

Company Package Manual for Admins

Thank you for choosing Boxcryptor.

Boxcryptor is an easy-to-use solution for cloud-based encryption. In this manual you will learn how to set up the Boxcryptor Company Package and how to use Boxcryptor to ensure privacy in the cloud.

The screenshots and instructions in this manual use Google Chrome and Windows 8.1 Pro.

New: Boxcryptor with Whisply Integration



Content

New: Boxcryptor with Whispaly Integration	1
1. About Boxcryptor	3
1.1 Boxcryptor Company Package	3
2. Create and Enable your Boxcryptor Company Package	3
2.1 Create a Boxcryptor Account.....	3
2.2 Start the Company Package Trial	4
3. Setting up the Boxcryptor Company Package.....	4
3.1 Add Users	4
3.1.1 Add Users via Email	5
3.1.2 Add Users via Active Directory	6
3.1.3 Add Users Using Dropbox Business.....	9
3.2 Set Policies.....	11
3.2.1 Policy Overview	11
3.2.2 Add Policy.....	13
3.3 Create a Master Key	15
3.3.1 Generate Key.....	15
3.3.2 Set the Master Key Policy	17
3.3.3 How to Unlock the Master Key.....	18
4. Track User Activities	19
5. Two-Factor Authentication	21
5.1 Setup Duo and Boxcryptor	21
6. Whispaly Integration	25
Advantages of Whispaly	25
6.1 Whispaly Features	25
6.2 Send Files with Boxcryptor via Whispaly.....	26
Downloading the File	29
6.3 Whispaly Use Cases	29
7. Support	30

1. About Boxcryptor

Boxcryptor is a user-friendly encryption software optimized for the cloud. It allows the secure use of cloud storage services without sacrificing comfort. Boxcryptor supports all major cloud storage providers as well as all clouds using the WebDAV standard. With Boxcryptor, your files go to your cloud provider protected and you can enjoy peace of mind knowing your information cannot fall into the wrong hands.

Boxcryptor creates a virtual drive on your computer that allows you to encrypt your files locally before uploading them to your cloud or clouds of choice. It encrypts the single files - and does not create containers. Any file dropped into an encrypted folder within the Boxcryptor drive will be encrypted automatically before it is synced to the cloud. To protect your files, Boxcryptor uses the AES-256 and RSA encryption algorithms.

1.1 Boxcryptor Company Package

The Boxcryptor Company Package adds features specifically developed for teams and companies.

- **Master Key**
Decrypt every file which is accessible by any member of your organization.
- **Active Directory Support**
Sync your Boxcryptor user with users of your internal directory.
- **Policies and Centralized Management**
Define policies and manage your users and devices.
- **Encrypt Network Shares**
Protect your in-house network storage by adding it to Boxcryptor.

2. Create and Enable your Boxcryptor Company Package

2.1 Create a Boxcryptor Account

Boxcryptor requires a Boxcryptor account. You can sign up following this [link](#). You can change your email address afterwards.

After you have successfully created your account, you will receive an email with a verification link. Click on this link once to verify that this is a valid email address. You have to verify your account within seven days.

Using the Boxcryptor Web App to create an account requires you to sign in with our client software in order to change your temporary password and to generate your encryption keys.

Please go to the Boxcryptor [download page](#) to download the client software. Available for Windows and Mac OS X.

After the first sign in, Boxcryptor automatically generates your encryption keys.

2.2 Start the Company Package Trial

You can do this on the “My Account” tab within the Boxcryptor Web App.

Please fill in all information and start your trial.

Congratulations. You successfully activated your Boxcryptor Company Package Trial.

Do you have any question regarding your Boxcryptor license or product key? Please contact sales@boxcryptor.com.

3. Setting up the Boxcryptor Company Package

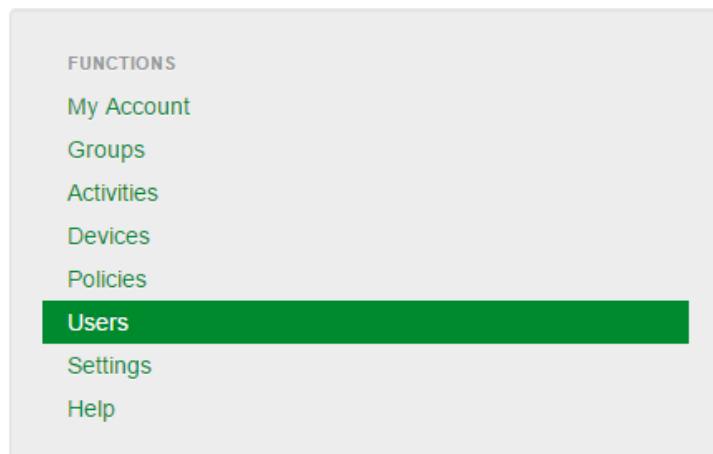
After successfully activating your Boxcryptor Company Package, you can start setting up Boxcryptor for your company or team. The Boxcryptor Company Package adds various useful features for teamwork.

3.1 Add Users

One of the most important features and advantages of using the cloud is collaboration. Boxcryptor was designed to satisfy this need and enables you to share permissions while working with encrypted files. In order to share permissions and manage groups, every user needs a Boxcryptor account.

As a Boxcryptor company admin, only you can add users.

Go to the “Users” tab.



You will see your currently existing users. As you have not added any users yet, you should only see your own admin account.

You are using 1 out of 9,999 possible users. If you need more click here to upgrade to another package.			
Firstname	Lastname	Email	
Boxcryptor	Manual	boxcryptor.manual@secomba.com	Edit · Remove · Revoke admin rights

3.1.1 Add Users via Email

The easiest way to add users is to register them via email.
Just enter the user's email address and click "Add User".

testuser1@secomba.com	Add User
-----------------------	----------

It is also possible to add more than one user at a time by simply separating the email addresses with a comma.

testuser2@secomba.com, testuser3@secomba.com, testuser4@secomba.com,	Add User
--	----------

The users will receive an email with a verification link and a temporary password.
If a user doesn't verify his account within seven days, the account will be disabled until the user verifies his account.

Firstname	Lastname	Email	
Boxcryptor	Boxcryptor	testuser1@secomba.com	Edit · Remove · Grant admin rights
Boxcryptor	Boxcryptor	testuser2@secomba.com	Edit · Remove · Grant admin rights
Boxcryptor	Boxcryptor	testuser4@secomba.com	Edit · Remove · Grant admin rights
Boxcryptor	Boxcryptor	testuser3@secomba.com	Edit · Remove · Grant admin rights
Boxcryptor	Manual	boxcryptor.manual@secomba.com	Edit · Remove · Revoke admin rights

3.1.2 Add Users via Active Directory

If you manage your users in your organization with an Active Directory or LDAP you can easily import these users to Boxcryptor. This requires an Active Directory or LDAP server which can be reached from our servers and the read access to your directory.

To configure Boxcryptor with your user directory, click on the button "Setup LDAP".

User Directory

You can integrate Boxcryptor with third party user directories like Microsoft Business account to keep your users in sync.

Setup LDAP

Setup Dropbox for Business

Now you can configure your access to your user directory.

User Directory

Server Address	<input type="text" value="ldap://server.company.com:386/"/>
User Base	<input type="text" value="dc=company,dc=com"/>
User for authentication	<input type="text" value="cn=Administrator,cn=Users,dc=company,dc=com"/>
Password for authentication	<input type="password" value="Password"/>
Search String	<input type="text" value="(objectClass=user)"/>
Search Base	<input type="text" value="cn=users"/>
Field of Firstname	<input type="text" value="givenname"/>
Field of Lastname	<input type="text" value="sn"/>
Field of Email	<input type="text" value="userprincipalname"/>
Deletion Procedure	<input type="text" value="Delete"/>

Save

Cancel

Most of the settings should be clear to an Active Directory / LDAP administrator.

The last field “Deletion Procedure” has three options which concern cases where a user is part of your Boxcryptor organization but not in your directory anymore:

- **Delete:** The user will be deleted from Boxcryptor and will not have access to any encrypted file or the Boxcryptor apps
- **Remove:** The user will be deleted from your Boxcryptor organization. He will be a free user and can still access his personal files. All organization policies are not applied to the user anymore
- **Disable:** The account will be disabled (so he will not count to your subscription limit). The user will not be able to login, but you can easily re-activate this account if you need it at a later point.

If you have configured and saved your connection, the screen will look like this:

The screenshot shows the 'User Directory' configuration page in Boxcryptor. It features a form with the following fields and values:

- Server Address:** ldap://elvis.secomba.com:389/
- User Base:** dc=secomba,dc=com
- User for authentication:** cn=Administrator,cn=Users,dc=secomba,dc=com
- Password for authentication:** (masked with dots)
- Search String:** (objectClass=user)
- Search Base:** cn=users
- Field of Firstname:** givenname
- Field of Lastname:** sn
- Field of Email:** userprincipalname
- Deletion Procedure:** Delete (selected from a dropdown menu)

At the bottom of the form are three buttons: a green 'Save' button, a red 'Delete Connection' button, and a grey 'Cancel' button.

Below the form is the 'Import Users' section, which includes a 'Dry run' checkbox (checked) with the text 'If checked, you will see what happens but no user is added or deleted!'. A green 'Start Import' button is located at the bottom of this section.

We recommend to set the “Dry run” option, to see what would happen if proceeded. You will see a result similar to this one:

Import Users

Dry run ☒ If checked, you will see what happens but no user is added or deleted!

Start Import

Because you did a dry run the following only shows you what would happen, if you start to import your users from your directory.

The following users would have been imported to your Boxcryptor company:

Firstname	Lastname	Email
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

The following users would have been invited to join your Boxcryptor company. This would happen because they already own a Boxcryptor account.

Firstname	Lastname	Email
[REDACTED]	[REDACTED]	[REDACTED]

The following users will not be added to your Boxcryptor company, because they belong to another Boxcryptor company. Please contact the administrator of their company to remove them from the company and start the import process again.

Firstname	Lastname	Email
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

The following users would have been deleted.

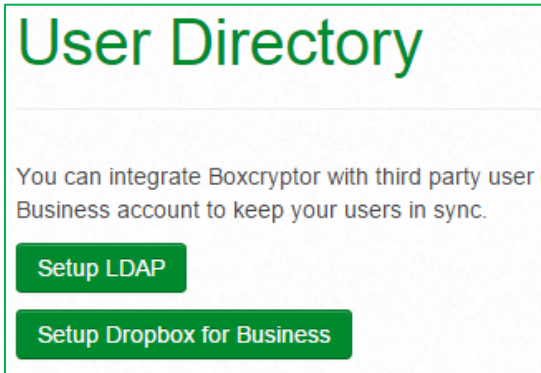
Firstname	Lastname	Email
[REDACTED]	[REDACTED]	[REDACTED]

If you think everything is fine, you can remove the “Dry run” checkbox and the changes will be written to the database.

If you need to resync your users at a later time, simply start the import process again.

3.1.3 Add Users Using Dropbox Business

It is also possible to add users already integrated in your company's Dropbox Business. Simply click on the button "Setup Dropbox Business" and you will be able to connect to your Dropbox Business account:

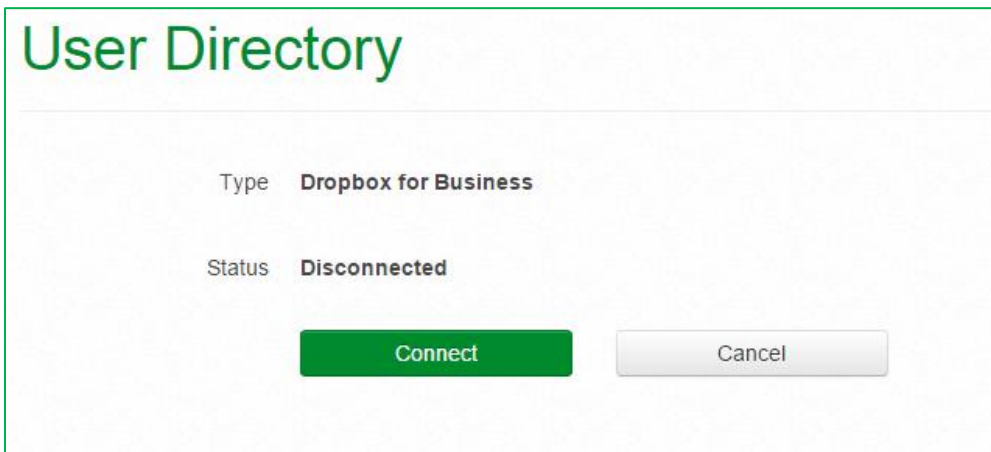


User Directory

You can integrate Boxcryptor with third party user directories. Select a Business account to keep your users in sync.

[Setup LDAP](#)

[Setup Dropbox for Business](#)

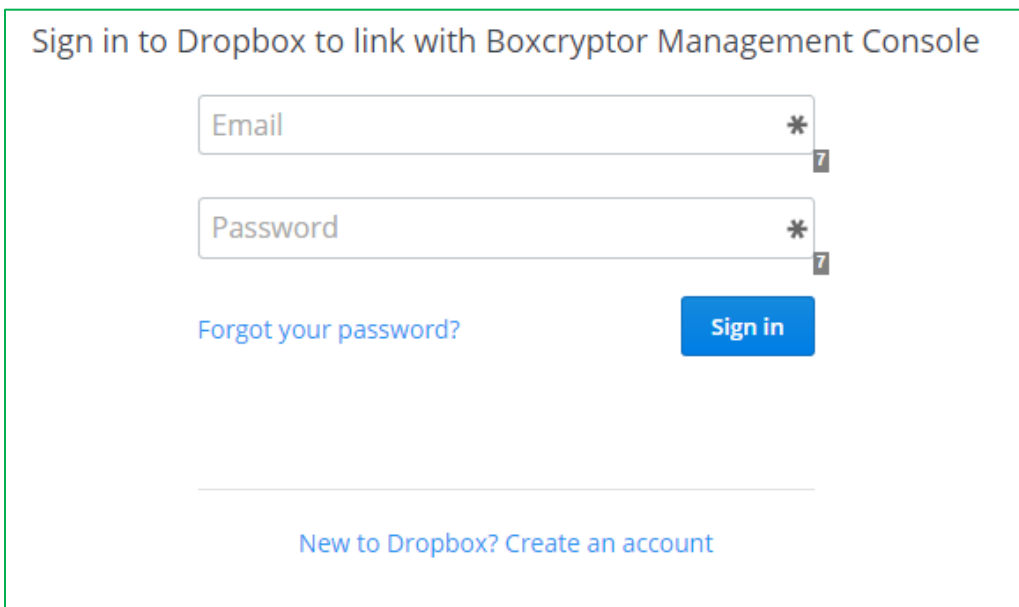


User Directory

Type **Dropbox for Business**

Status **Disconnected**

[Connect](#) [Cancel](#)



Sign in to Dropbox to link with Boxcryptor Management Console

Email *

Password *

[Forgot your password?](#) [Sign in](#)

[New to Dropbox? Create an account](#)

Please use your Dropbox Business login credentials. After you signed in to link with Boxcryptor, you will be redirected back to the Boxcryptor Web App.

The screenshot shows the 'User Directory' section of the Boxcryptor web app. It features a form with the following elements:

- Type:** A dropdown menu set to 'Dropbox for Business'.
- Status:** A dropdown menu set to 'Connected as Secomba'.
- Deletion Procedure:** A dropdown menu set to 'Disable'.
- Buttons:** Three buttons are located below the form: a green 'Save' button, a red 'Disconnect' button, and a grey 'Cancel' button.

Below the 'User Directory' section is the 'Import Users' section, which includes:

- Dry run:** A checkbox that is checked, followed by the text 'If checked, you will see what happens but no user is added or deleted!'.
- Start Import:** A green button.

The last field “Deletion Procedure” has three options which concern cases where a user is part of your Boxcryptor organization, but not in your directory anymore:

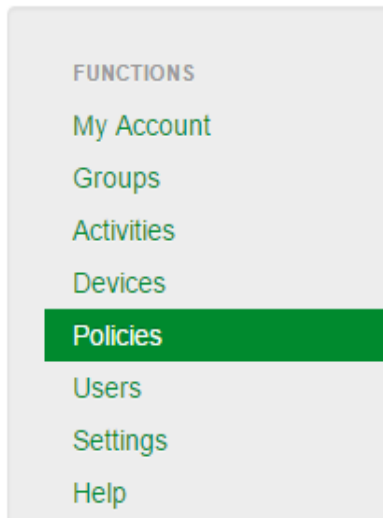
- **Delete:** The user will be deleted from Boxcryptor and will not have access to any encrypted file or the Boxcryptor apps
- **Remove:** The user will be deleted from your Boxcryptor organization. He will be a free user and can still access his personal files. All organization policies are not applied to the user anymore
- **Disable:** The account will be disabled (so he will not count to your subscription limit). The user will not be able to login, but you can easily re-activate this account if you need it at a later point.

We recommend to set the “Dry run” option, to see what would happen if you import your users.

If you think everything is fine, you can remove the “Dry run” checkbox and the changes will be written to the database.

If you need to resync your users at a later time, simply start the import process again.

3.2 Set Policies



Using the Boxcryptor Company Package, you can define a set of policies (rules) which apply to all users and groups belonging to your company.

You can add or edit these policies by navigating into the “Policies” tab. Here you have an overview of all policies that apply to your company. You can see which policies are enabled, which users are included / excluded and the value of the policy (if available).

3.2.1 Policy Overview

Policy Name	Description	Example Value (if available)
Disable Remember Password	A user cannot use the remember password feature and has to enter his password every time Boxcryptor starts.	
Disable Creation of Groups	A user cannot create new groups.	
Disallow Filename Encryption	Filename encryption is forbidden and cannot be enabled by a user.	
Disallow to Join Groups	A user cannot join groups.	
Restrict sign in to specific IP addresses	A user can only login to this account from IP addresses which match the regular expression specified in the value field.	<code>^123\.123\.123\.([0-9][0-9]) 200)\$</code>
Restrict sign in to specific countries	A user can use Boxcryptor only in specific countries. If a user is connected from any other country, he will be signed out and won't be able to sign in. Enter the two-letter country codes (ISO 3166-1 alpha-2) of allowed countries separated by white space in the Value field. E.g. “US CA GB”, to allow	US CA GB

	access for users from within the United States, Canada or United Kingdom. If you don't want to restrict signed in users, take a look at the Restrict sign in from specific countries policy. Tip: We recommend to exclude your own user from the policy while you are setting up the policy and testing it.	
Restrict use to specific countries	A user can use Boxcryptor only in specific countries. If a user is connected from any other country, he will be signed out and won't be able to sign in. Enter the two-letter country codes (ISO 3166-1 alpha-2) of allowed countries separated by white space in the Value field. E.g. "US CA GB", to allow access for users from within the United States, Canada or United Kingdom. If you don't want to restrict signed in users, take a look at the "Restrict sign in from specific countries" policy. Tip: We recommend to exclude your own user from the policy while you are setting up the policy and testing it.	US CA GB
Restrict use to specific IP addresses	A user can use Boxcryptor only from an IP address which matches the regular expression specified in the value field. If a user is connected from any other IP address, he will be signed out and won't be able to sign in. If you don't want to restrict signed in users, take a look at the "Restrict sign in from specific IP countries" policy. Tip: We recommend to exclude your own user from the policy while you are setting up the policy and testing it.	
Master Key	The password key of a user is additionally encrypted with the master key. This allows the company administrator to access all encrypted files of the company members. You have to generate the master key in Boxcryptor for Windows and paste it into the value field.	
Maximum Number of Devices	A user can only be connected to a maximum number of devices at the same time. Please enter the maximum number of devices in the value field.	5
Maximum Number of Root Folders	A user can only have a maximum number of locations (on Windows and Mac OS X) or providers (on Android and iOS) configured at the same time.	2
Minimum Password length	New passwords must have a minimum number of characters. Please enter the minimum number of characters in the value field.	12
Require Filename Encryption	Filename encryption is obligatory and cannot be disabled. IMPORTANT: This policy is not yet implemented on all clients.	

Disable Auditing	Do not store any auditing information. This only applies to new auditing data - existing auditing data will not be deleted.	
Disallow Account Reset	Disallow users to reset their account.	
Disallow Key Export	Disallow your users from exporting their account data.	
Maximum Number of Devices	A user can only be connected to a maximum number of devices at the same time. Please enter the maximum number of devices in the value field.	4
Disallow creation of groups	A user may not create any new group.	
Require two-factor authentication using Duo	Boxcryptor supports two-factor authentication using Duo (https://duo.com/). A user is forced to approve his sign in with a second factor, e.g. his mobile device.	

3.2.2 Add Policy

You can easily add any policy by clicking on the “Add” button within the policies tab.

Add policy

Basic Settings

Policy

Disable remember password ▼

Description

Value

Advanced Settings

Save

Cancel

Please select the policy you want to add and (if needed) provide a value.

If you want to include / exclude specific users you can do so using the advanced settings.

Advanced Settings

Enabled ☒

Applies to all users ☒

Included users

Selected Users

Available Users

Boxcryptor Bcryptor (testuser1@se
Boxcryptor Bcryptor (testuser2@se
Boxcryptor Bcryptor (testuser4@se
Boxcryptor Bcryptor (testuser3@se
Boxcryptor Manual (boxcryptor.manua

This list is used if the policy does not apply to all users.

Excluded users

Selected Users

Available Users

Boxcryptor Bcryptor (testuser1@se
Boxcryptor Bcryptor (testuser2@se
Boxcryptor Bcryptor (testuser4@se
Boxcryptor Bcryptor (testuser3@se
Boxcryptor Manual (boxcryptor.manua

This list is used if the policy applies to all users.

Notes

Save

Cancel

Please save your changes. After you saved the changes, you can always edit or disable the new policy.

Policies

+ Add Policy

▼ Expand all ▲ Collapse all

Disable remember password

Enabled: **true**

Applies to all users: **true**

Edit

Delete

3.3 Create a Master Key

The Master Key is one of the Boxcryptor features we offer for companies with our Company Package. If enabled, the Master Key gives you the power to decrypt every file which is accessible by users of your company or organization - without having to know your user's passwords. With the Master Key, you are protected against the loss of access to your property (your files) even in complicated situations (e.g. when a user forgets his password or leaves the company).

To create a Master Key you need Boxcryptor for Windows. (see: [4. Set up Boxcryptor on a Windows Machine](#)).

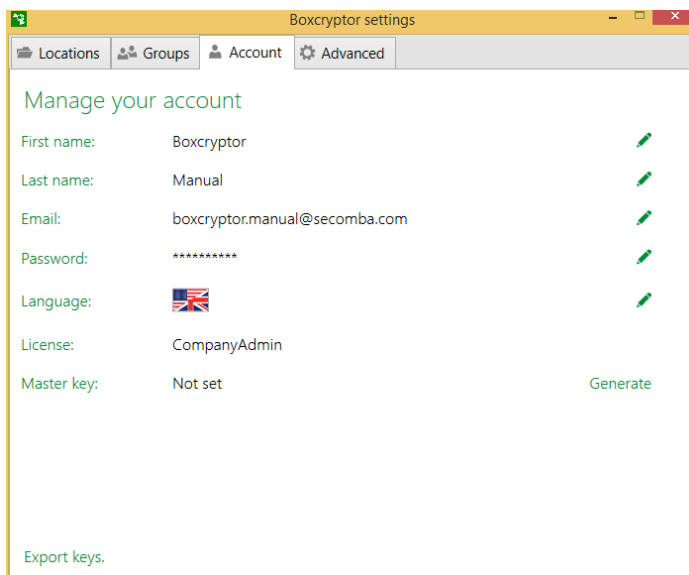
Creating a Master Key is divided into two steps:

1. Generate the key on your local machine using Boxcryptor for Windows
2. Set the policy "Master Key" on the Boxcryptor Web Interface

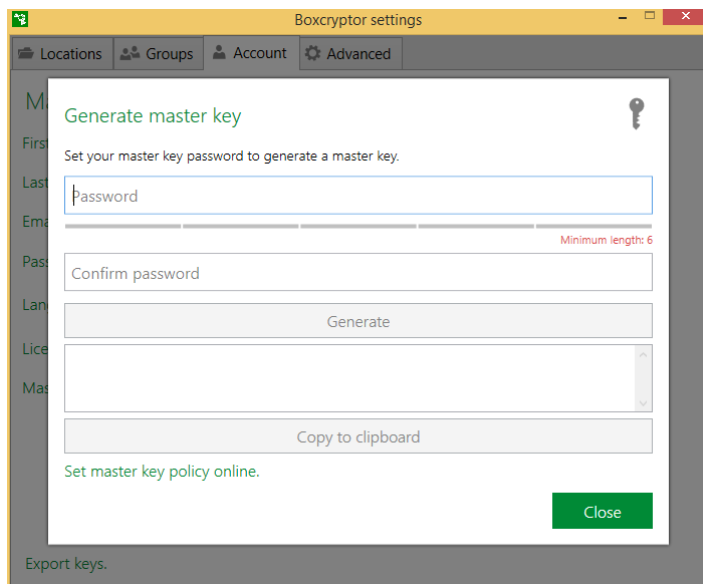
Please note: Dividing this procedure into two steps is necessary due to Boxcryptor's zero-knowledge policy. The key generation takes place on your local machine and your password never leaves your computer.

3.3.1 Generate Key

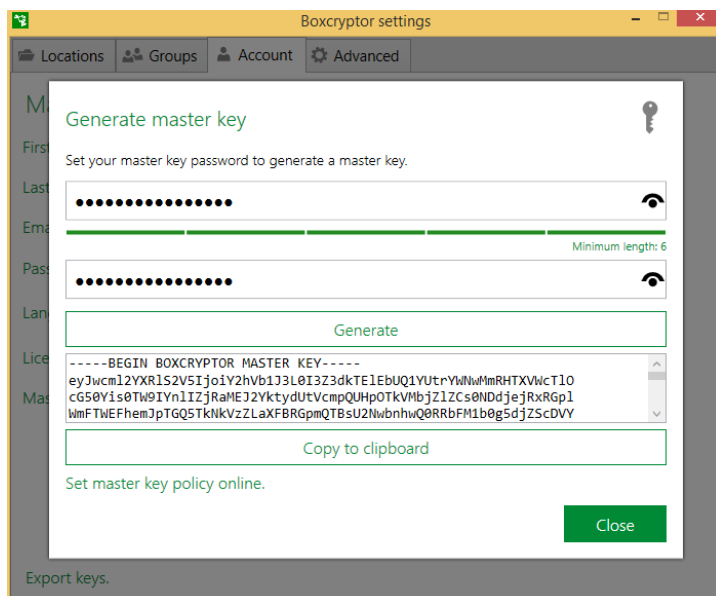
To generate a Master Key, open "Settings", select the "Account" tab and click on "Generate".



Boxcryptor will then ask you to enter a "second" password, which is going to become the company's Master Key password (this one is not your personal administrator password).



Please keep in mind: The company's Master Key password never leaves your computer, which means that we cannot restore it. Please keep a saved copy for the company. If you forget this password, you will lose access to the Master Key. Once you entered the password click on "Generate".



Boxcryptor will now generate your company's Master Key and encrypt it with the entered password. When finished, your Master Key will be displayed in the corresponding box. Copy this Master Key to your clipboard.

3.3.2 Set the Master Key Policy

Go to the Boxcryptor Web Interface and navigate to the “Policies” tab. Click on the “Add” button and choose the Master Key policy. Paste the Master Key into the value box. Click save and the Master Key policy is enabled.

The screenshot shows the 'Basic Settings' section of the Boxcryptor web interface. The 'Policy' dropdown is set to 'Master key'. The 'Description' field contains text explaining that the user's password key is encrypted with the master key, granting administrators access to all encrypted files. The 'Value' field contains a long alphanumeric string representing the master key, starting with 'eXg5K2dkeUF1bkJhVWp2RUp1L3NoWSthd1dkT2J5ZS9DZGhZRIZhQ1prZUpJdn' and ending with '-----END BOXCRIPTOR MASTER KEY-----'. Below the settings are 'Save' and 'Cancel' buttons.

Basic Settings

Policy: Master key

Description: The password key of a user is additionally encrypted with the master key and stored. This grants the company administrator access to the private key of a user and thus all encrypted files to which the user has access. You have to generate the master key in Boxcryptor for Windows or Boxcryptor for Mac and paste it into the "Value" field.

Value: eXg5K2dkeUF1bkJhVWp2RUp1L3NoWSthd1dkT2J5ZS9DZGhZRIZhQ1prZUpJdn
b0c2Q2UvYXBzS283ZW1pZEphbiB0S00xNGQzckFzSEVrZjAxQmdlTy9aM044PSI
ImtkZkl0ZXJhdGlvbnMiOjEwMDAwMCwic2FsdCI6Ing0cncyRm14bndSRnhnTHZX
TTlyZFVpZ2o5ODE3bDRYIn0=
-----END BOXCRIPTOR MASTER KEY-----

Advanced Settings

Save Cancel

To apply the Master Key, each member of the company will be asked to save a new password the next time they log in. That also applies to the administrator who created the Master Key.

The screenshot shows a 'Boxcryptor' dialog box titled 'Enter password'. It includes a warning message: 'Warning: The master key is active. This means that your company can decrypt your encrypted files at any time.' Below the warning, it says 'Please enter your current password.' and provides a text input field. An 'OK' button is at the bottom right.

Boxcryptor

Enter password

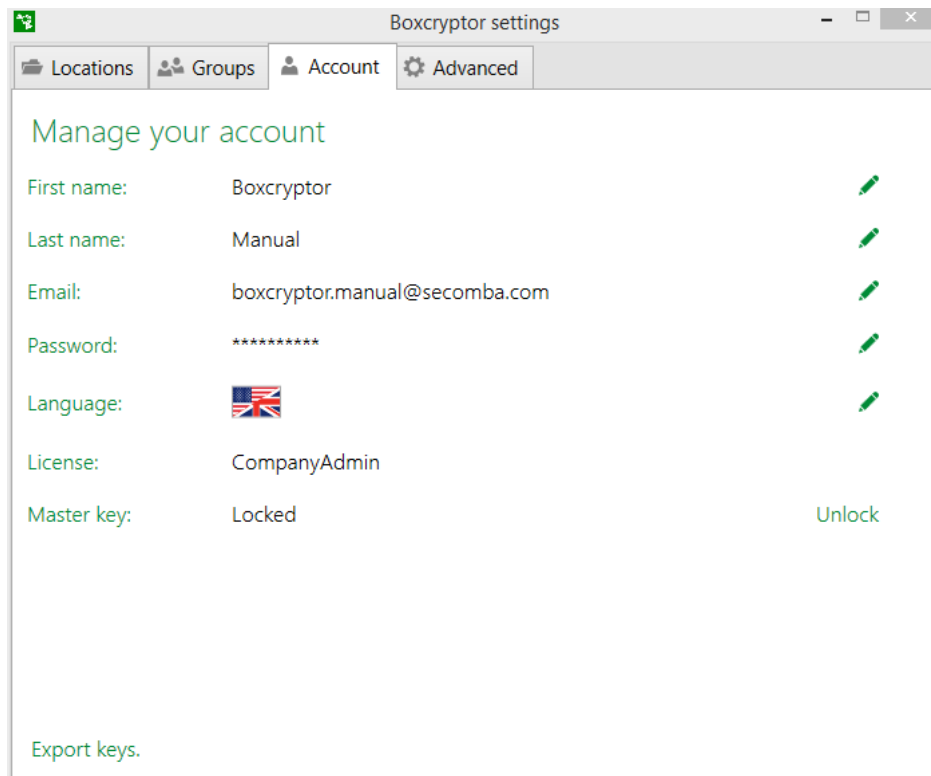
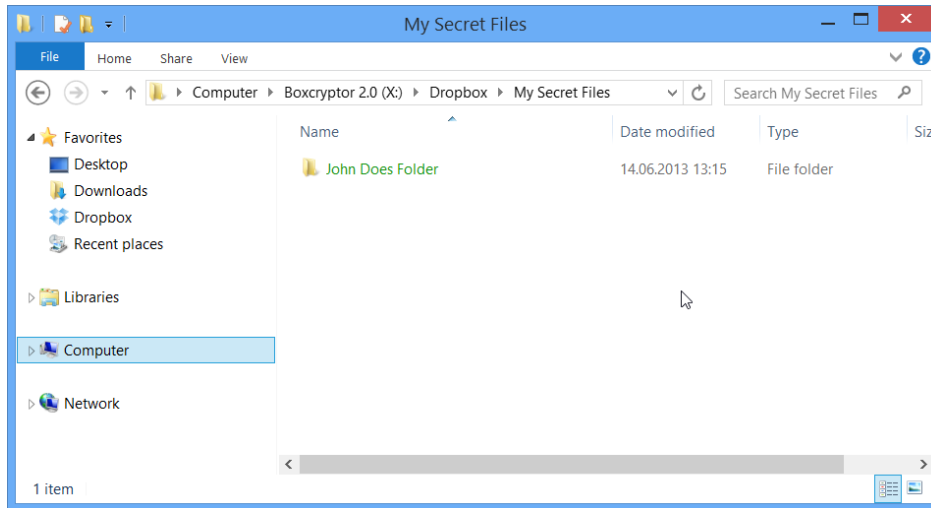
Warning: The master key is active. This means that your company can decrypt your encrypted files at any time.

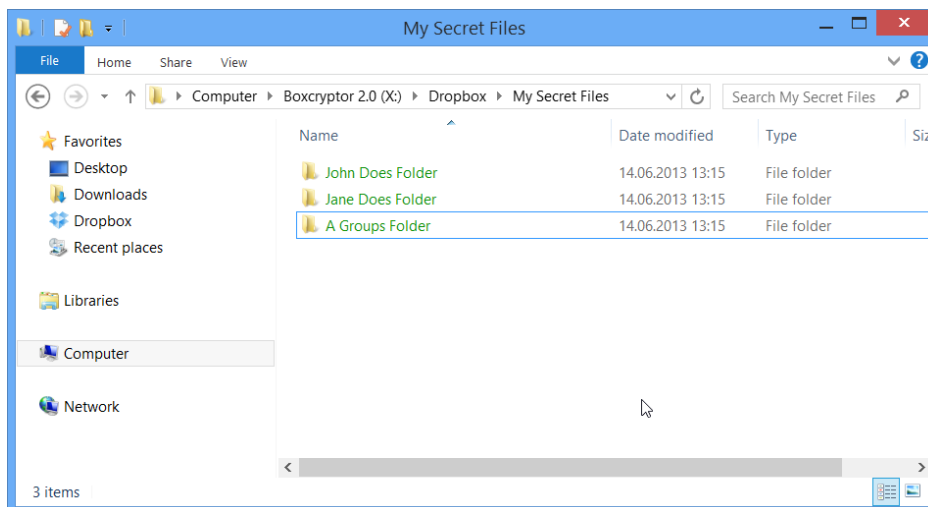
Please enter your current password.

OK

3.3.3 How to Unlock the Master Key

As default, your administrator account is the same as any regular user account. You can only access your own files (or files that are shared with you). When using the Master Key you can see all files and folders of all users in your company. You can easily unlock the Master Key on the account page in “Settings” by entering the Master Key password. After this you will see all files for your company.





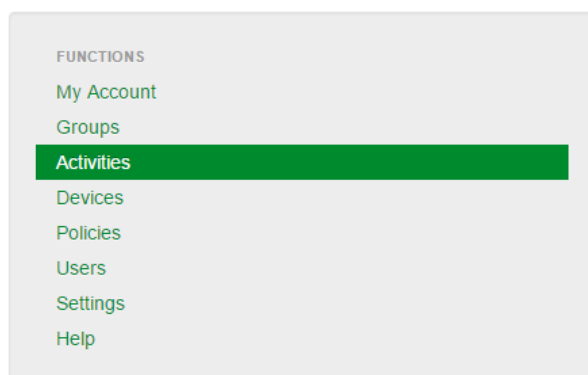
4. Track User Activities

With the latest update we added the possibility to track user activities. This toolset answers the questions around user activities by monitoring, logging and recording events related to accounts, devices and administration.

Types of tracked events:

- Account related
- Device related
- Group related
- Policy related

Navigate into the Activity Tab to start observing the timeline.



You now have the possibility to set a specific period, filter for a specific user and set the maximum activities displayed on one page.

Activity











From:

To:

User:

Hit count:

Change

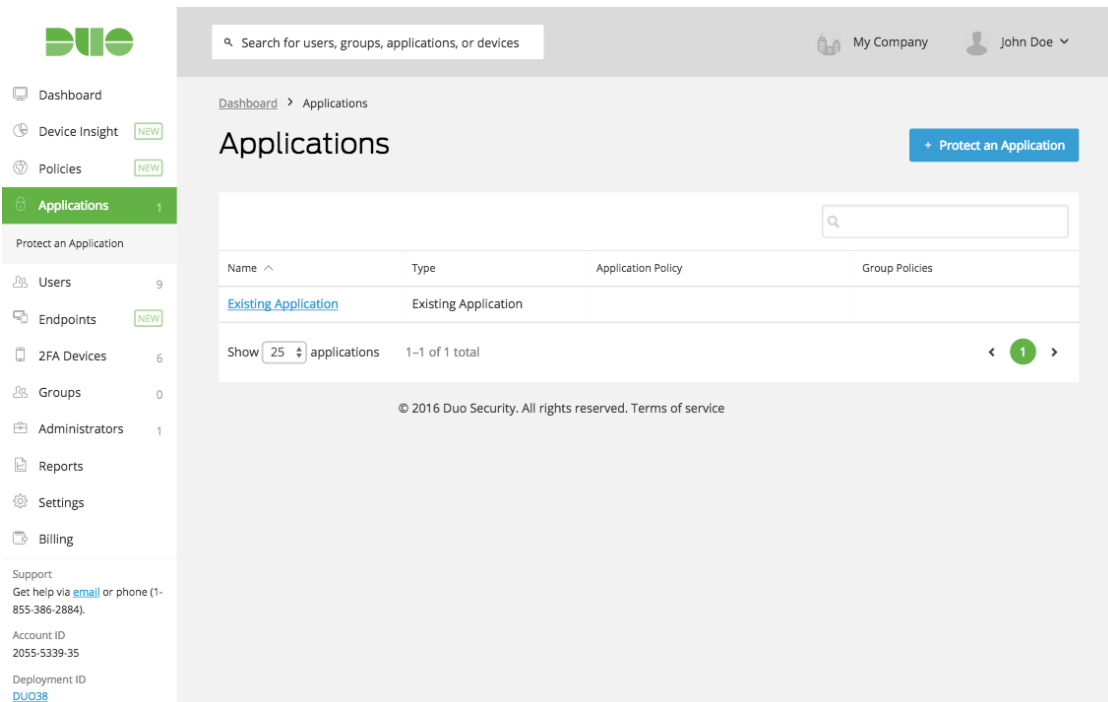
Date / Time	Activity	Description	Country
2015-09-30 / 15:13:35	Password Changed	Ellen Adams changed her password.	 CN
2015-09-29 / 05:01:18	Sign In Disallowed	Ellen Adams has been disallowed to sign in from an unauthorized IP address.	 IN
2015-09-27 / 12:05:01	Sign In Failed	Ellen Adams failed to sign in.	 ZA
2015-09-27 / 12:03:45	Sign in Failed	Ellen Adams failed to sign in.	 AT
2015-09-25 / 11:11:11	Sign In Disallowed	Ellen Adams has been disallowed to sign in from an unauthorized country.	 US
2015-09-23 / 16:57:06	Member Removed	Austin Ehrhardt removed Ellen Adams from the group "Development".	 CN
2015-09-22 / 09:17:12	Member Added	Austin Ehrhardt added Percy Bowman to the group "Managment".	 GB
2015-09-20 / 15:00:05	Group Deleted	Austin Ehrhardt deleted the group "Development".	 JP
2015-09-17 / 13:11:15	Group Created	Austin Ehrhardt created the group "Development".	 TW
2015-09-17 / 07:13:20	Email Changed	Ellen Adams changed her email address to "ea@contoso.com".	 US

5. Two-Factor Authentication

Boxcryptor supports two-factor authentication with Duo Security. You can learn more about Duo at the official website: <https://duo.com/>

5.1 Setup Duo and Bcryptor

1. Create a Duo security account (you need at least an Enterprise Plan), and sign in.
2. Choose Applications → Protect an Application



The screenshot shows the Duo Security dashboard interface. On the left is a sidebar with navigation links: Dashboard, Device Insight (NEW), Policies (NEW), Applications (1), Protect an Application, Users (9), Endpoints (NEW), 2FA Devices (6), Groups (0), Administrators (1), Reports, Settings, and Billing. Below these are support links and account information. The main content area is titled 'Applications' and includes a search bar, a '+ Protect an Application' button, and a table with one entry: 'Existing Application'. The table has columns for Name, Type, Application Policy, and Group Policies. At the bottom of the table, it says 'Show 25 applications 1-1 of 1 total'. The footer of the dashboard contains the copyright notice '© 2016 Duo Security. All rights reserved. Terms of service'.

Duo

Search for users, groups, applications, or devices

My Company John Doe

Dashboard > Applications

Applications

+ Protect an Application

Name ^	Type	Application Policy	Group Policies
Existing Application	Existing Application		

Show 25 applications 1-1 of 1 total

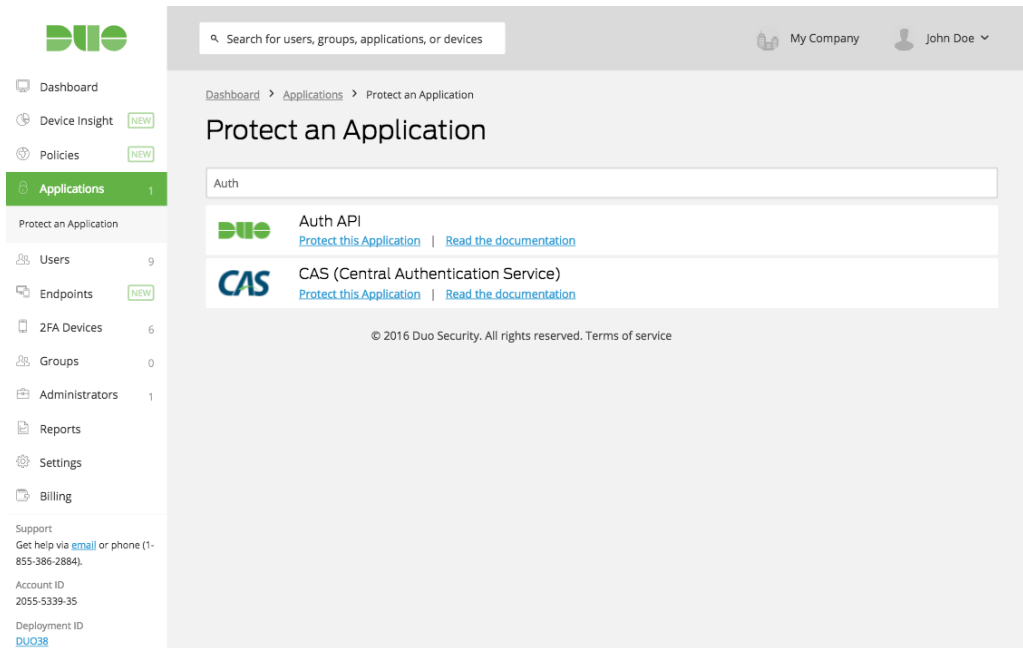
© 2016 Duo Security. All rights reserved. Terms of service

Support
Get help via [email](#) or phone (1-855-386-2884).

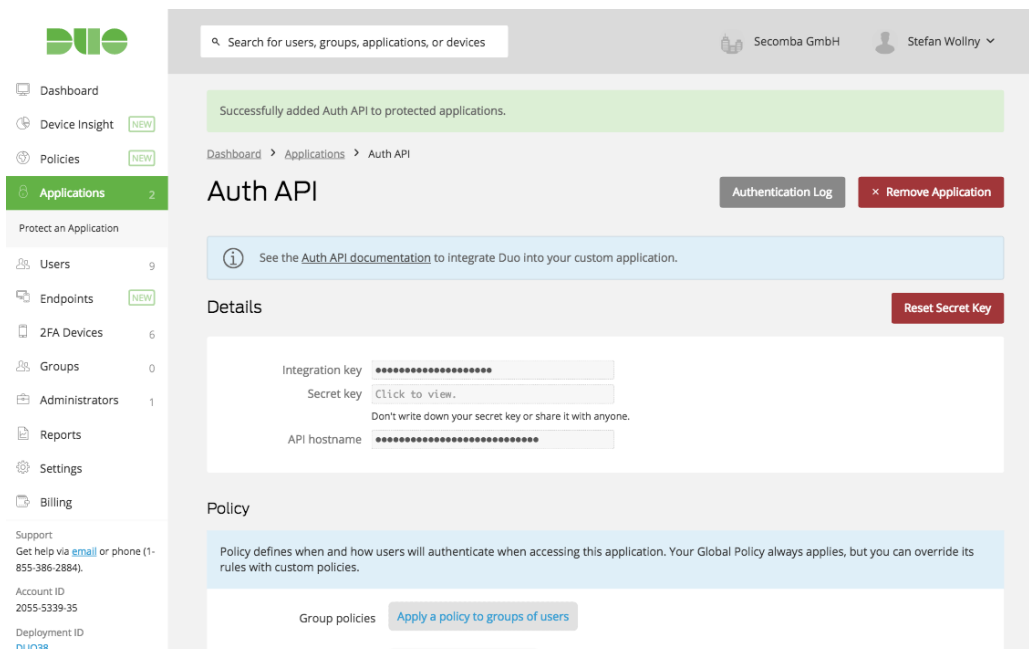
Account ID
2055-5339-35

Deployment ID
[DUQ38](#)

3. Search for Auth API and click on “Protect this Application”



4. Duo will show you a page with details about the Auth API, including the integration key, secret key and the API hostname. Write these down for the setup with Boxcryptor (step 7).



5. (Optional) Scroll down and enable username normalization: 'simple' if your Duo usernames do not match the email addresses of your Boxcryptor users.

Settings

General

Type: Auth API

Name:

Duo Push users will see this when approving transactions.

Username normalization: ☐ None ☒ **Simple**

"DOMAIN\username", "username@example.com", and "username" are treated as the same user.

Controls if usernames should be altered before trying to match them to a user account.

Voice greeting:

Specify the message read to users who use phone callback, followed by authentication instructions.


Notes:

For internal use.

Group access: ☐ Only allow authentication from users in certain groups

When unchecked, all users can authenticate to this application.

6. Sign in to the Boxcryptor web interface and select Policies → "Add Policy".

John Doe Language ▾ ➤ Sign out

FUNCTIONS

- My Account
- Groups
- Activities
- Devices
- Policies**
- Users
- Settings
- Help

Policies

▼ Expand all ▲ Collapse all

▼ Expand all ▲ Collapse all

Download

Windows

Windows Phone

Windows RT

Mac OS X

Android

iOS

7. Select the policy “Require two-factor authentication using Duo”. Enter the Auth API details from Step 4 and save your changes.

The screenshot shows the Boxcryptor web interface. On the left is a sidebar with a 'FUNCTIONS' menu (My Account, Groups, Activities, Devices, Policies, Users, Settings, Help) and a 'Download' section with buttons for Windows, Windows Phone, Windows RT, Mac OS X, Android, and iOS. The main area is titled 'Add policy'. It contains a 'Basic Settings' section with a dropdown for 'Policy' (selected: 'Require two-factor authentication using Duo'), a 'Description' box, and input fields for 'Integration key', 'Secret key', and 'API hostname'. Below this is an 'Advanced Settings' section. At the bottom are 'Save' and 'Cancel' buttons.

Congratulations. You have successfully setup the Boxcryptor two-factor authentication with Duo Security.

The screenshot shows the Boxcryptor web interface after saving the policy. A green notification banner at the top says 'Policy Require two-factor authentication using Duo created'. The main area is titled 'Policies'. It includes an '+ Add Policy' button and 'Expand all' / 'Collapse all' links. A policy card for 'Require two-factor authentication using Duo' is shown, with 'Enabled' and 'Applies to all users' both set to 'true'. It has 'Edit' and 'Delete' buttons. The 'Value' field contains a JSON object:

```
{\"apiHostName\": \"*****\", \"integrationKey\": \"*****\", \"secretKey\": \"*****\"}
```

. 'Expand all' and 'Collapse all' links are also present at the bottom of the card.

Users are enrolled in Duo (see https://duo.com/docs/enrolling_users). Boxcryptor users and Duo users are linked by their email addresses.

6. Whisply Integration

Whisply is a web application, which enables you to send files directly from your browser, protected by state-of-the-art end-to-end encryption using AES-256. After choosing the files you want to send, you connect to Dropbox, Google Drive or Microsoft OneDrive and upload them encrypted.

Whisply is the second encryption solution created by the company behind Boxcryptor, Secomba GmbH, and is integrated since Boxcryptor version 2.3.

Advantages of Whisply

Unlike Boxcryptor, Whisply does not need any local installation. Every user with a modern browser can send and receive files with Whisply.

6.1 Whisply Features

As a user with a company license, you have access to additional Whisply features. You can determine how long a download link should be available. You can also enable the One Time Download option. If enabled, the download can be received only once.

You can choose between three security levels depending on your use case:

- **Link only**

Only individuals who receive the link can download the file.

- **Link & PIN**

Only individuals who receive the 4-digit PIN and the link can download the file.

- **Link & Password**

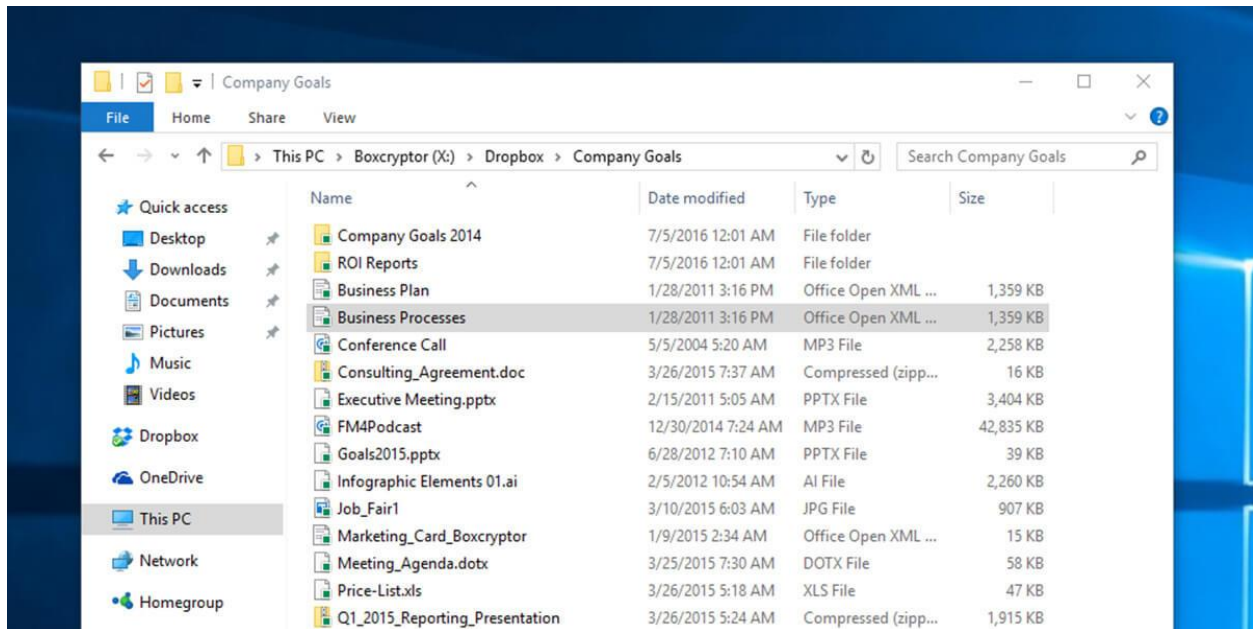
Only individuals who receive the custom password and the link can download the file.

The Whisply integration currently supports Dropbox, OneDrive and Google Drive.

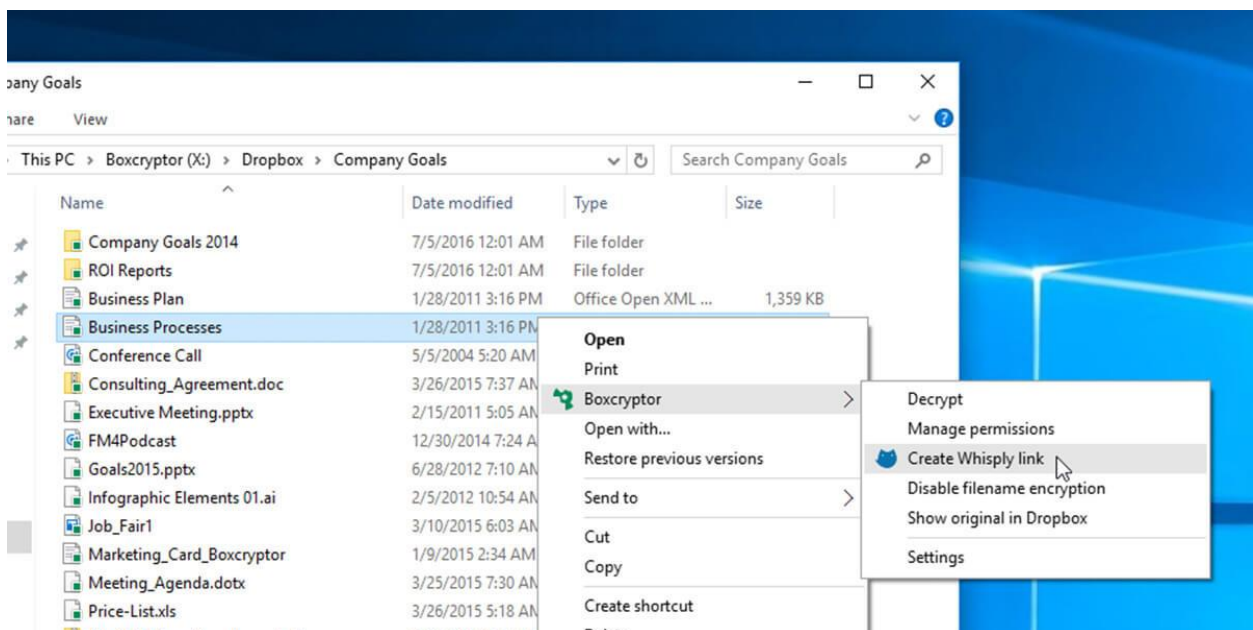
6.2 Send Files with Boxcryptor via Whisply

With Whisply we integrated our second product into Boxcryptor. From now on you can share files to non-Boxcryptor users right from your Boxcryptor drive.

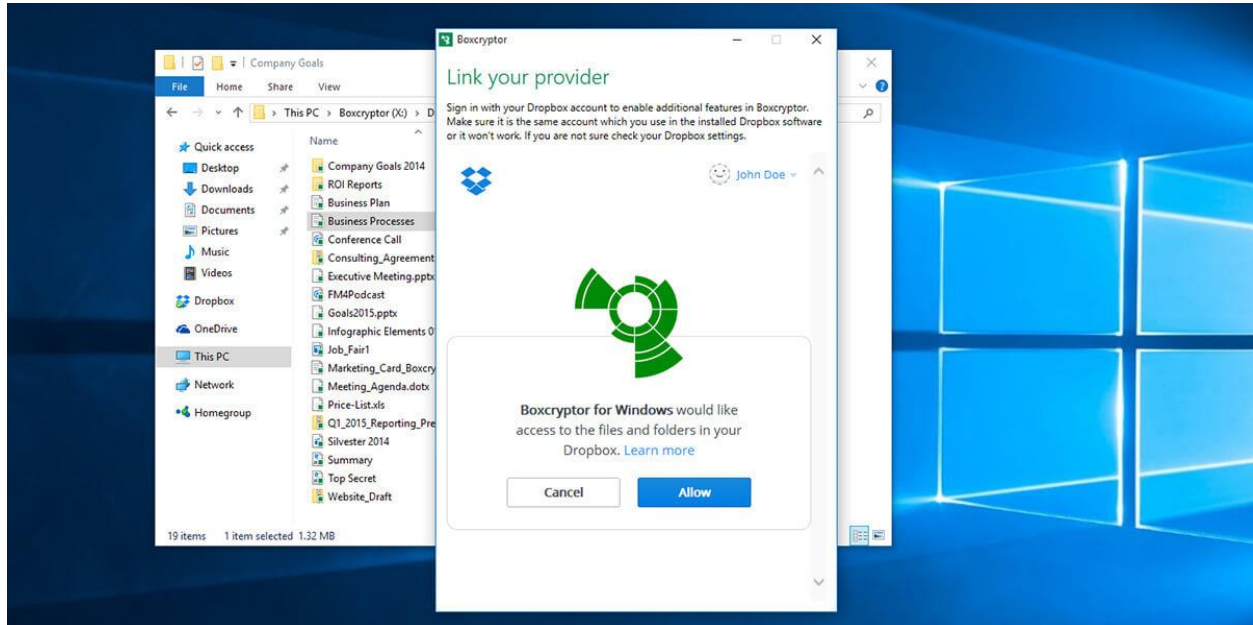
1. Open your Boxcryptor Drive which is located under This PC > Boxcryptor. Browse to the file you want to share via secure Whisply link.



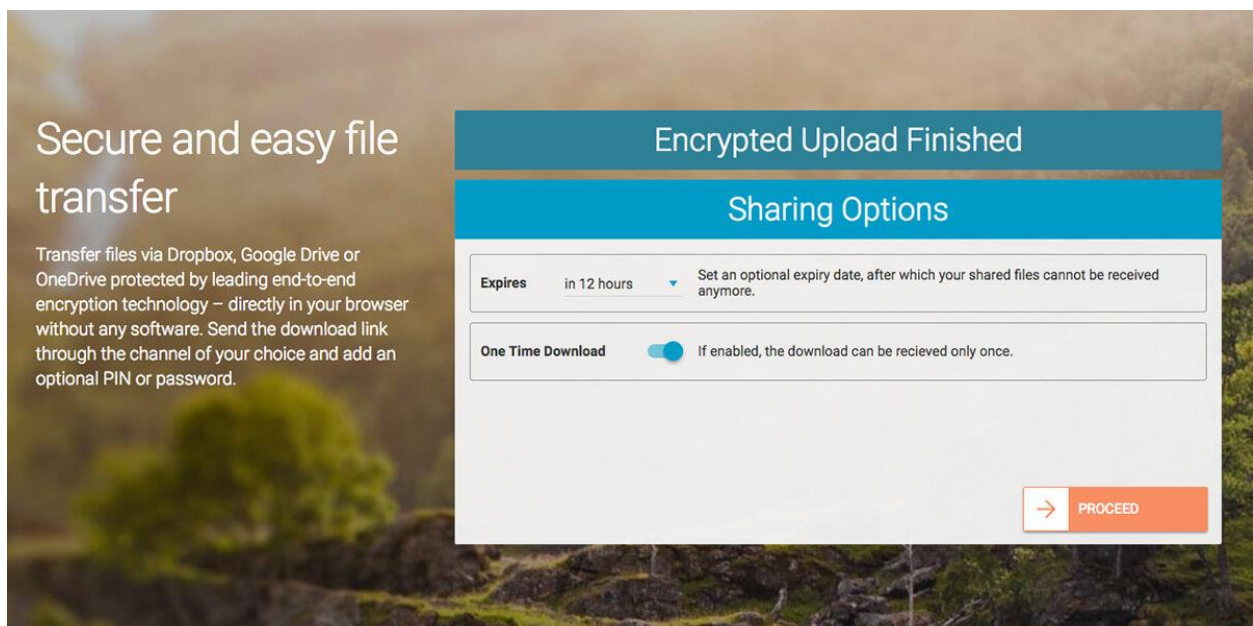
2. Right click on the file to open the context menu. Hover over the entry 'Boxcryptor' to see the available Boxcryptor options and select the option "Create Whisply link".



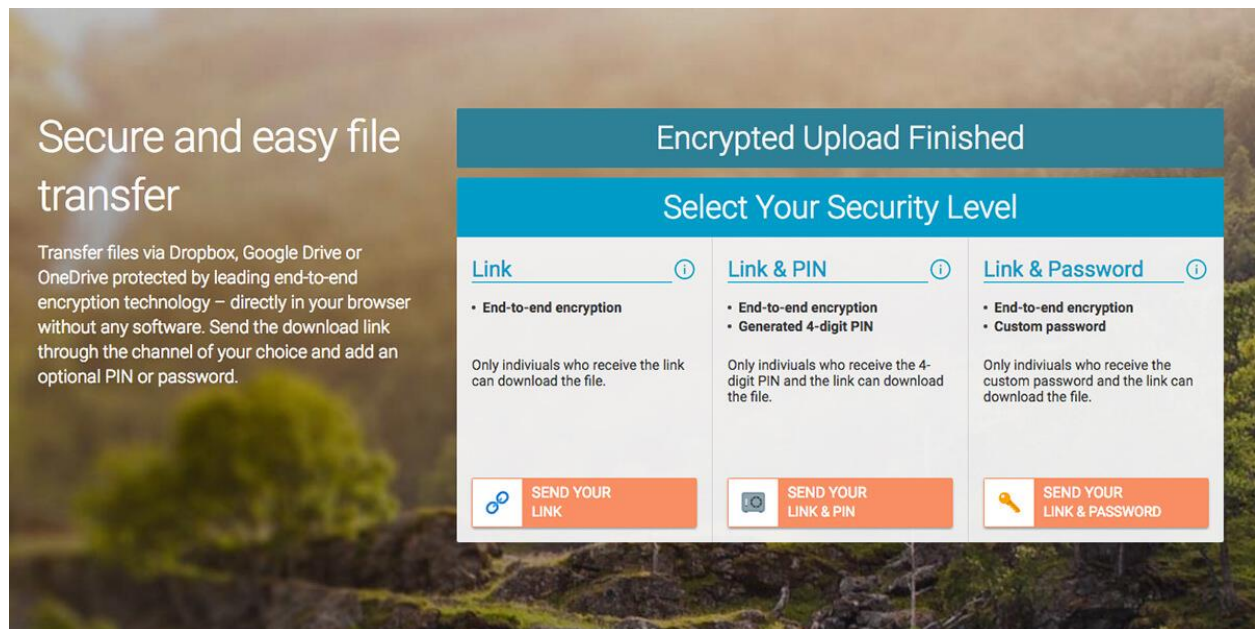
3. You'll be asked to enter the credentials for Dropbox, OneDrive or Google Drive. After that, you need to confirm the connection between Boxcryptor and your cloud storage provider. It is important that you link the exact account which you use with Boxcryptor. Otherwise it won't work.



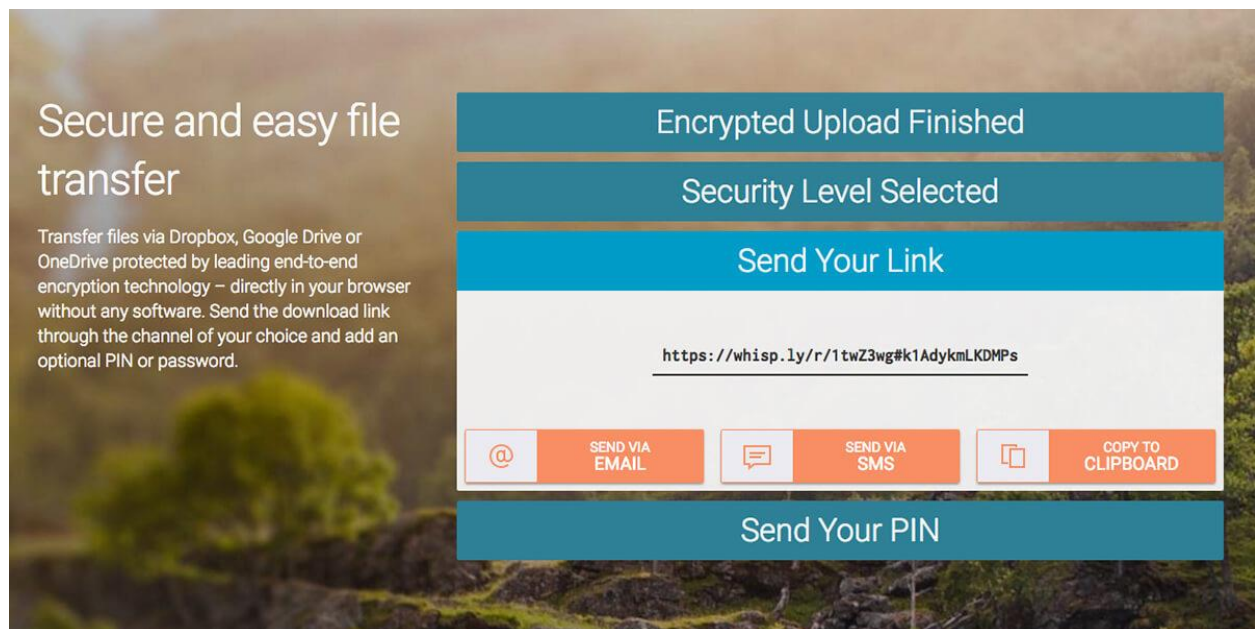
4. Once you successfully connected your cloud storage provider, the browser opens and navigates to our web application Whisply. If you're using Whisply with a Boxcryptor Unlimited Personal or Business license, you can determine your sharing options for the file. You can set a customized expiry date for the download link, or toggle the option that the file can only be downloaded once.



5. In the next step, you can choose if you want to add additional access protection by requiring a randomly generated PIN or a custom password. If you chose Link & Password, you are prompted to set your custom password.



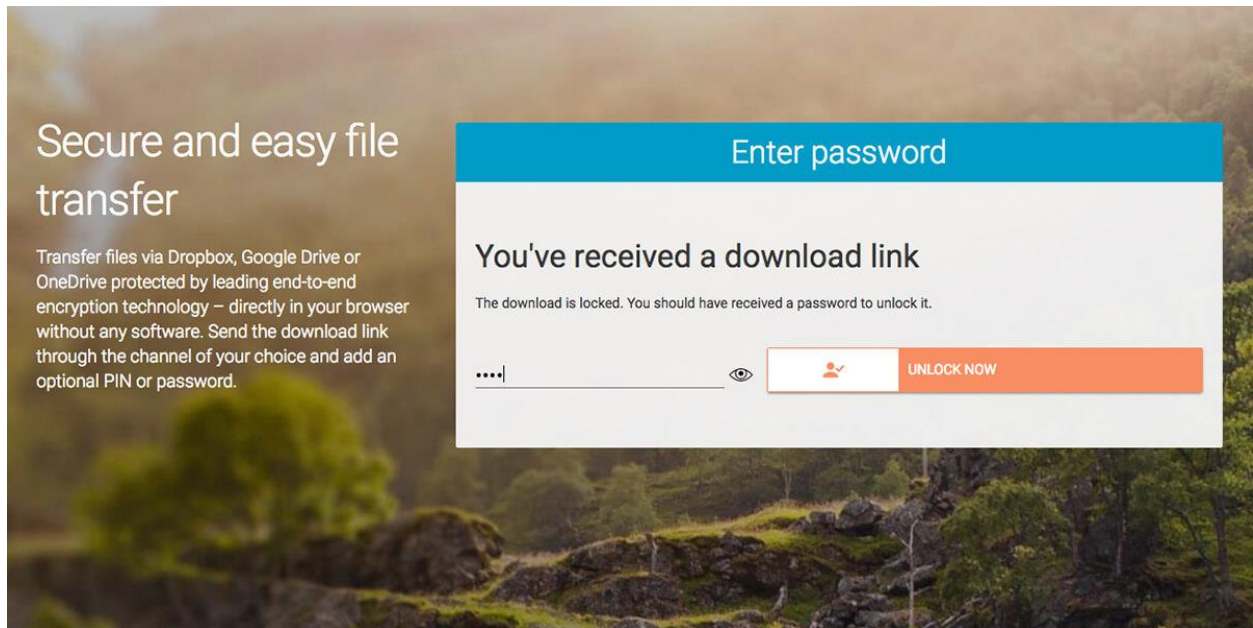
6. Now Whisply shows you the download link of the file you want to share. Depending on the security level you chose in the step before, Whisply displays the random PIN or the custom password in the final step.



Downloading the File

The person who receives the link will be asked to enter the PIN or Password if you have chosen one of these two security levels during the sending process.

The great thing about the Whisply link is: When you edit the sent file, those changes will be updated for the receiver as well. The receiver of the link will have the most recent version of the file when downloading it again later.



6.3 Whisply Use Cases

Boxcryptor is great to ensure privacy and protection within the cloud while maintaining the benefits of cooperation. This implies that every Boxcryptor user has a local version of Boxcryptor installed.

If you want to share files securely and encrypted with potential partners that are not Boxcryptor users or do not use any cloud, Whisply is your solution.

Whisply is great for these use cases in particular but not exclusively:

- Easy correspondence with clients and sharing of sensitive contracts
- Send sensitive files internally or to other companies
- Send bank or payment details
- Share passwords or access keys using the One Time Download feature

Using Whisply is highly recommend when working with sensitive data, not just to ensure privacy but also to generate trust.

7. Support

If you have any unanswered questions or unresolved issues, please feel free to contact our support team anytime by sending an email to support@boxcryptor.com.

Also, please check our helpdesk for any information regarding the Boxcryptor clients:
<https://support.boxcryptor.com>.