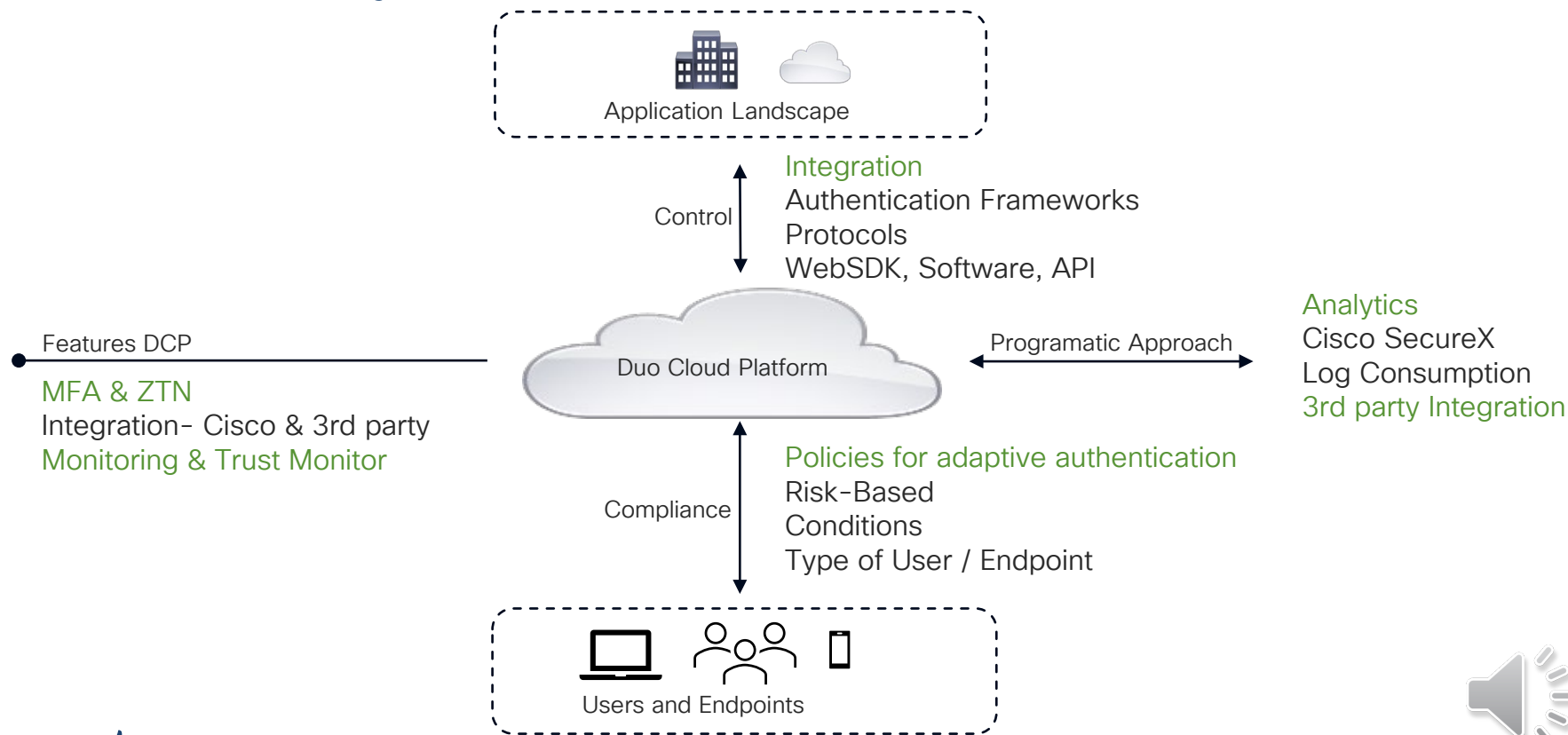
Secure Access to Applications

Hang on Alice, I am about to get the data you are looking for. I just need to

```
ip prefix-list 1 permit 10.0.0.0/8
ip as-path access-list 1 permit ^100_
ip as-path access-list 2 permit ^200_
ip community-list 1 permit 300:105
!
route-map foo permit 10
  match ip address prefix-list 1
  set local-preference 105
```



Duo Security – Conceptual Overview



Duo Security – Fundamentals

- Duo is a user-centric access security platform that provides two-factor authentication, endpoint security, remote access solutions and more to protect sensitive data
- Duo Security is NOT an Identity Management Solution
 - On-premises software services like Duo Access Gateway (DAG), Authentication Proxy but also Duo hosted SSO performs primary authentication against user directories, like on-premises Active Directory
 - Primary Credentials are processed by Duo Security, but not maintained, altered or even managed



Duo SSO & Duo Central

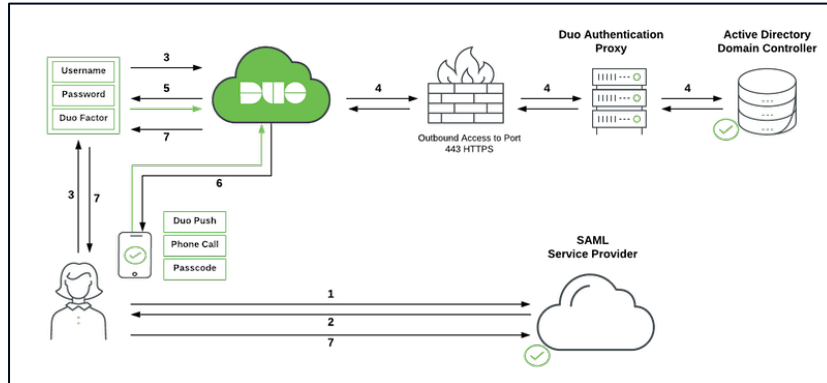
CISCO *Live!*



Duo Single Sign-On

Base Concept

- Duo Single Sign-On is a **cloud-hosted SAML identity provider (IdP)** that is managed using Duo Cloud Platform
 - High-Availability naturally built in
- Duo SSO supports 2 authentication flows
 - On-Premises Active Directory via Duo Authentication Proxy and SAML IdP

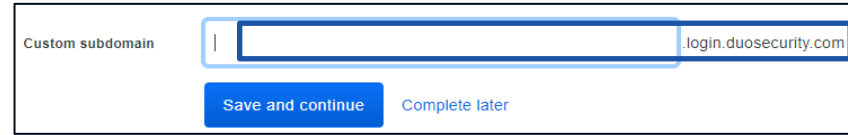


On-Premises
authentication flow

Duo Single Sign-On

Duo SSO- Subdomain and permitted E-Mail Domains

- A **Subdomain** is used to prevent users from entering their credentials on the wrong Cloud SSO login page

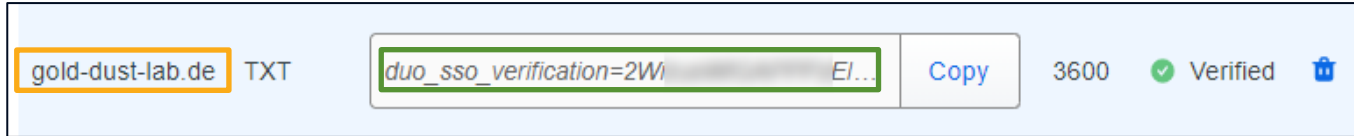


Custom subdomain

Save and continue Complete later

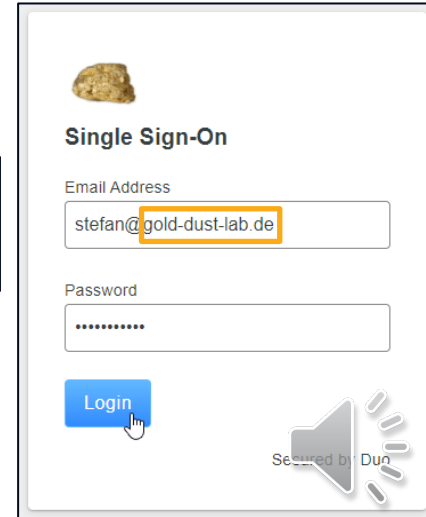


- Access to **DNS** for the user **email domains** you'll use with SSO to add **TXT records**



gold-dust-lab.de TXT

Copy 3600 Verified



Single Sign-On

Email Address

Password

Login

Secured by Duo

Duo Single Sign-On

Base Concept – Duo Central

- A **cloud-hosted portal** that your users can visit to get access to all your organization's applications and links
- Once enabled, it is a **one-stop access point** for your users. Hosted by Duo, but customizable for your company
- Flip Status, Self-Service Portal, Permitted AD Groups

Duo Central
Tiles Configuration & Policy

Duo Central name * Gold-Dust-Lab User Portal

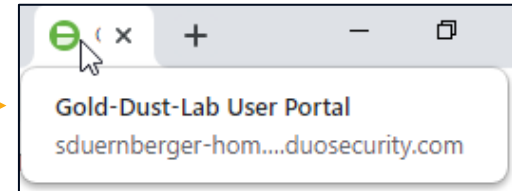
Shown on browser tab and during authentication

Self-service portal ☒ Show "My Settings and Devices" link in Duo 2FA prompt

These options let users add and remove devices and reactivate Duo Mobile.

Permitted groups ☐ Only allow authentication from users in certain groups

This name
shows up on
Browser tab



Video

Duo Central

The screenshot shows a web browser window with the Cisco website. The browser's address bar displays "https://www.cisco.com". The website's navigation bar includes the Cisco logo, "Products", "Support & Learn", "Partners", and "Events & Videos". On the right side of the navigation bar are icons for search, user profile, and language (US/EN). The main content area features a dark blue background with a large, colorful graphic that says "TURN IT UP" in white, with "cisco Live!" in a smaller font to the right. Below this graphic, the text "Americas: March 30-31", "APJC: March 31 - April 1", and "EMEAR: March 31 - April 1" is displayed. Further down, it says "Cisco Live is going global" and "Join us for a two-day digital event. Grab your front-row seat to watch innovation talks, celebrity". A "Watch replay" button is visible in the top right corner of the main content area. A cookie consent banner is at the bottom of the page, stating "Cookies allow us to optimise your use of our website. We also use third-party cookies for advertising and analytics. Please read our [Privacy Statement](#) and [Cookie Notice](#) for more information." with buttons for "No, manage cookie settings" and "Accept".

cisco *Live!*



LDAP Signing and Channel Binding



LDAP Signing and Channel Binding

Base Concept

- LDAP channel binding and signing increase the security for communications between LDAP clients and AD domain controllers
 - LDAP Channel Binding. Binds the LDAP session to the TLS connection
 - LDAP Signing. Requires a secure connection
- A Microsoft Update can potentially change behavior for channel binding and LDAP signing with the aim to prevent an attacker from performing a man-in-the-middle attack on an LDAP server



LDAP Signing and Channel Binding

How it affects Duo?

- This **configuration** will **fail** in Version 4.X after Binding/Signing on AD is enabled

```
[ad_client]
host=10.1.200.102
service_account_username=Username
service_account_password=Password
search_dn=DC=gold-dust-lab,DC=de
auth_type=ntlm2 ]
transport=clear ]
```

Default settings

```
2020-11-02T20:38:14+0100 [_ADAuthClientProtocol,client] C<-S LDAPMessage(id=2,
value=LDAPBindResponse(resultCode=8, errorMessage='00002028: LdapErr: DSID-
0C09027F, comment: The server requires binds to turn on integrity checking if
SSL\TLS are not already active on the connection, data 0, v3839\x00',
serverSaslCreds=LDAPBindResponse_serverSaslCreds(value='')), controls=None)
...
Returning response code 3: AccessReject
```



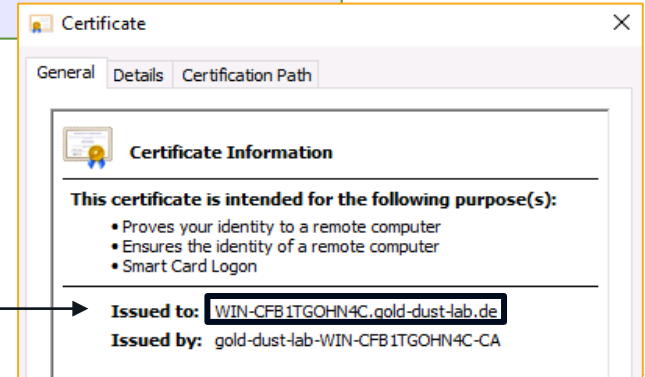
LDAP Signing and Channel Binding

Solution

- Either use **SASL Sign and Seal** supported by **Auth-Proxy 5.0** and greater or **STARTTLS/LDAPS**

```
LDAP 135 bindRequest(151) "<ROOT>" , NTLMSSP_NEGOTIATEsasl
LDAP 395 bindResponse(151) saslBindInProgress , NTLMSSP_CHALLENGE
TCP 66 43612 → 389 [ACK] Seq=70 Ack=330 Win=64128 Len=0 TSval=1540898943 TSecr=142198708
LDAP 551 bindRequest(152) "<ROOT>" , NTLMSSP_AUTH, User: GOLD-DUST-LAB\Administratorsasl
LDAP 91 bindResponse(152) success
```

```
[ad_client]
host=WIN-CFB1TGOHN4C.gold-dust-lab.de
service_account_username=Username
service_account_password=Password
search_dn=DC=gold-dust-lab,DC=de
ssl_ca_certs_file=conf/CA.pem
transport=ldaps
ssl_verify_hostname=true
```



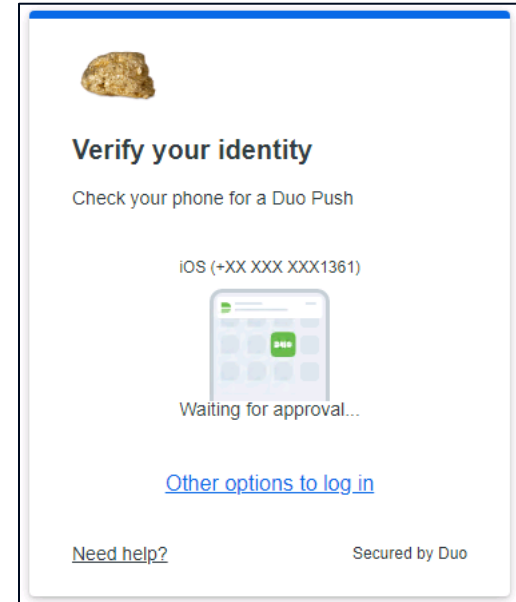
Duo Universal Prompt



Duo Universal Prompt

Base Concept

- Current Duo Prompt is delivered via an iFrame using WebSDKv2
- New Frameless approach, derived from **OIDC standards**
 - Protected application will redirect to a page hosted by Duo to show the Prompt, and then redirect back to the protected application after the user completes 2FA

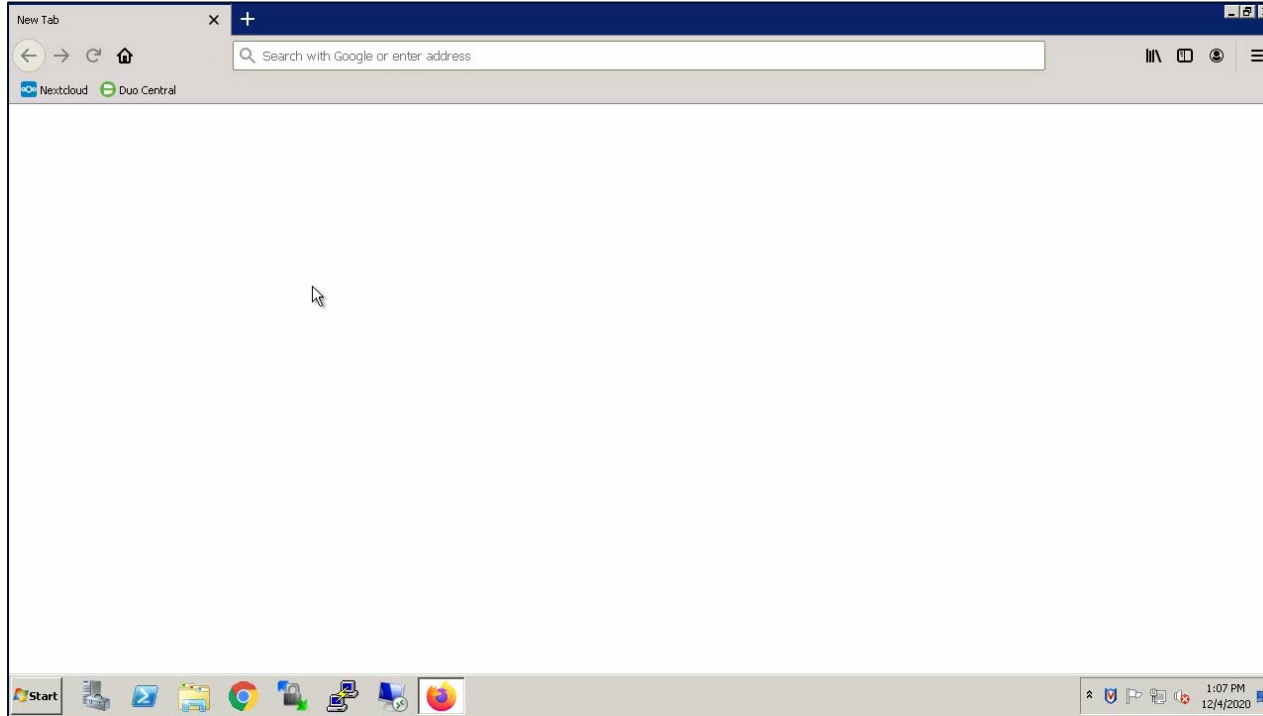


Destination URL	Protocol	Type	Method	
https://nextcloud.gold-dust-lab.de/index.php/apps/...	SAML	Response	POST	X
https://api-c[redacted]f.duosecurity.com/oauth/v1/aut...	OAuth 2.0	Request	GET	X
https://sso-c[redacted]f.sso.duosecurity.com/saml2/sp...	SAML	Request	GET	X



Video

Universal Prompt



Device Health Application

CISCO *Live!*



Duo Device Health Application (DHA)

Base Concept

- Prevents access if the device fails the health checks
 - Gives organizations **control** over which devices can access applications
 - Helps achieve and demonstrate **compliance** to regulations

	Access	Beyond
OS Patch level	X	X
Disk Encryption status	X	X
OS-based Firewall status	X	X
Password status	X	X
Agents	N/A	Cisco AMP4E, 3rd party

☐ Don't require users to have the app

☒ **Require users to have the app** ⓘ

☒ Block access if firewall is off.

☒ Block access if disk encryption is off.

☒ Block access if system password is not set.

☒ Block access if an endpoint security agent is not running.

When the user is blocked, the app will provide remediation. [See what it looks like](#) ⓘ

Select which Duo supported endpoint security agent(s) are allowed

BitDefender Endpoint Security Duo Beta

Cisco AMP for Endpoints

CrowdStrike Falcon Sensor

McAfee Endpoint Security Duo Beta

SentinelOne Duo Beta

Sophos AV Duo Beta

Symantec Endpoint Protection

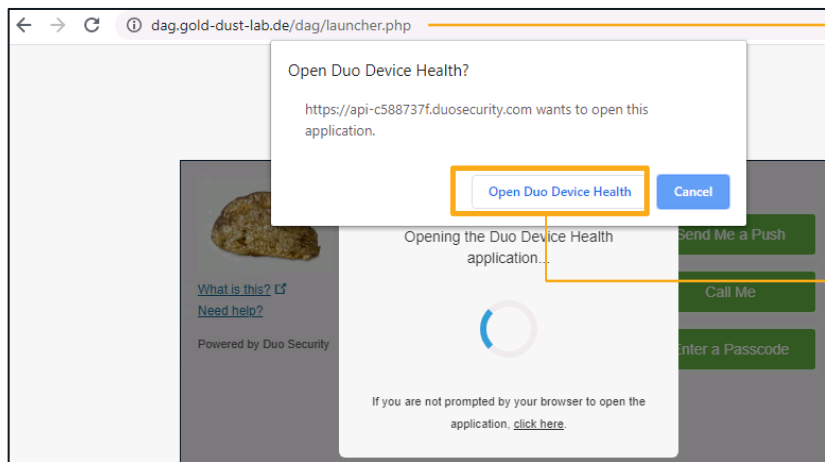
Trend Micro Apex One Duo Beta

VMware Carbon Black Cloud Duo Beta

Windows Defender

Duo Device Health Application (DHA)

Application Operation



netstat - an 1 | find "53100"

Command Prompt			
TCP	127.0.0.1:51961	127.0.0.1:53100	SYN_SENT
TCP	127.0.0.1:51962	127.0.0.1:53101	SYN_SENT
TCP	127.0.0.1:51963	127.0.0.1:53102	SYN_SENT
TCP	127.0.0.1:51964	127.0.0.1:53103	SYN_SENT
TCP	127.0.0.1:51965	127.0.0.1:53104	SYN_SENT
TCP	127.0.0.1:51966	127.0.0.1:53105	SYN_SENT

Command Prompt			
TCP	127.0.0.1:53100	0.0.0.0:0	LISTENING
TCP	127.0.0.1:53100	127.0.0.1:51973	ESTABLISHED
TCP	127.0.0.1:53100	127.0.0.1:51979	ESTABLISHED
TCP	127.0.0.1:53106	0.0.0.0:0	LISTENING

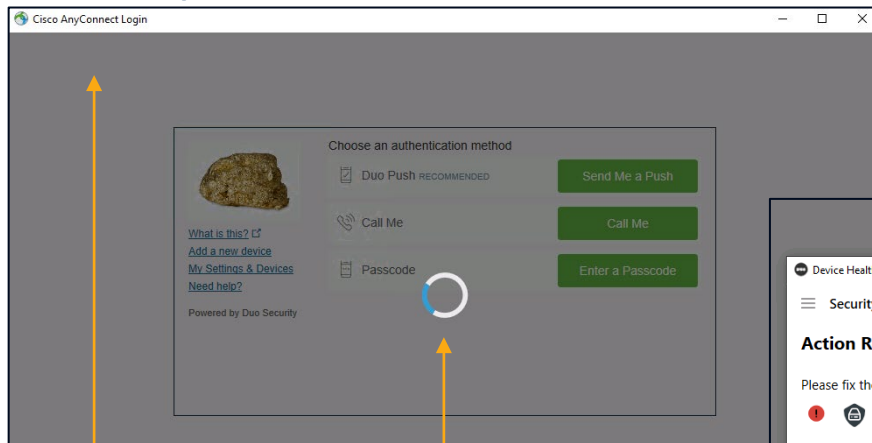
| INFO | DuoDeviceHealth.App | Starting application with version 2.8.0

| INFO | DuoDeviceHealthLibrary.Communication.HttpServer | Opening HttpServer on port 53100

```
92 Standard query 0x211d A 4.endpointhealth.duosecurity.com
140 Standard query response 0x211d A 4.endpointhealth.duosecurity.com A 35.158.52.236 A 3.123.83.70 A 18.194.121.141
66 63834 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

Duo Device Health Application (DHA)

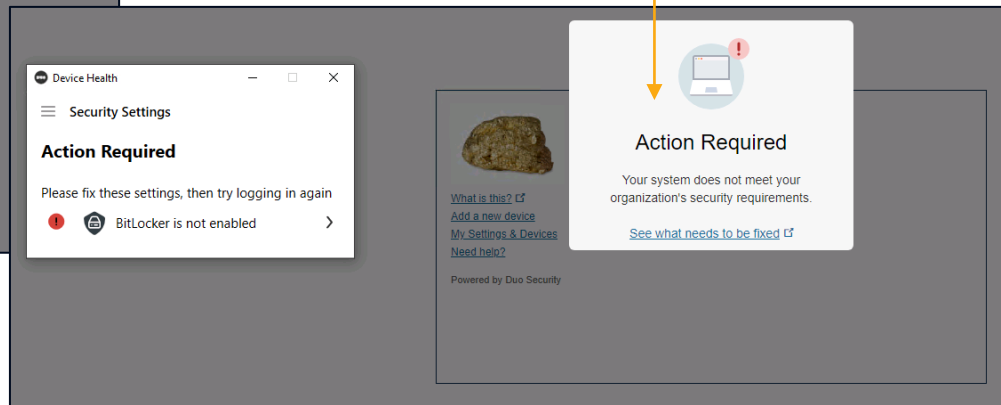
User Experience



Integration into
AnyConnect

Spinning wheel for a very
short period of time. It's very
fast!!!

Uncompliant state
requires user's
attention and action




Duo & Umbrella



Duo & Umbrella

Umbrella Webpolicy – SAML Authentication and Policy Evaluation

- Policy is evaluated top down for matching identity
- Identity is matched and SAML authentication starts
- Policy is re-evaluated but includes SAML User and Groups identity received from SAML response

 **Enable SAML** ⓘ
Enables SAML authentication on the networks and tunnels configured in this policy.

1	Authenticated User Policy	Protection Web Policy	Applied To 3 Identities	Contains 4 Policy Settings	Last Modified Dec 8, 2020	▼
2	Gold-Dust-Lab Web Policy	Protection Web Policy	Applied To 1 Identity	Contains 4 Policy Settings	Last Modified Dec 9, 2020	▼
3	Default Web Policy	Protection Web Policy	Applied To All Identities	Contains 4 Policy Settings	Last Modified Dec 8, 2020	▼

SAML is enabled for this Policy



Duo & Umbrella

Use Case: Tenant Control

- Control identity access to SaaS applications
 - Microsoft Office 365, Google GSuite, Slack Enterprise

Gold-Dust-Lab Tenant Control	Office 365 Tenants 1	G Suite Domains 0	Slack Workspaces 0	Date Modified Dec 08, 2020
------------------------------	-------------------------	----------------------	-----------------------	-------------------------------

- Tenant Control is part of a Web policy

Provide a list of domains. In most cases, these are your enterprise domains.

Tenant Domain

ADD

1 Domain

X

To track Office 365 access in Azure Reports, provide a Tenant Directory ID. Find your tenant ID in the Azure portal.

Tenant Directory ID

Vendor specific
block page



stedue@gold-dust-lab.de

You can't get there from here

It looks like you're trying to access a resource that belongs to an organization that's not approved by your IT department.

Duo Trust Monitor

CISCO *Live!*



Duo Security Trust Monitor

Basics

- Duo Trust Monitor is a threat detection feature that analyzes real-time authentication data to create a **baseline** of normal user behavior
 - Available for all Beyond and Access customers
- Building the Baseline- Patterns
 - Who typically accesses, which applications, from which devices, at what times, from what locations, using which authentication methods

The screenshot displays the Duo Security Trust Monitor interface. At the top, it says "Authentication" with a yellow shield icon. Below this, the timestamp "12:17 PM UTC | Dec 7, 2020" is shown. On the right, there are two buttons: "Mark as Suspicious" (blue) and "Dismiss Event" (blue). Below the timestamp, there are four filter tabs: "New Location", "New Access Device IP", "New Application Access", and "Unrealistic Geovelocity". The "Unrealistic Geovelocity" tab is selected. Below the tabs, there is a table with the following columns: User, Result, Access IP, Access Location, and Application. The table contains one row of data: User (redacted), Result (Denied: Location restricted), Access IP (redacted), Access Location (China), and Application (SAML - Salesforce). To the right of the table, there is a yellow callout box with the text "What key category is it?" and an arrow pointing to the "Unrealistic Geovelocity" tab. Below the callout box, there is a link "More Details >".

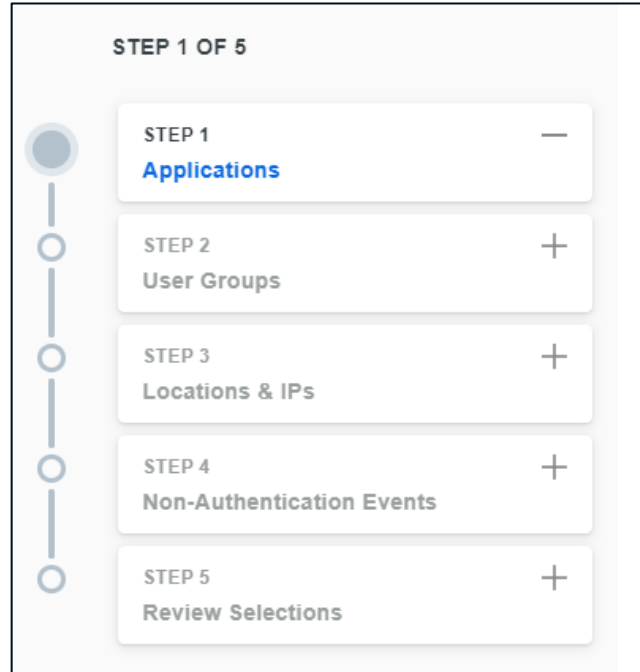
User	Result	Access IP	Access Location	Application
[Redacted]	Denied: Location restricted	[Redacted]	China	SAML - Salesforce



Duo Security Trust Monitor

Configuration

- Create Risk Profile
 - Applications
 - Users and User Groups
 - Location and IP's
 - Non-Authentication Events



Duo Security Trust Monitor

New Location

has not logged in from this location recently.

Most frequent locations

US	101 (99%)	<div></div>
----	-----------	-------------

This event's location

HR	1 (<1%)	<div></div>
----	---------	-------------

Unrealistic Geovelocity

The velocity between the two authentications is not plausible.

~5353 miles in ~49 minutes

Previous Authentication → This Authentication

United States	Zagreb, 21, Croatia (Hrvatska)
	New Country

IP Range and Carrier

74.38.160.0/19, frontier communications of america inc.	44.170.220.0/23, sedmi odjel d.o.o.
---	-------------------------------------

User Marked Fraud

rejected the Duo Push request and flagged the event as a fraud attempt

The user has flagged 0 other fraud events in the past 30 days

New Access Device IP

has not logged in from this IP recently.

Most frequently used IP ranges

198.176.199.0/24	2 (15.4%)	<div></div>
66.245.0.0/18	2 (15.4%)	<div></div>

This event's IP range

44.170.220.0/23	1 (7.7%)	<div></div>
-----------------	----------	-------------

User Marked Fraud

User	Result	Access IP	Access Location	Application
stefan	Fraud: User marked fraud	192.168.30.15	Unknown	Gold-Dust-Lab Cisco RADIUS VPN

Threat context, historical information

[More Details](#) >

Duo Trusted Endpoint

CISCO *Live!*




Duo Trusted Endpoint

Basics – Windows, MacOS, and iOS

- Duo's Trusted Endpoints feature lets you define and manage trusted endpoints and grant secure access to your organization's applications with device certificate verification policies
- Need to distribute Duo certificate or configuration to your managed devices
- A variety of options exists, like Active Directory, **Meraki Systems Manager**, Mobile Iron Cloud, Microsoft Intune, Jamf Pro, ...
- Helps to **distinguish between unmanaged and managed endpoints** that access your browser-based applications

< Device Management Profile



Root MDM Profile
Cisco Systems, Inc.

Signed by *.mobileiron.com
Verified ✓


Description The top-level MDM payload containing the MDM profile, the identities and the trust certificates necessary to MDM-manage this device.

Contains Mobile Device Management
Password Policy
Web Clip
Device Identity Certificate
2 Certificates

Remove Management

< Profile Root MDM Profile

CERTIFICATES (2)



Duo Device Authentication
Issued by: Duo Endpoint Validation Issuing CA 1
Expires: 8. December 2021

Trusted Endpoints


☐ Allow all endpoints
Endpoints will be checked for trustworthiness to aid reporting, but un-trusted endpoints will be allowed.

☒ **Require endpoints to be trusted**
Only Trusted Endpoints will be able to access browser-based applications.

☐ Allow AMP for Endpoints to block compromised endpoints

Save Policy


Duo Trusted Endpoint

**OS**
Windows 10 latest

Trusted Endpoint
Yes
Valid certificate collected

Certificate
Source: Active Directory Domain Services 5
Serial: 1200132d93b4dbe4541a0e9eac000000132d93
Device User: stefan@gold-dust-lab.de
Device Id: DESKTOP-JG3D52M.gold-dust-lab.de
Expiration: Sep 9, 2021 4:15 PM CEST

Issued via
ADDS

**Certificate Information**

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- 1.3.6.1.4.1.48626.1.1.1

Issued to: Duo Device Authentication

Issued by: Duo Endpoint Validation Issuing CA 1

Issued by Duo
Issuing CA

Do you want to export the private key with the certificate?

☐ Yes, export the private key

☒ No, do not export the private key

Note: The associated private key is marked as not exportable. Only the certificate can be exported.

Keys are non
exportable

1.3.6.1.4.1.48626.100.1 0c 14 44 41 35 53 5a 4c 4d 43...

0c 14 44 41 35 53 5a 4c 4d 43 56 4e 4c 41 4a 33 54 36 5a 4e 51 43

..DA5SZL
MCVNLAJ3
T6ZNQC

1.3.6.1.4.1.48626.100.2 0c 14 44 4d 32 35 45 31 47 4a...

0c 14 44 4d 32 35 45 31 47 4a 56 38 37 50 46 55 4e 4d 38 37 30 53

..DM25E1
GJV87PFU
NM870S

1.3.6.1.4.1.48626.100.3 0c 20 44 45 53 4b 54 4f 50 2d ...

0c 20 44 45 53 4b 54 4f 50 2d 4a 47 33 44 35 32 4d 2e 67 6f 6c 64 2d 64 75 73 74 2d 6c 61 62 2e 64 65

..DESKTO
P-JG3D52
M.gold-d
ust-lab.
de

1.3.6.1.4.1.48626.100.4 0c 17 73 74 65 66 61 6e 40 67...

0c 17 73 74 65 66 61 6e 40 67 6f 6c 64 2d 64 75 73 74 2d 6c 61 62 2e 64 65

..stefan
@gold-du
st-lab.d
e

Cert is linked to
Tenant ID,
Management
Integration,
User and
Device



[What is this?](#)

[Add a new device](#)

[My Settings & Devices](#)

[Need help?](#)



We're sorry. Access is not allowed.

- If you are using a personal or public device, try again with a company-approved device.
- If you are using the device you normally log in with, further help may be required.

To fix this problem, please reach out to your administrator or IT Helpdesk

fritz

Gold-Dust-Lab User Portal

▼ Windows 10

Chrome 87.0.4280.66

Flash Not installed

Java Not installed

Mismatched Customer Certificate

Endpoint is not trusted because the certificate belongs to different customer account.



Duo Network Gateway (DNG)

CISCO *Live!*



Duo Network Gateway

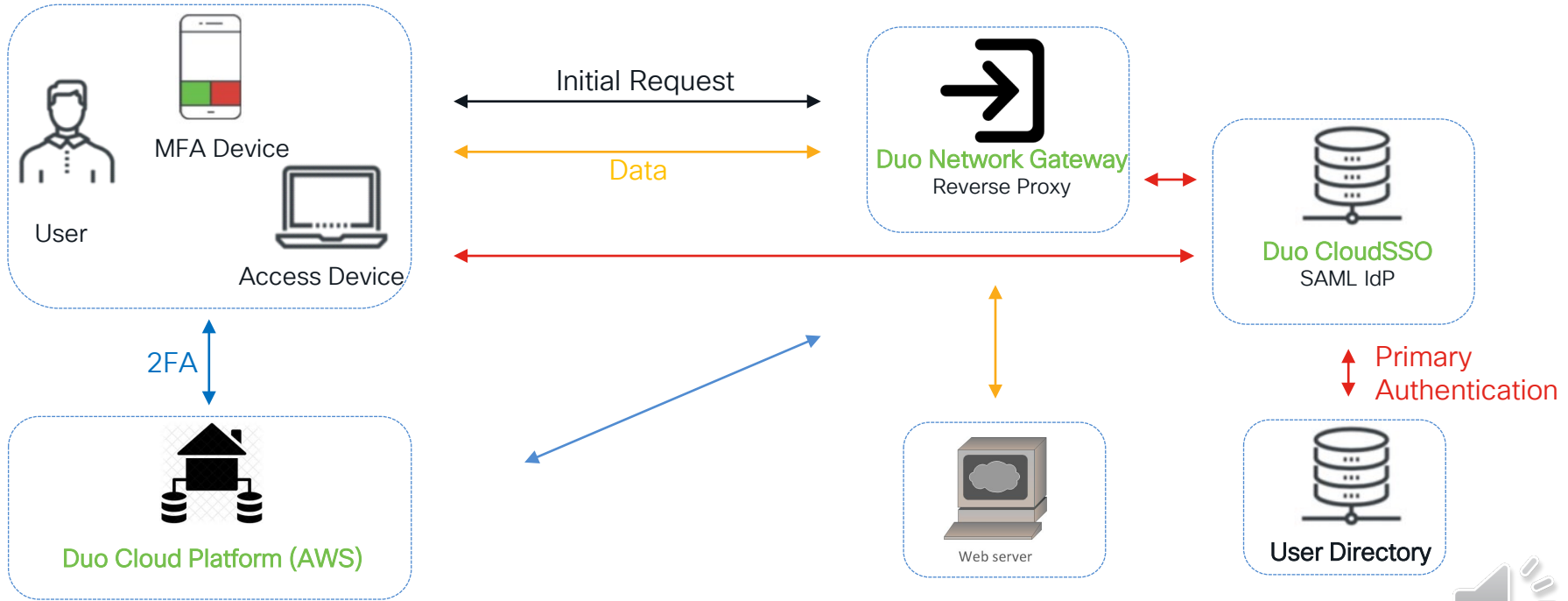
Basics

- Duo Network Gateway allows your users to access your on-premises websites, web applications, and SSH servers without requiring a VPN connection
- Acts as a reverse proxy and provides access to resources without granting network level access
 - It requires a SAML 2.0 IdP
- Deployment options
 - AWS
 - Customer hosted Docker container deployment



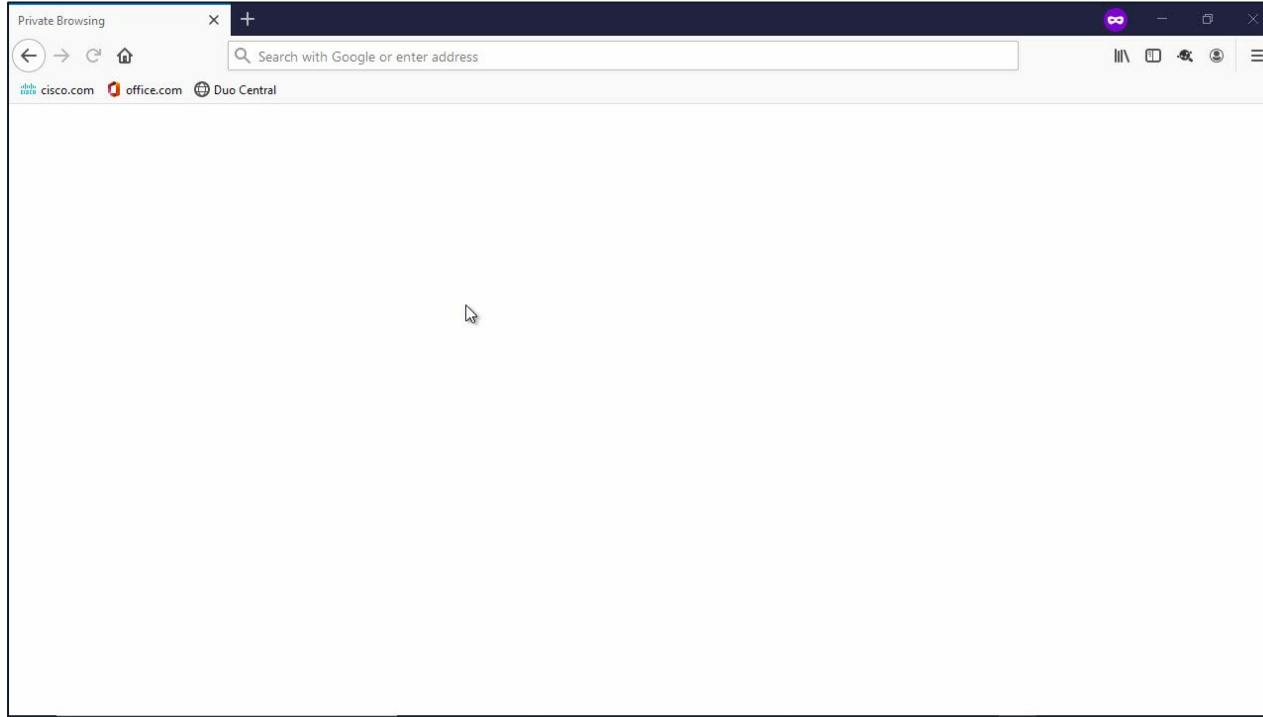
Duo Network Gateway

Solution Overview



Video

DNG Protected Applications – Duo Central



Summary

- Duo Security helps customers building a true **Zero Trust Networking** solution by providing them with the **right tools**
- **Duo Security** secures application access
 - Device and User Compliance
 - Reduces Risk
- **Take Action**
 - Use Webex teams to collaborate
 - Setup a trial <https://signup.duo.com/>
 - Check related session BRKSEC-2103 & BRKSEC-2105





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive



TURN IT UP

CISCO *Live!*



#CiscoLive