CISCO
SECURE

Yubikey and Duo

Leo Lahteenmaki

Engineer

7.11.2024

CISCO The bridge to possible

Introducing Continuous Identity Security

Verified Users

+

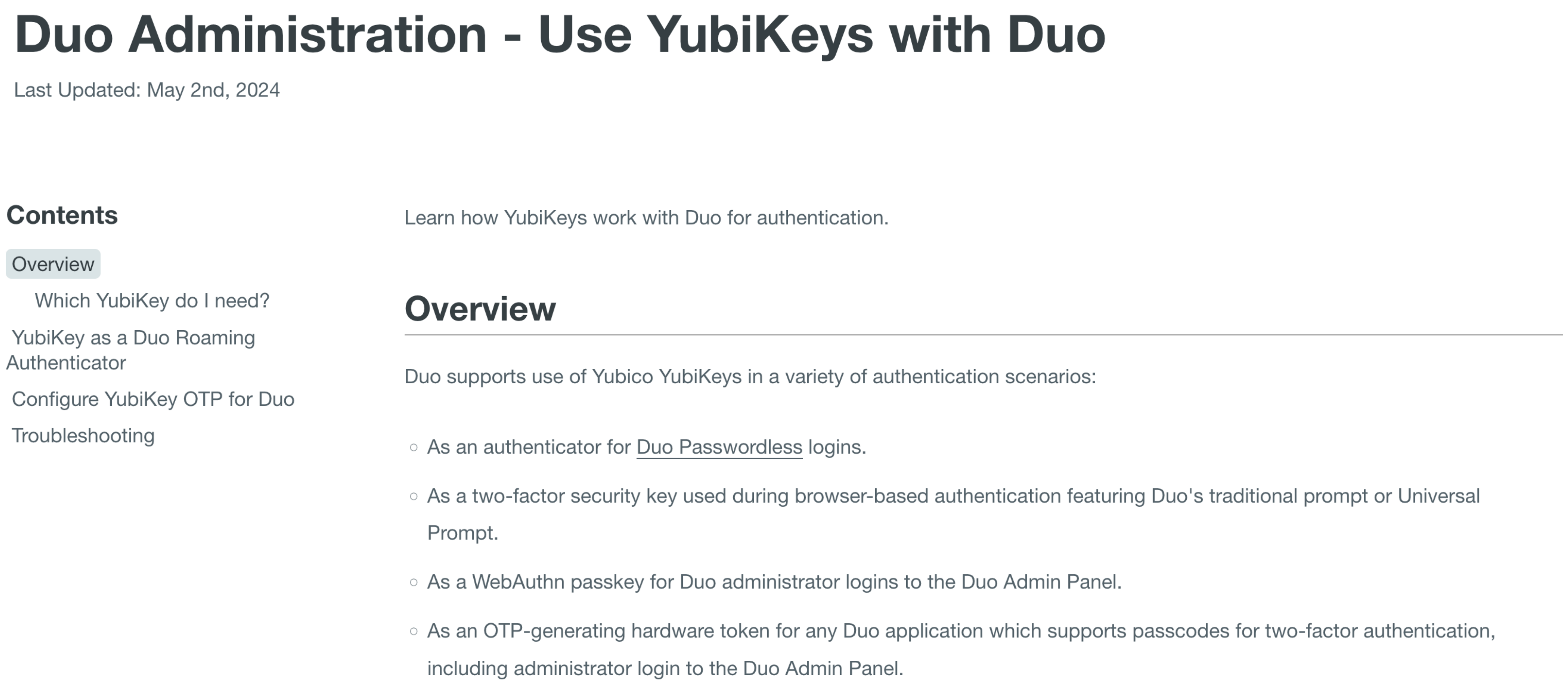
Trusted Devices

+

Identity Context

Continuous Risk Assessment and Experience Management

Pre login | At Login | Post Login



Duo Administration - Use YubiKeys with Duo

Last Updated: May 2nd, 2024

Contents

Learn how YubiKeys work with Duo for authentication.

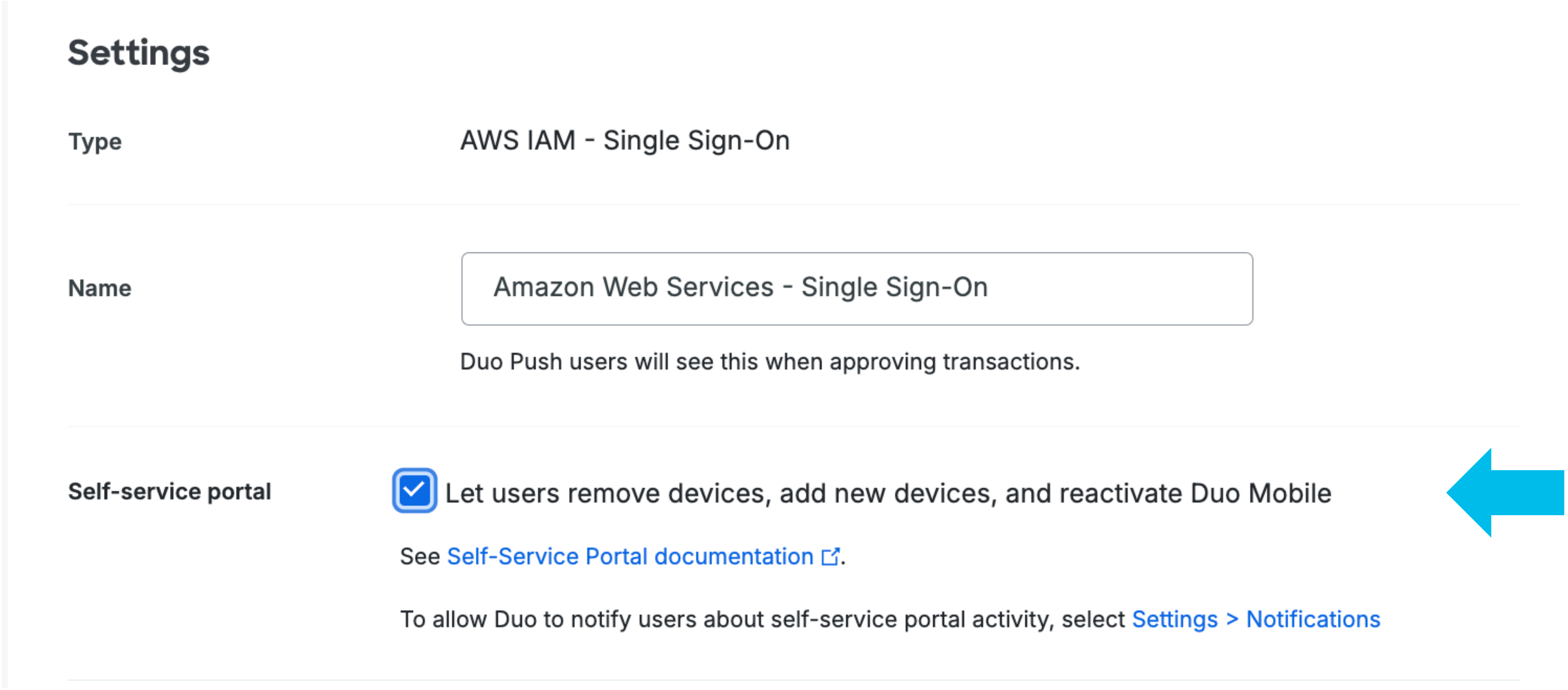
Overview

Duo supports use of Yubico YubiKeys in a variety of authentication scenarios:

- As an authenticator for Duo Passwordless logins.
- As a two-factor security key used during browser-based authentication featuring Duo's traditional prompt or Universal Prompt.
- As a WebAuthn passkey for Duo administrator logins to the Duo Admin Panel.
- As an OTP-generating hardware token for any Duo application which supports passcodes for two-factor authentication, including administrator login to the Duo Admin Panel.

https://duo.com/docs/yubikey

But is extra hardware hard to manage ?



Settings

Type: AWS IAM - Single Sign-On

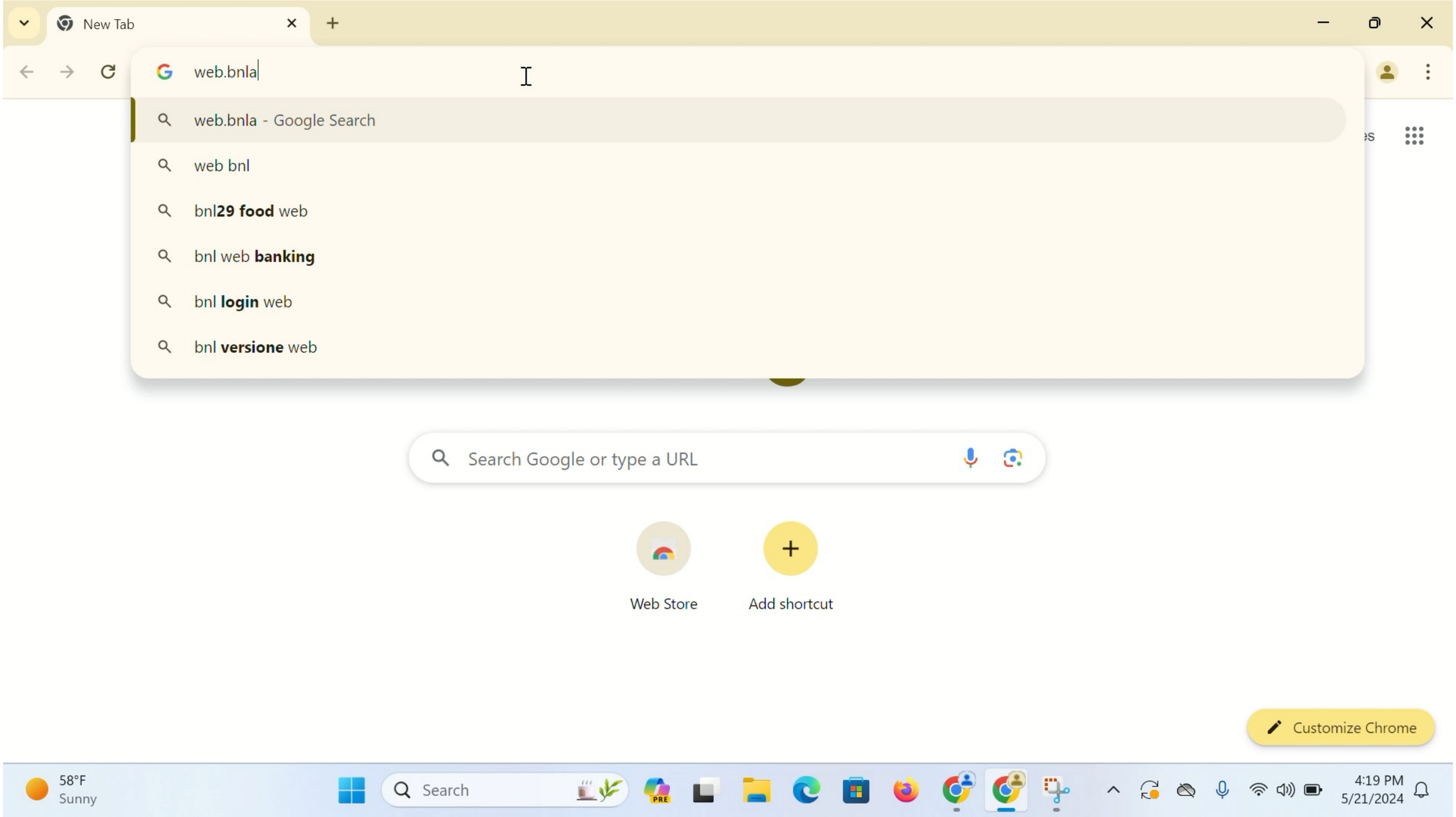
Name: Amazon Web Services - Single Sign-On

Duo Push users will see this when approving transactions.

Self-service portal: ☑ Let users remove devices, add new devices, and reactivate Duo Mobile

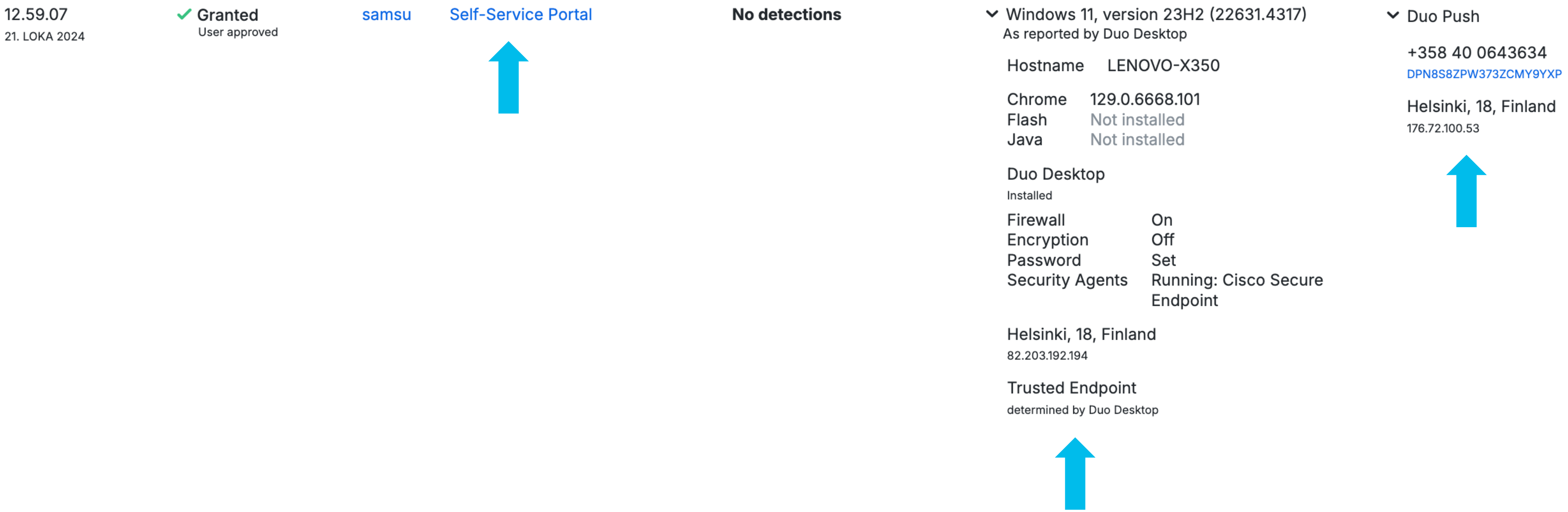
See Self-Service Portal documentation.

To allow Duo to notify users about self-service portal activity, select Settings > Notifications



web.bnla

New Tab
web.bnla - Google Search
web bnl
bnl29 food web
bnl web banking
bnl login web
bnl versione web
Search Google or type a URL
Web Store
Add shortcut
Customize Chrome
58°F
Sunny
Search
4:19 PM
5/21/2024



12.59.07
21. LOKA 2024

✓ Granted
User approved

samsu

Self-Service Portal

No detections

Windows 11, version 23H2 (22631.4317)
As reported by Duo Desktop

Hostname LENOVO-X350

Chrome 129.0.6668.101
Flash Not installed
Java Not installed

Duo Desktop
Installed

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

Helsinki, 18, Finland
82.203.192.194

Trusted Endpoint
determined by Duo Desktop

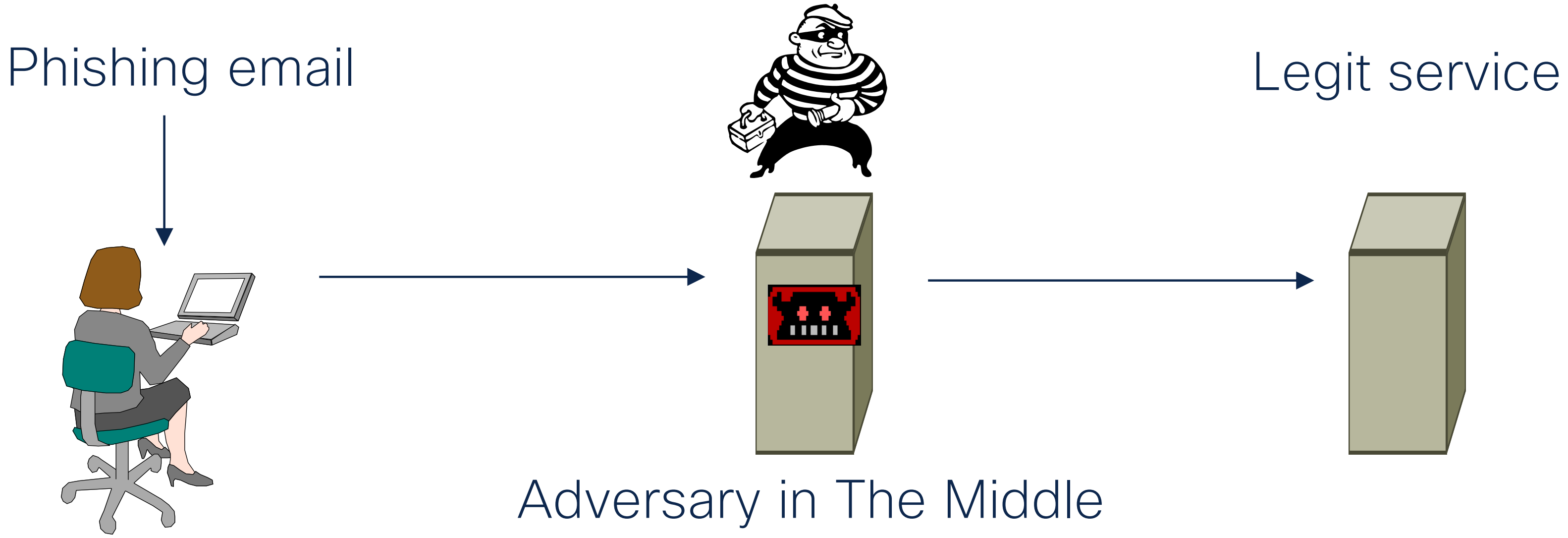
Duo Push

+358 40 0643634
DPN8S8ZPW373ZCMY9YXP

Helsinki, 18, Finland
176.72.100.53

OK, this is convenient but how about security ?

Increasing number of M365 data breaches utilise AiTM phishing technique

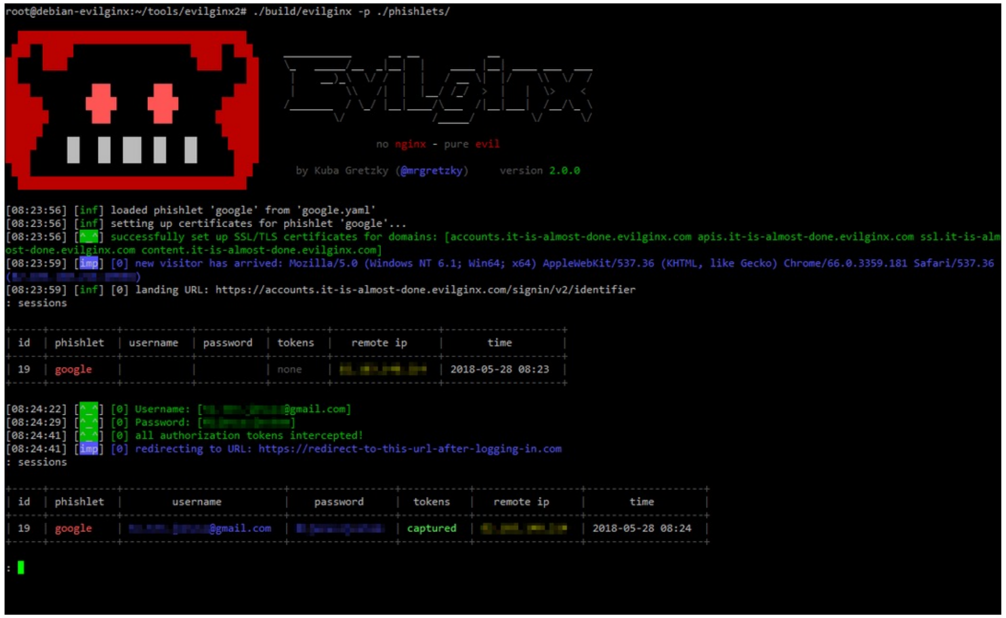


https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/increasing-number-m365-data-breaches-utilise-aitm-phishing

Evilginx 3.0

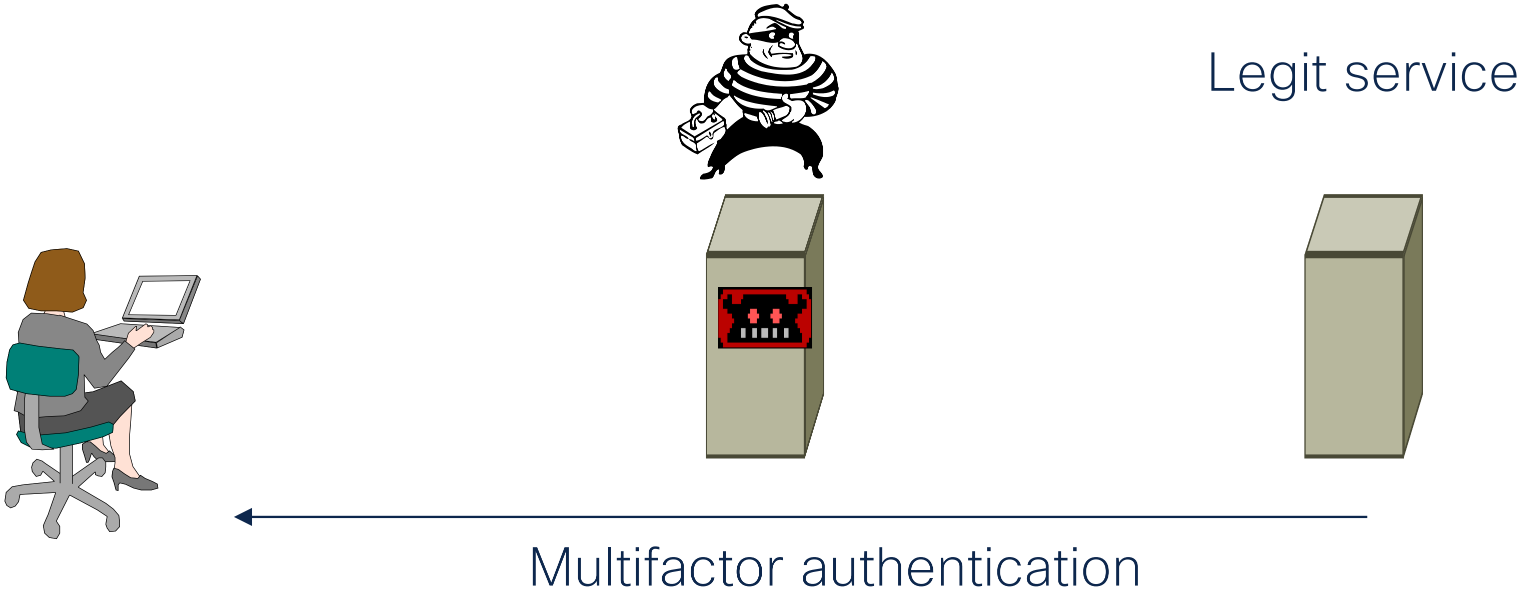
Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to Evilginx, released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.



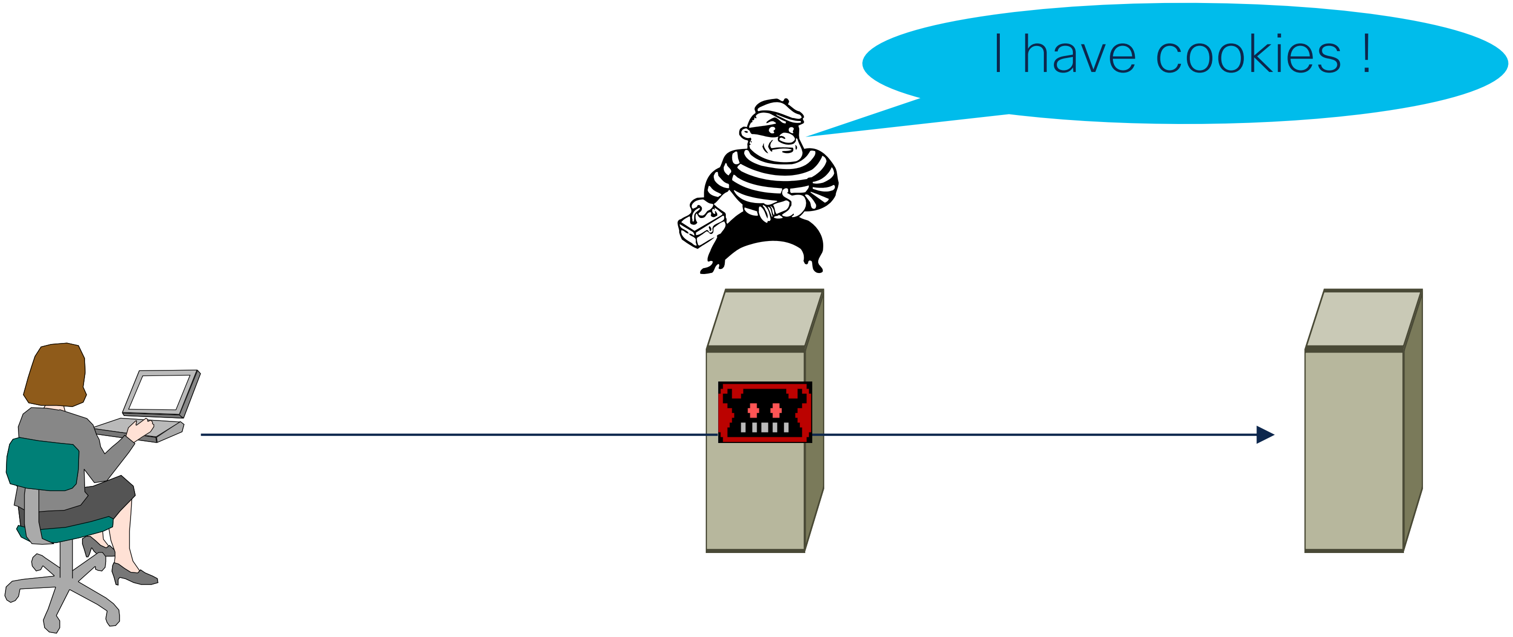
```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                    no nginx - pure evil

          by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+----+----------+----------+----------+--------+-------------+------------------+
| id | phishlet | username | password | tokens |  remote ip  |       time       |
+----+----------+----------+----------+--------+-------------+------------------+
| 19 | google   |          |          | none   | [redacted]  | 2018-05-28 08:23 |
+----+----------+----------+----------+--------+-------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+----+----------+-----------------------+------------+----------+-------------+------------------+
| id | phishlet |       username        |  password  |  tokens  |  remote ip  |       time       |
+----+----------+-----------------------+------------+----------+-------------+------------------+
| 19 | google   | [redacted]@gmail.com  | [redacted] | captured | [redacted]  | 2018-05-28 08:24 |
+----+----------+-----------------------+------------+----------+-------------+------------------+

: 
```

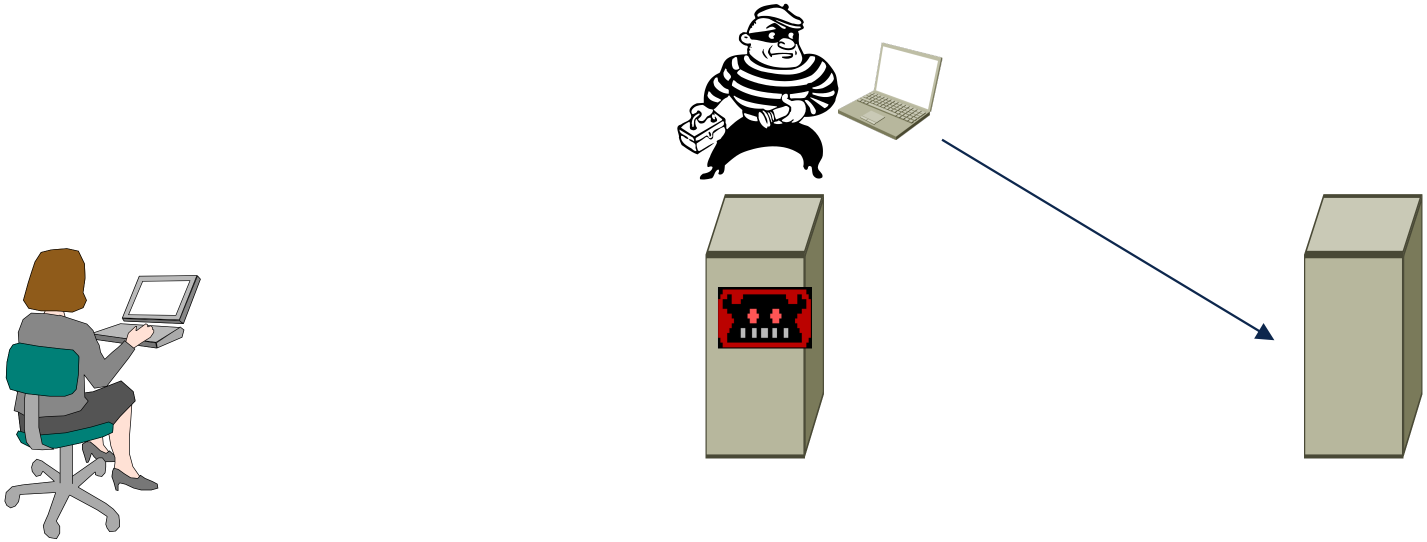
https://github.com/kgretzky/evilginx2



Legit service

Multifactor authentication


I have cookies !



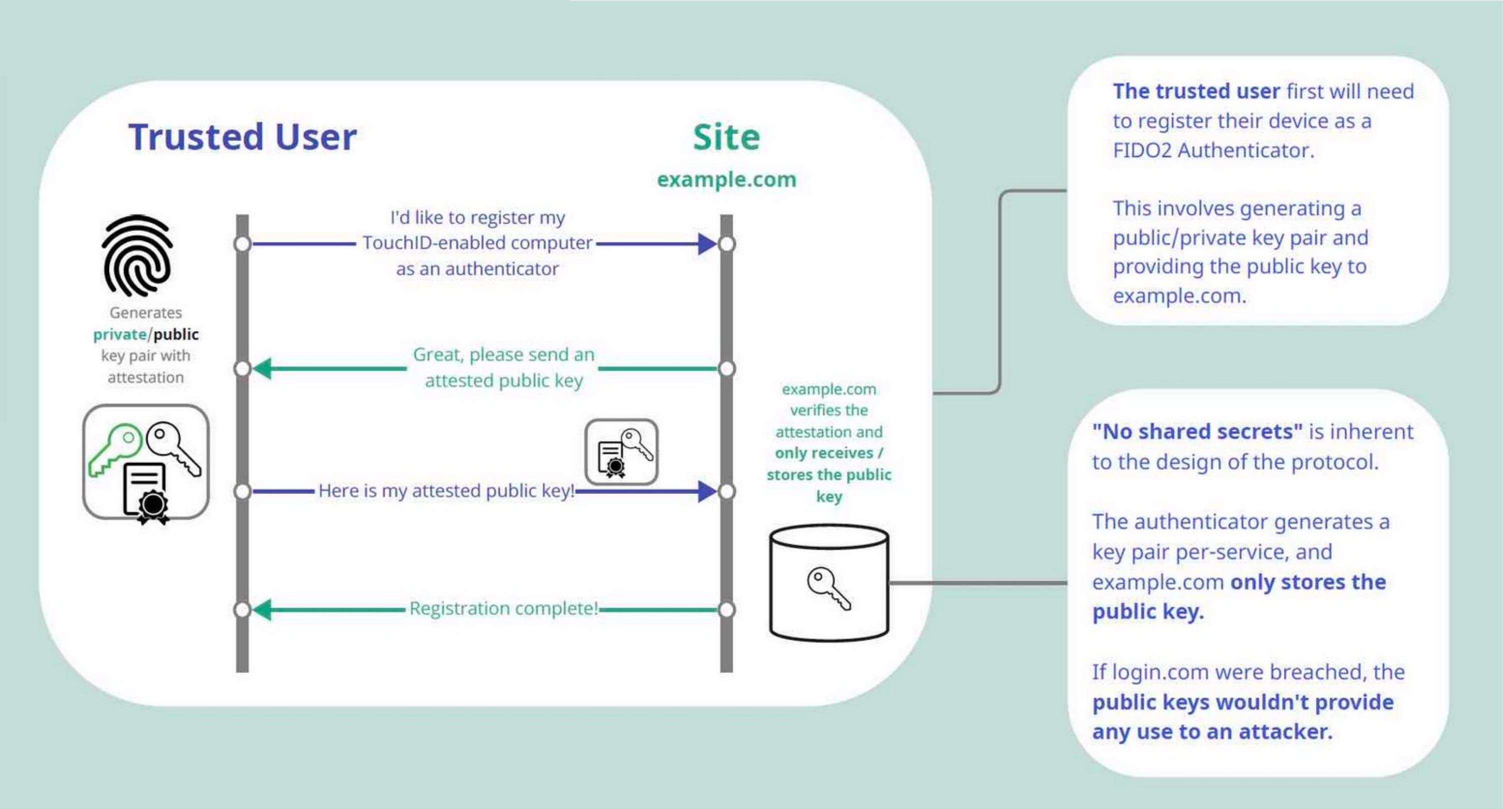
Protections against AiTM

- Certificate based authentication
- Only allow logins from Trusted Devices
- Passwordless using Yubikey or biometrics

And maybe you want to detect threats using

- Identity Threat Detection and Mitigation

No Shared Secrets


Trusted User
Site
example.com
Generates private/public key pair with attestation
I'd like to register my TouchID-enabled computer as an authenticator
Great, please send an attested public key
Here is my attested public key!
example.com verifies the attestation and only receives / stores the public key
Registration complete!

The trusted user first will need to register their device as a FIDO2 Authenticator.

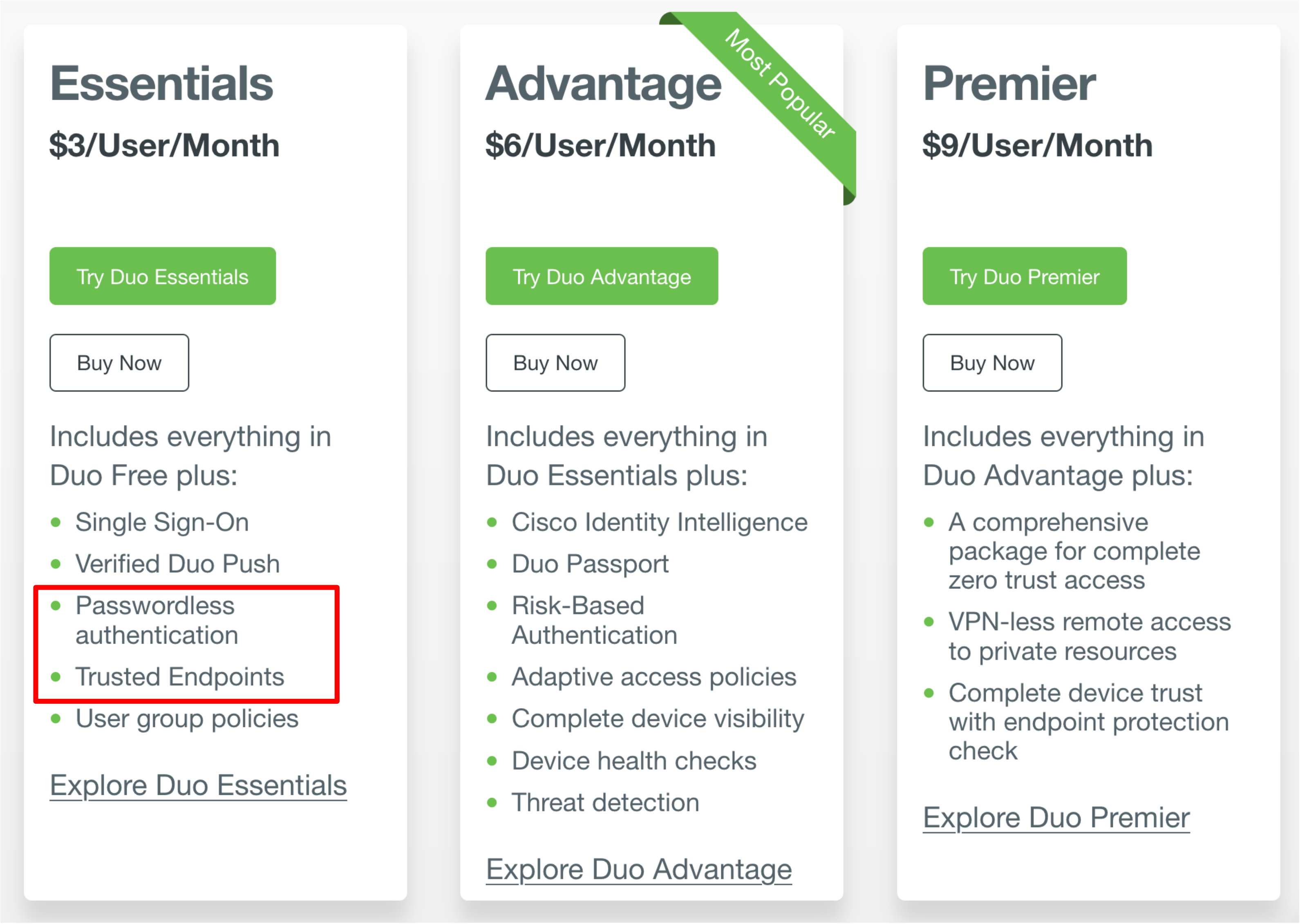
This involves generating a public/private key pair and providing the public key to example.com.

"No shared secrets" is inherent to the design of the protocol.

The authenticator generates a key pair per-service, and example.com **only stores the public key.**

If login.com were breached, the **public keys wouldn't provide any use to an attacker.**

https://duo.com/blog/understanding-defending-against-adversary-in-the-middle-aitm-attacks



Essentials

$3/User/Month

Try Duo Essentials

Buy Now

Includes everything in Duo Free plus:

- Single Sign-On
- Verified Duo Push
- Passwordless authentication
- Trusted Endpoints
- User group policies

Explore Duo Essentials

Advantage

$6/User/Month

Try Duo Advantage

Buy Now

Includes everything in Duo Essentials plus:

- Cisco Identity Intelligence
- Duo Passport
- Risk-Based Authentication
- Adaptive access policies
- Complete device visibility
- Device health checks
- Threat detection

Explore Duo Advantage

Premier

$9/User/Month

Try Duo Premier

Buy Now

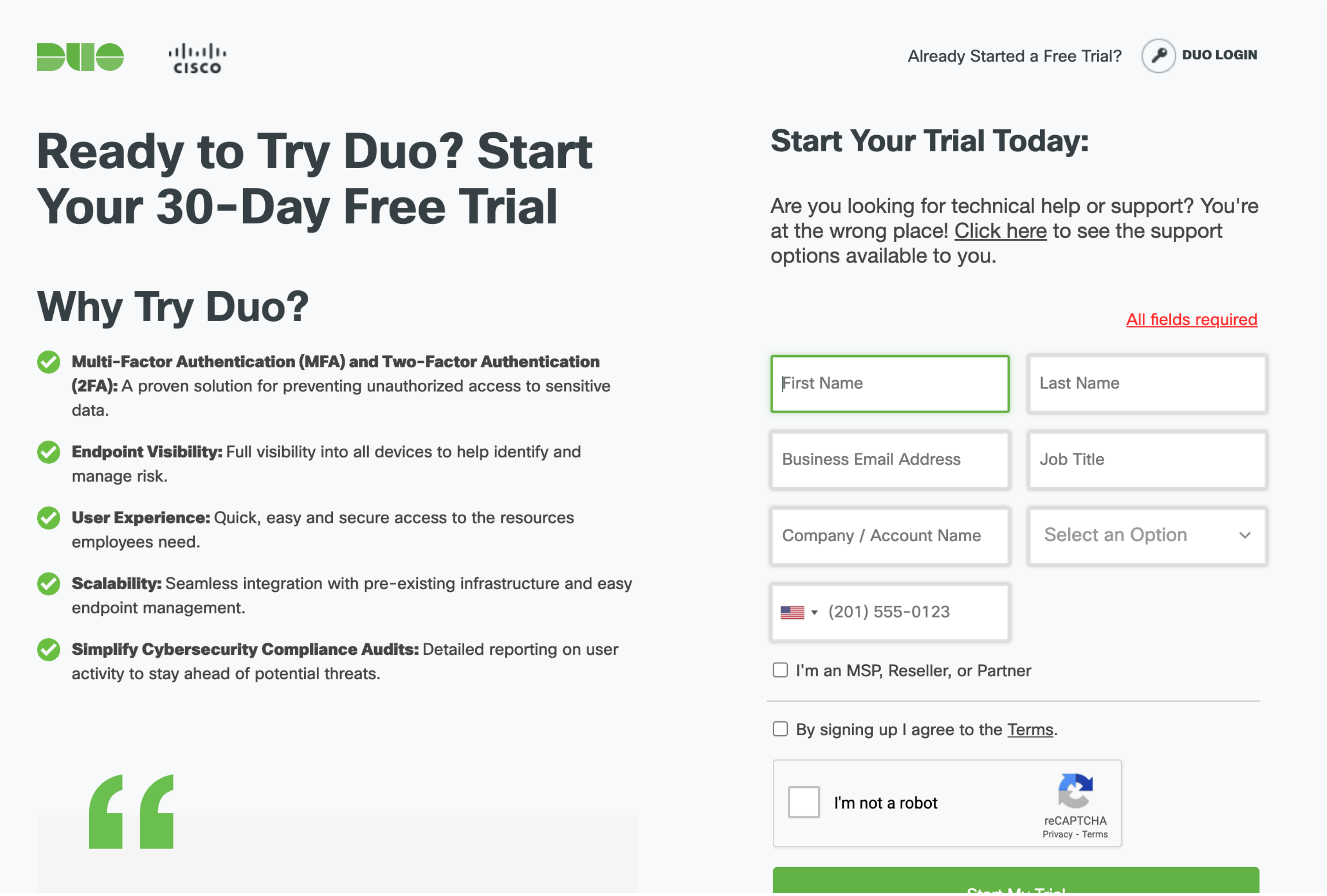
Includes everything in Duo Advantage plus:

- A comprehensive package for complete zero trust access
- VPN-less remote access to private resources
- Complete device trust with endpoint protection check

Explore Duo Premier

https://duo.com/editions-and-pricing

https://signup.duo.com



Already Started a Free Trial?

Ready to Try Duo? Start Your 30-Day Free Trial

Why Try Duo?

- ✓ **Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA):** A proven solution for preventing unauthorized access to sensitive data.
- ✓ **Endpoint Visibility:** Full visibility into all devices to help identify and manage risk.
- ✓ **User Experience:** Quick, easy and secure access to the resources employees need.
- ✓ **Scalability:** Seamless integration with pre-existing infrastructure and easy endpoint management.
- ✓ **Simplify Cybersecurity Compliance Audits:** Detailed reporting on user activity to stay ahead of potential threats.

“

Start Your Trial Today:

Are you looking for technical help or support? You're at the wrong place! Click here to see the support options available to you.

All fields required

First Name	Last Name
Business Email Address	Job Title
Company / Account Name	Select an Option
(201) 555-0123	

□ I'm an MSP, Reseller, or Partner

□ By signing up I agree to the Terms.

□ I'm not a robot

More info

- https://duo.com/blog/cybersecurity-threats-2023-how-itdr-can-help
- https://duo.com/resources/ebooks/2024-duo-trusted-access-report
- https://duo.com/resources/webinars/so-identity-is-the-new-perimeter-why-is-it-so-hard-to-defend

CISCO SECURE