LastPass in combination with DUO

Use Case documentation

Silta
a Ferranti company

Author(s)	Ronnie Dibbaut
Issue	major
Date	24/07/2020

Company confidential

Table of Contents

1 Introduction

Shift in IT landscape:

With cloud applications all over the place, teleworking being the new normal and employees working on all sorts of devices, from mobile corporate devices to BYOD, security has taken a new turnaround.

There is clearly a shift in IT landscape where the perimeter has been evolving meaning that the business challenges are also evolving. The attack surface and access possibilities are increasing and the CISO's visibility and control over users, devices, applications and the broader network is decreasing.

Basically, accessing IT systems happens from everywhere on all sorts of devices.

How can you gain visibility and control over that shattered network and all those devices?

How can you prevent risks and reduce it before a breach occurs?

The secret lies in the Zero Trust approach where you need to shift from a traditional security approach, i.e. trust being based on the network location that an access request is coming from, to this Zero Trust approach where every access request needs to be verified, regardless where the request is coming from.

Zero Trust:

Do you need to block everything and work only via corporate devices which are centrally managed?

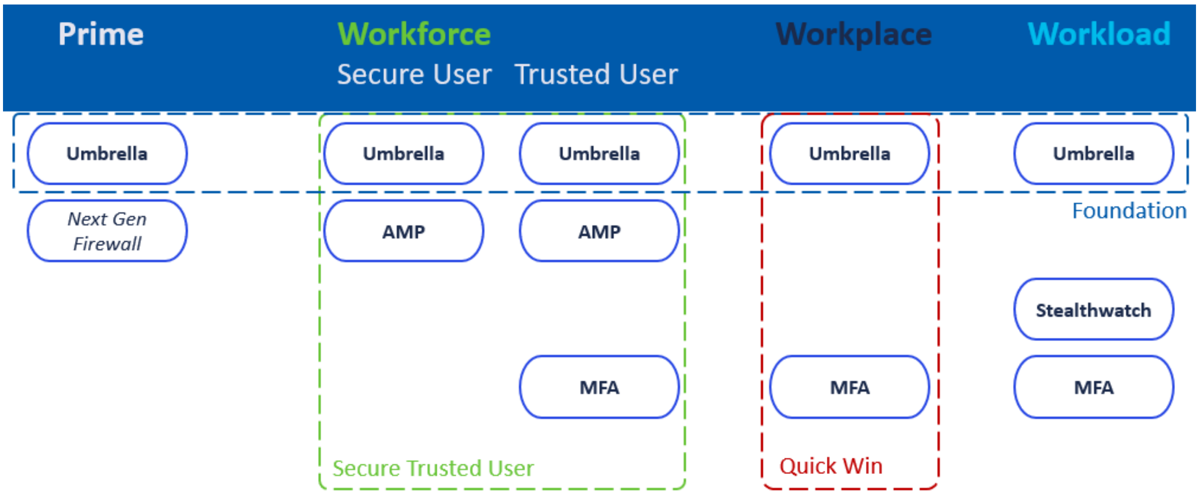
You need to extend trust to support a modern enterprise with BYOD, cloud apps, hybrid environments and more.

Secure access across your applications, network and ensure that only the right users and devices have access.

Silta created a framework, working with Cisco's finest SAAS solutions to help you implement your Zero Trust approach, organized around three pillars:

- Workforce:
  - Is the user who he says he is?
  - Does he have access to the right applications?
  - Is the device secure and trusted?
- Workload:
  - What applications are used in the enterprise?
  - What is communicating with these applications and data?
  - Is the communication trusted?
- Workplace:
  - Do users and devices authenticate for network access?
  - What access are they granted
  - Are devices on the network secure
  - Is there network segmentation based in trust?

Silta’s security product portfolio:



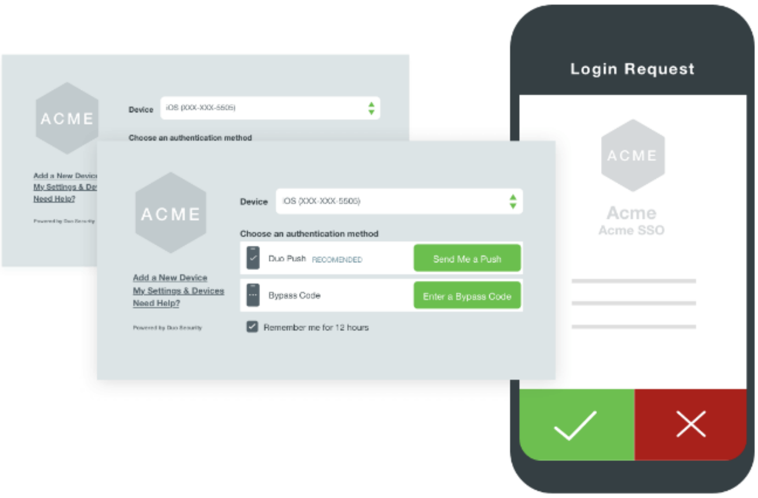
For every organisation there is a solution that can be build around those pillars. From the Silta Prime solution with basic DNS protection using Cisco Umbrella in combination with already existing Firewalling, to a combination of multiple pillars and products for a trusted, secure user accessing secure workloads from a secure workplace.

Use Case:

In this use case documet, we will explain how to implement DUO as a multi factor authenticator (MFA) in combination with accessing the LastPass password vault. The principle of adding an application is always the same.

2 Cisco DUO

Multi-factor authentication from Cisco's Duo protects your applications by using a second source of validation, like a phone or token, to verify user identity before granting access. Duo is engineered to provide a simple, streamlined login experience for every user and application, and as a cloud-based solution, it integrates easily with your existing technology.

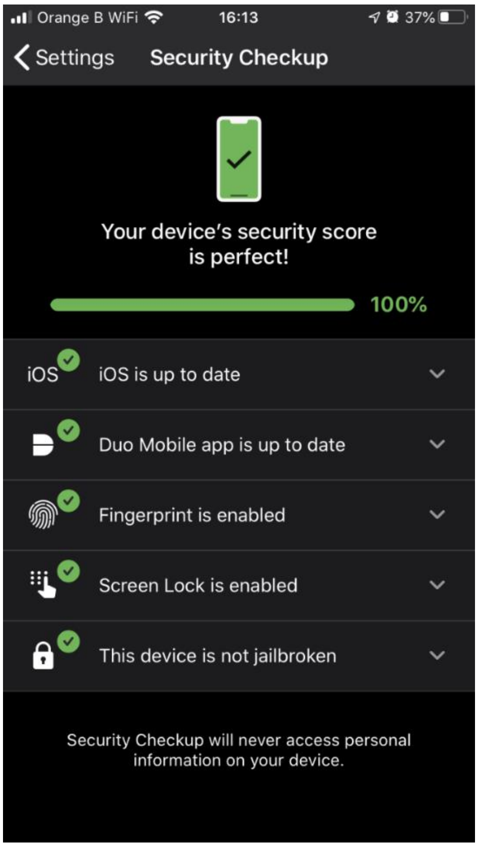


With DUO MFA, you can easily manage your users, but also the devices linked to those users. DUO gives you insight in de login attempts, in the OS versions of your phones, in the operating systems of your end points, etc.

Not just a regular MFA

It's way more than just an MFA. It enables you to create policies on how DUO is used (e.g. for every login attempt) and helps you in managing the devices' operating systems by giving you OS insights.

A security check-up is also embedded in the DUO mobile app and gives the user an insight in regards to the health status of his device and the DUO application:



Your device's security score is perfect!

100%

- ✓ iOS is up to date
- ✓ Duo Mobile app is up to date
- ✓ Fingerprint is enabled
- ✓ Screen Lock is enabled
- ✓ This device is not jailbroken

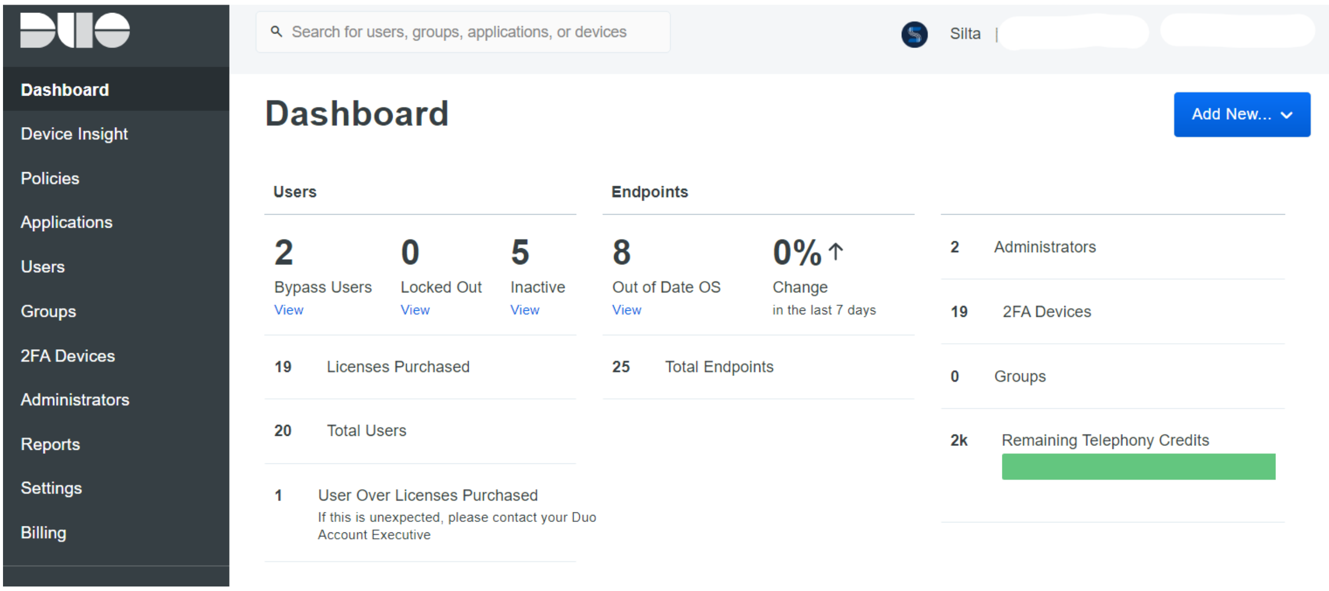
Security Checkup will never access personal information on your device.

Administrator user interface

DUO offers administrators a comprehensive user interface where the licenses, users, devices and devices can be managed.

By creating a profile/account via https://duo.com/ and test the free trial, you get access to the admin pane of duo-security.

Dashboard:



Search for users, groups, applications, or devices

Silta | [redacted] [redacted]

- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- 2FA Devices
- Administrators
- Reports
- Settings
- Billing

Dashboard

Add New...

Users

2 Bypass Users View

0 Locked Out View

5 Inactive View

19 Licenses Purchased

20 Total Users

1 User Over Licenses Purchased
If this is unexpected, please contact your Duo Account Executive

Endpoints

8 Out of Date OS View

0% ↑ Change in the last 7 days

25 Total Endpoints

2 Administrators

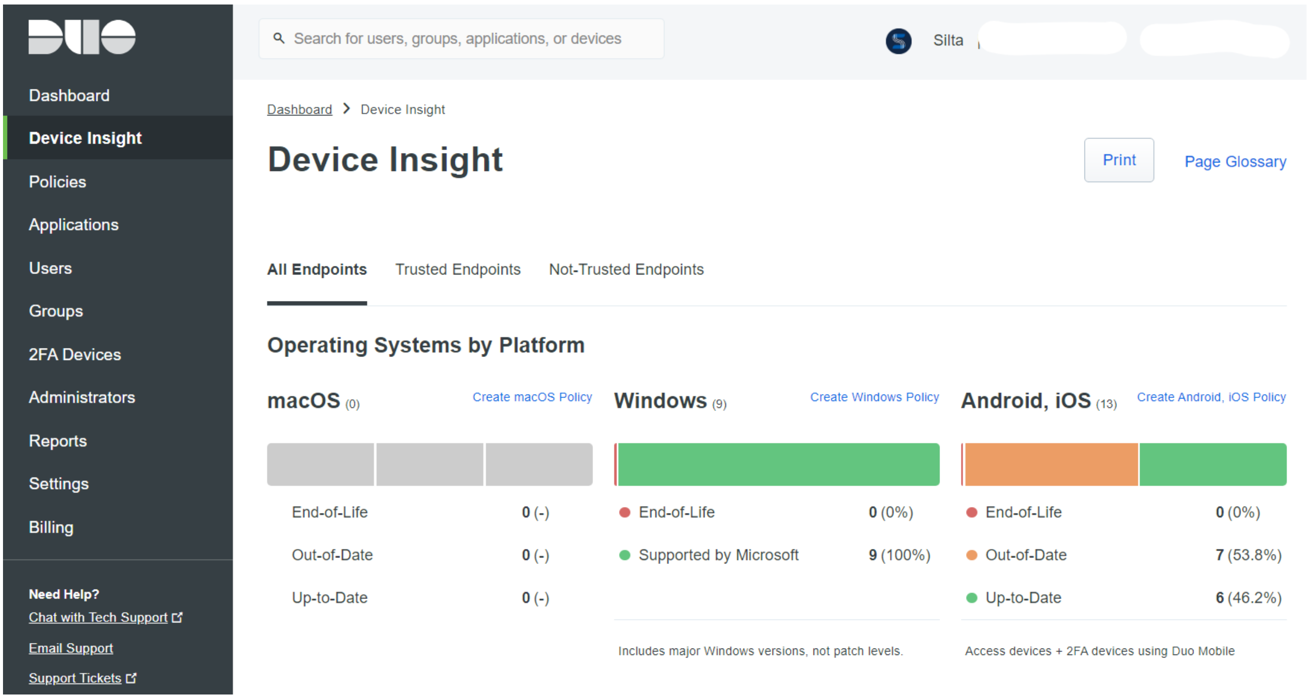
19 2FA Devices

0 Groups

2k Remaining Telephony Credits

The dashboard is an overview page.

Device Insight



Search for users, groups, applications, or devices

Silta [redacted] [redacted]

- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- 2FA Devices
- Administrators
- Reports
- Settings
- Billing

Need Help?
Chat with Tech Support
Email Support
Support Tickets

Dashboard > Device Insight

Device Insight

Print   Page Glossary

All Endpoints   Trusted Endpoints   Not-Trusted Endpoints

Operating Systems by Platform

macOS (0)   Create macOS Policy

End-of-Life	0 (-)
Out-of-Date	0 (-)
Up-to-Date	0 (-)

Windows (9)   Create Windows Policy

● End-of-Life	0 (0%)
● Supported by Microsoft	9 (100%)

Includes major Windows versions, not patch levels.

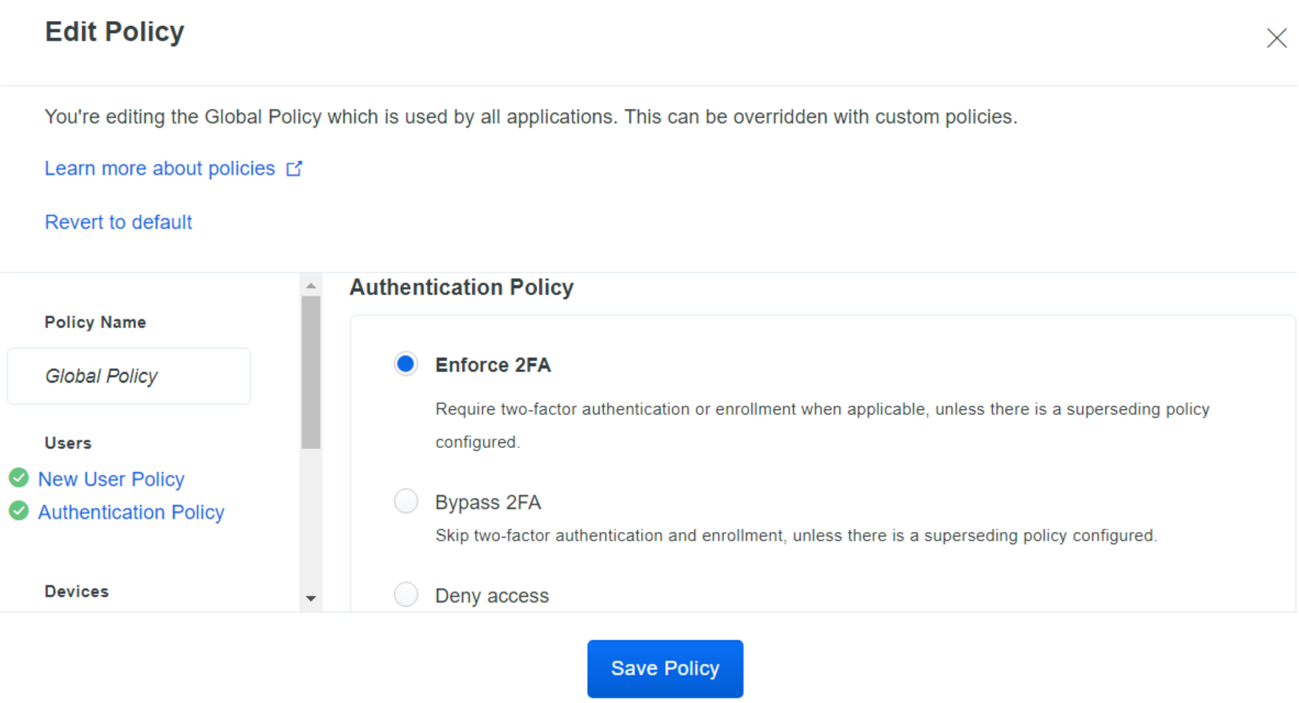
Android, iOS (13)   Create Android, iOS Policy

● End-of-Life	0 (0%)
● Out-of-Date	7 (53.8%)
● Up-to-Date	6 (46.2%)

Access devices + 2FA devices using Duo Mobile

This page gives an overview of the mobile devices and their operating systems. Interesting is to look at the mobile phones. Here you see that 7 devices have an out of date operating system.

The policies pane gives you the possibility to configure policies in regards to the use of 2FA, e.g. by enforcing the use of 2FA for authentication purposes as shown hereunder:



Edit Policy

You're editing the Global Policy which is used by all applications. This can be overridden with custom policies.

Learn more about policies

Revert to default

Policy Name: Global Policy

Users

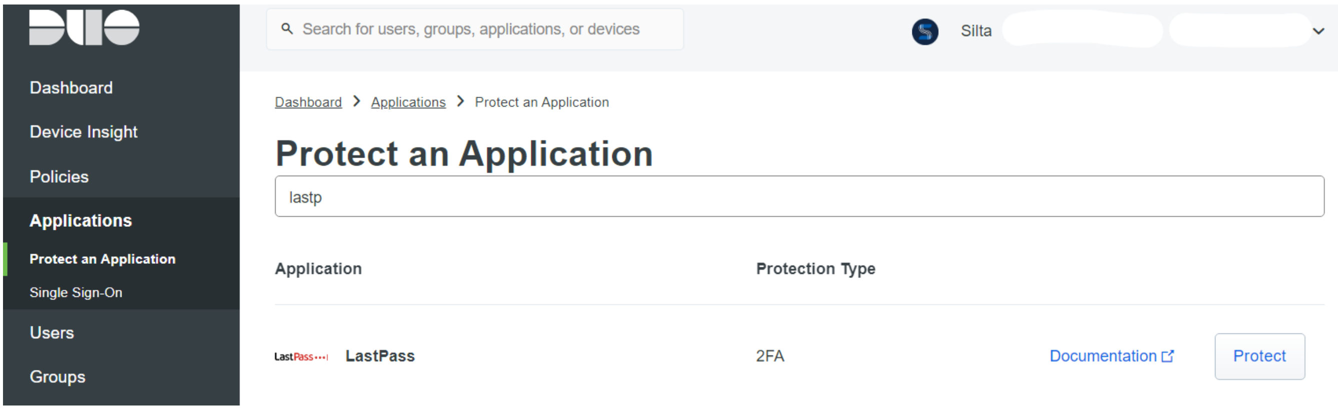
- ✓ New User Policy
- ✓ Authentication Policy

Devices

Authentication Policy

- ● Enforce 2FA
  Require two-factor authentication or enrollment when applicable, unless there is a superseding policy configured.
- ○ Bypass 2FA
  Skip two-factor authentication and enrollment, unless there is a superseding policy configured.
- ○ Deny access

Applications



Dashboard > Applications > Protect an Application

Protect an Application

lastp

Application	Protection Type		
LastPass	2FA	Documentation	Protect

An application is every 3rd party app that you want to protect with MFA. But it could also be meant for another operating systems (like macOS).

All the necessary documentation is foreseen as well to help you with the setup of the specified application or operating system.

3 LastPass

(Source: LastPass Technical Whitepaper)

LastPass encourages users to enable multifactor authentication to add an additional layer of protection to an account. Multifactor authentication requires another piece of information before access is granted.

Companies can mandate use of multifactor authentication with LastPass through policies available in the admin dashboard.

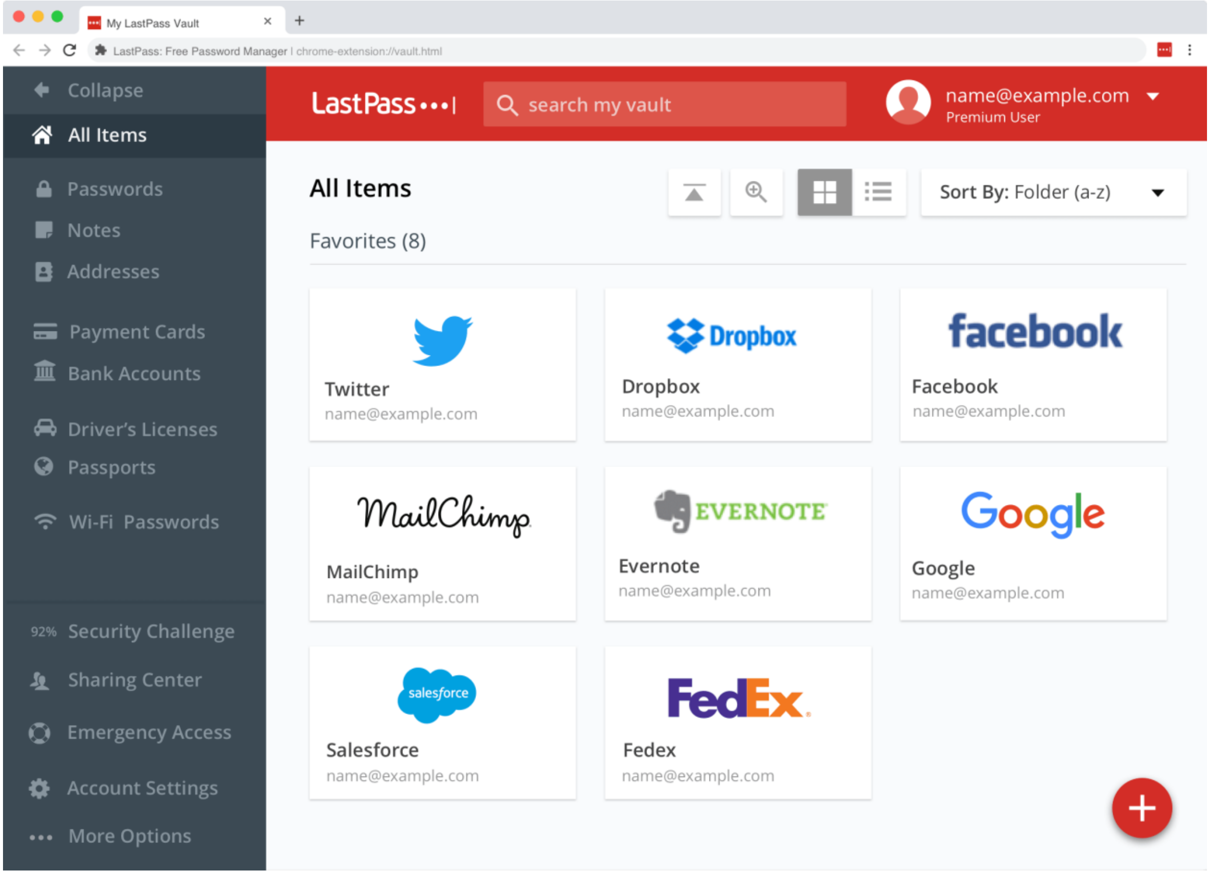
Multifactor authentication requires two or more authentication factors, including something the user

knows (the master password), in addition to something they have (a code, a key) and/or something they are (a fingerprint). By requiring not only the master password, but also an additional login step (like a one-time password, a fingerprint swipe, a randomly-generated 6-digit code), a user adds another layer of protection against unauthorized access to their account.

If an attacker were to discover a user's Master Password, it's unlikely that they would also have access to a valid multifactor token, therefore minimizing the chance that they would be unable to gain access to the user's account.

Admins can mandate multifactor authentication through policies in the admin dashboard, requiring use of any supported multifactor authentication option or requiring use of only specific, company-approved multifactor authentication options.

Administrator pane



LastPass is able to create different folders, e.g. a private folder and a shared folder, shared with a certain group or team.

We use LastPass to keep the passwords safe of all the different customer environments that we manage, in combination with a mandatory MFA step for user authentication.

4 Application set up

(source: https://duo.com/docs/lastpass)

The setup is described for LastPass Free and Premium editions.

1. Sign up for a Duo account. The Duo Free plan is free for up to ten users with unlimited applications.
2. Log in to the Duo Admin Panel and navigate to **Applications**.
3. Click **Protect an Application** and locate **LastPass** in the applications list. Click **Protect this Application** to get your **integration key**, **secret key**, and **API hostname**. (See Getting Started for help.)

Treat your secret key like a password

The security of your Duo application is tied to the security of your secret key (skey). Secure it as you would any sensitive credential. Don't share it with unauthorized individuals or email it to anyone under any circumstances!

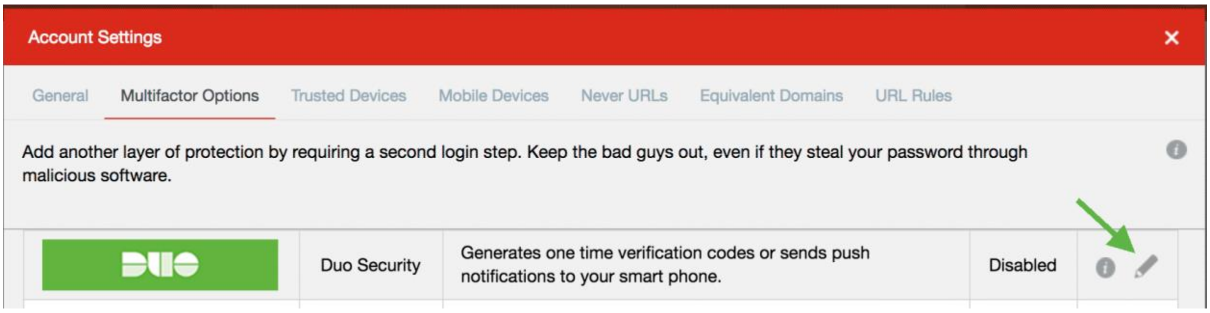
If you followed a Duo sign-up link from the LastPass site then we'll automatically create a LastPass application for you!

Configure Duo Security

1. Log in to your LastPass vault.

2. Once logged in to LastPass go to **Account Settings** → **Multifactor Options**.

3. Click the pencil icon to the right of the **Duo Security** multifactor option.



Account Settings

Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software.

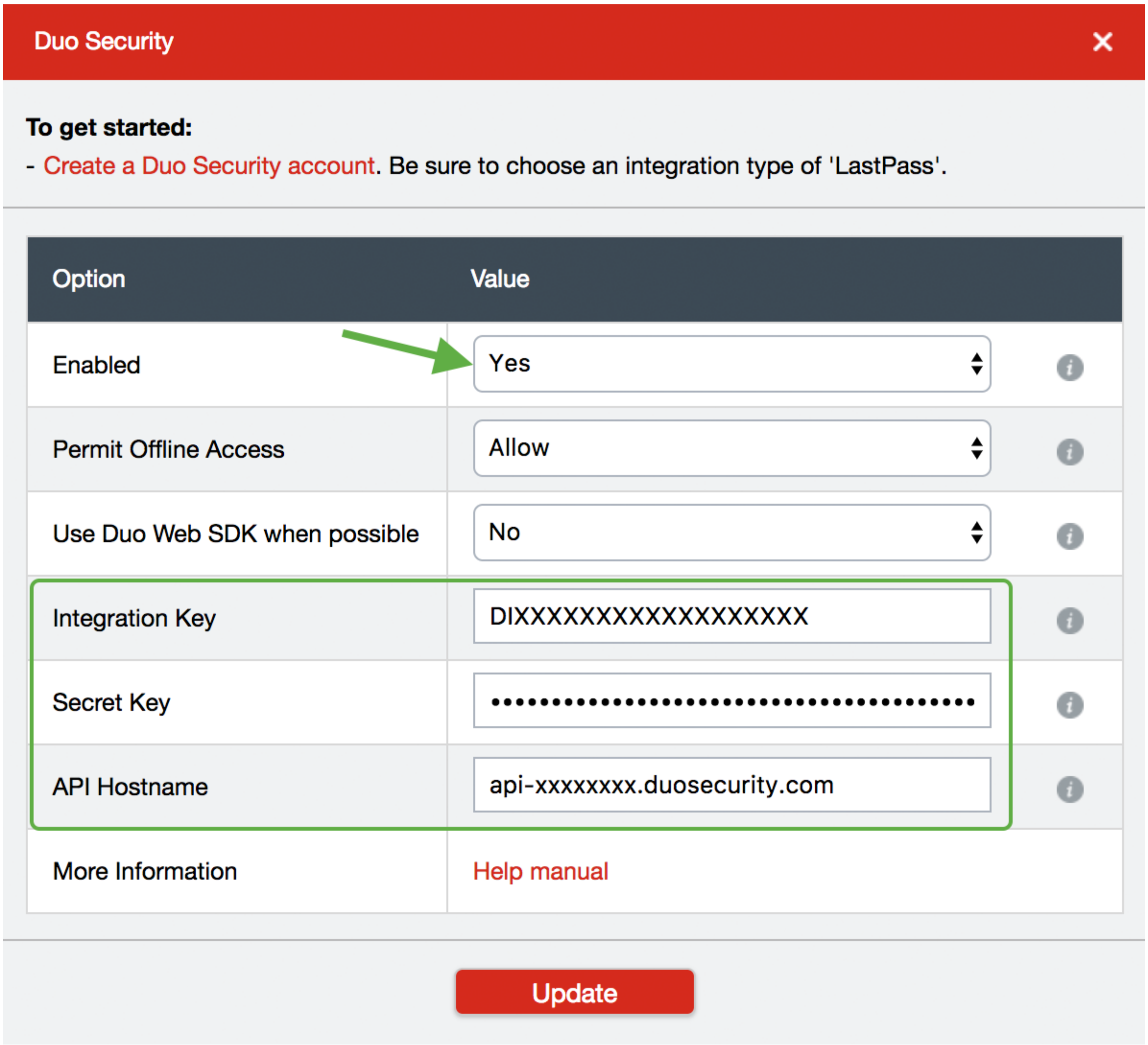
Duo Security	Generates one time verification codes or sends push notifications to your smart phone.	Disabled	

4. Configure the Duo Security options as follows:

Option	Value
Enabled	Select **Yes**.
Permit Offline Access	Set to **Allow** if you want access to your password vault even when LastPass is unreachable. For more information about this option please see the topic "Offline Access to Your LastPass Vault" in the LastPass User Manual.

Option	Value
Use Duo Web SDK when possible	The default setting (No) means that all types of clients see the same LastPass Duo prompt. If you'd like to enable the interactive authentication prompt for web browser logins to LastPass, change this setting to **Yes**.
Integration Key	Copy and paste in the **integration key** from the LastPass application you created earlier in the Duo Admin Panel.
Secret Key	Copy and paste in the **secret key** from the LastPass application you created earlier in the Duo Admin Panel.
API Hostname	Copy and paste in the **API hostname** from the LastPass application you created earlier in the Duo Admin Panel.

5. Click **Update** when done.



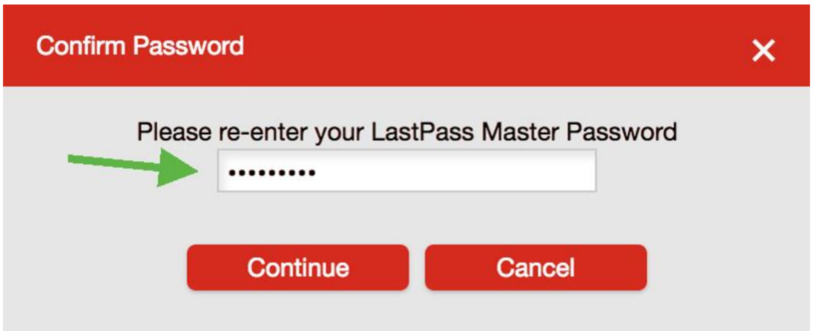
Duo Security

To get started:

- Create a Duo Security account. Be sure to choose an integration type of 'LastPass'.

Option	Value
Enabled	Yes
Permit Offline Access	Allow
Use Duo Web SDK when possible	No
Integration Key	DIXXXXXXXXXXXXXXXXXX
Secret Key	••
API Hostname	api-xxxxxxxx.duosecurity.com
More Information	Help manual

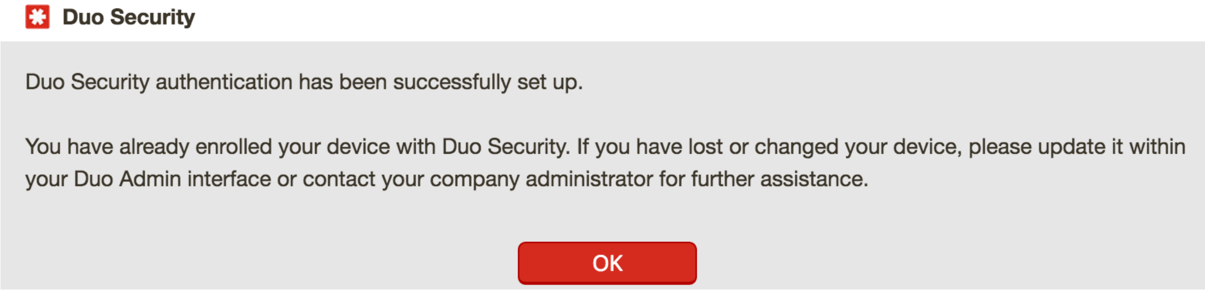
6. Enter your LastPass password to confirm the change to your account.



Confirm Password

Please re-enter your LastPass Master Password

7. If your LastPass email address is already enrolled in Duo there are no additional enrollment steps required.

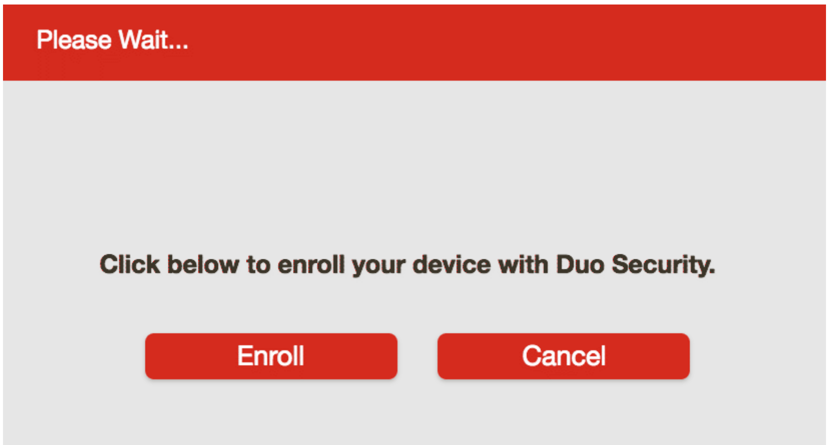


Duo Security

Duo Security authentication has been successfully set up.

You have already enrolled your device with Duo Security. If you have lost or changed your device, please update it within your Duo Admin interface or contact your company administrator for further assistance.

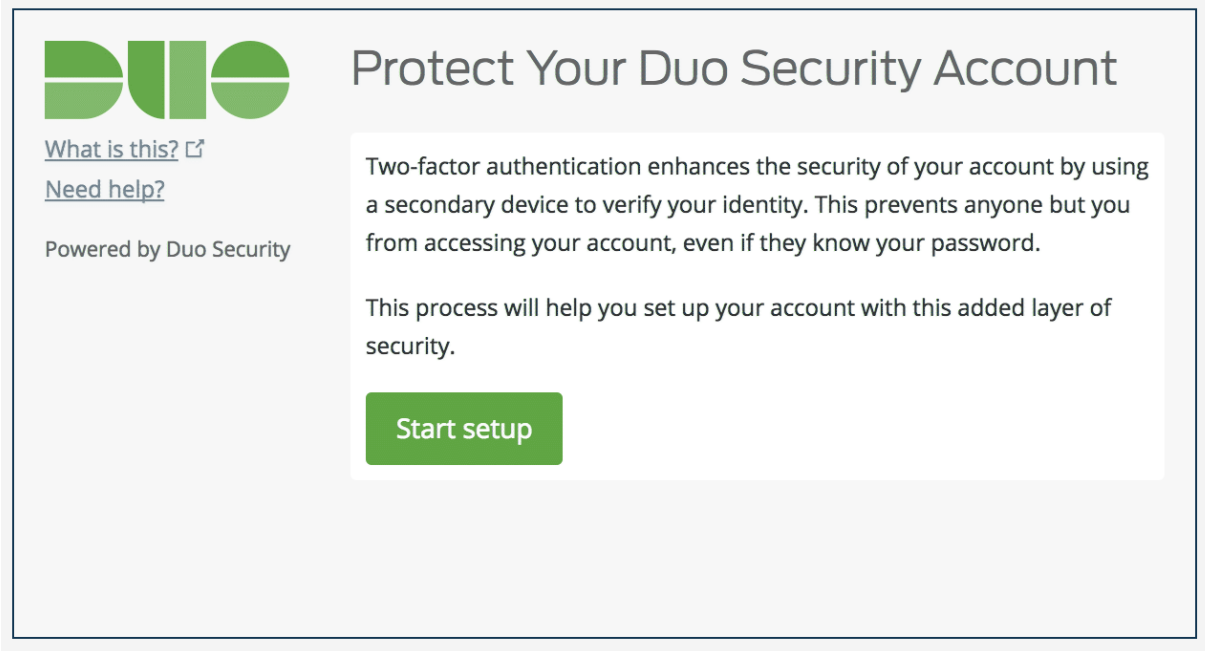
If the email address you use to log on to LastPass is not enrolled as a user in your Duo account, LastPass prompts you complete Duo enrollment in a new browser tab.



Please Wait...

Click below to enroll your device with Duo Security.

Follow the on-screen steps to complete device enrollment. Please see our user guide to enrollment for more information.

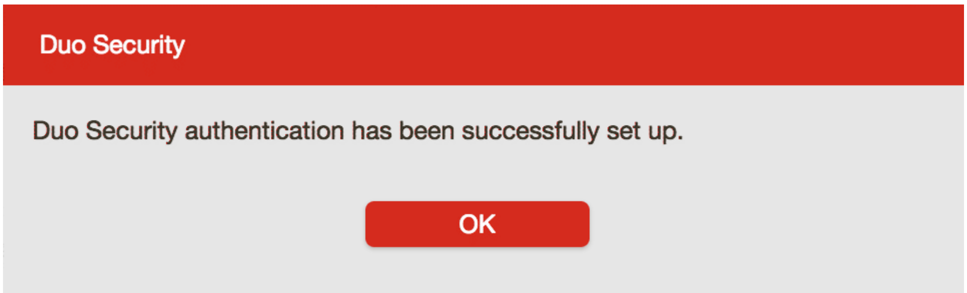


Protect Your Duo Security Account

Two-factor authentication enhances the security of your account by using a secondary device to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.

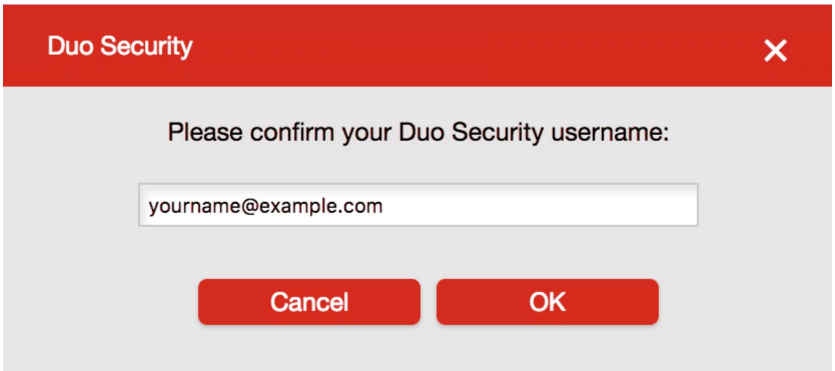
8. You can close the Duo browser tab when you see the message "Enrollment successful!" The LastPass browser window displays a message letting you know your setup is complete.



Duo Security

Duo Security authentication has been successfully set up.

9. Verify your LastPass account email address to apply all changes.

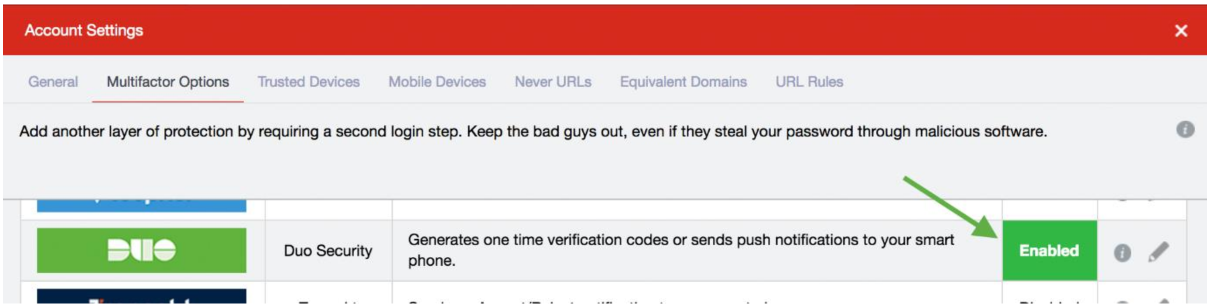


Duo Security

Please confirm your Duo Security username:

yourname@example.com

10. The Duo Security option now shows as "Enabled" on the LastPass Multifactor Options page.



Account Settings

General | Multifactor Options | Trusted Devices | Mobile Devices | Never URLs | Equivalent Domains | URL Rules

Add another layer of protection by requiring a second login step. Keep the bad guys out, even if they steal your password through malicious software.

DUO	Duo Security	Generates one time verification codes or sends push notifications to your smart phone.	Enabled

Instructions for configuring LastPass with Duo are also available in the [LastPass User Manual](https://).

Test Your Setup

Enable Hostname Whitelisting

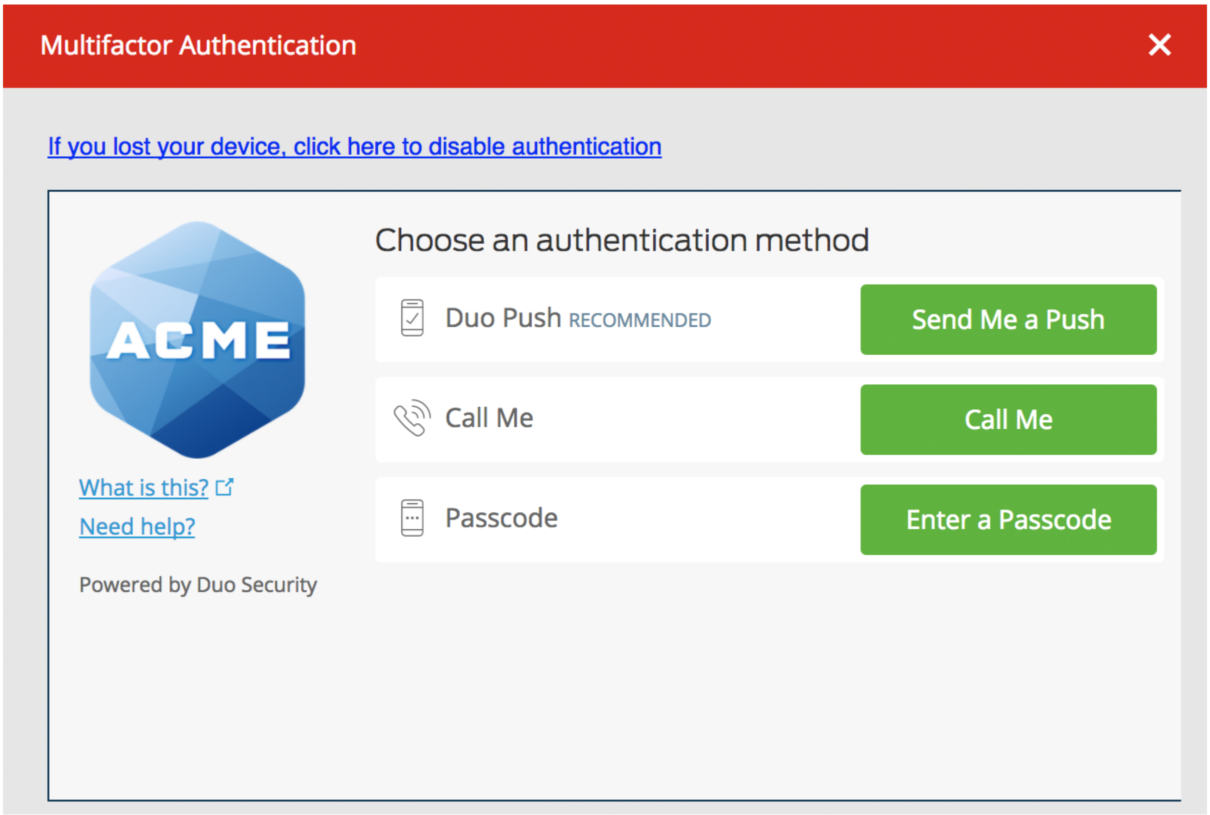
If you plan to permit use of WebAuthn authentication methods (security keys, U2F tokens, or Touch ID), Duo recommends enabling hostname whitelisting for this application and any others that show the inline Duo Prompt before onboarding your end-users.

After completing multifactor setup, you'll see the Duo authentication prompt when you log in to LastPass. You can approve a Duo Push authentication request on your smartphone or tablet, approve authentication over the phone, or enter a passcode generated via the Duo Mobile app, text message, or hardware token.

5 User Login Experience

After completing multifactor setup, users see the Duo authentication prompt when they log in to LastPass. Users can approve a Duo Push authentication request from a smartphone or tablet, approve authentication over the phone, or enter a passcode generated via the Duo Mobile app, text message, or hardware token.

If you did enable the Duo Web SDK policy for your organization, browser logons to LastPass show the interactive Duo prompt, while mobile app logins continue to show the original LastPass multifactor prompt.



Multifactor Authentication

If you lost your device, click here to disable authentication

Choose an authentication method

Powered by Duo Security

When your LastPass Enterprise users view their multifactor options for Duo, the setting shows as enforced by company policy.

Ready for your first implementation? Do not hesitate to contact us directly or via the website.