

Multi-Factor Authentication Instructions

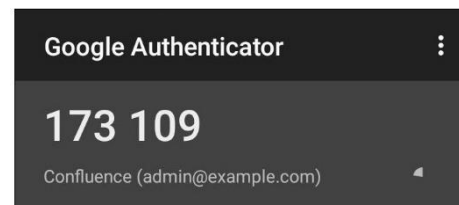
To all users of <http://wiki.d3nw.com/> :

In the next couple of weeks, we will be instituting multi-factor authentication as a new layer of security.

Intro

Please print or save these instructions locally on your laptop or work computer. Once Multi-Factor Authentication is implemented, you will not be able to access the wiki for this information.

After logging in with your username and password, you will be prompted for a second piece of information prior to being fully logged in. Specifically, a six digit code will appear in your authentication app on your phone. Enter this second piece of information to access the wiki.



Supported Browsers

Officially, only Chrome and Firefox are listed as being supported by the Multi-Factor Authentication software. Other browsers may be compatible but results are not guaranteed.

Chrome (no modifications needed)

Firefox – must change setting

In order to use Firefox, FIDO U2F must be enabled. The feature is turned off by default. In order to enable U2F support in Firefox, follow the steps below:

1. Type "about:config" (without quotes) into the Firefox address bar and press **Enter**
2. Search for "u2f"
3. Double-click on **security.webauth.u2f** to enable U2

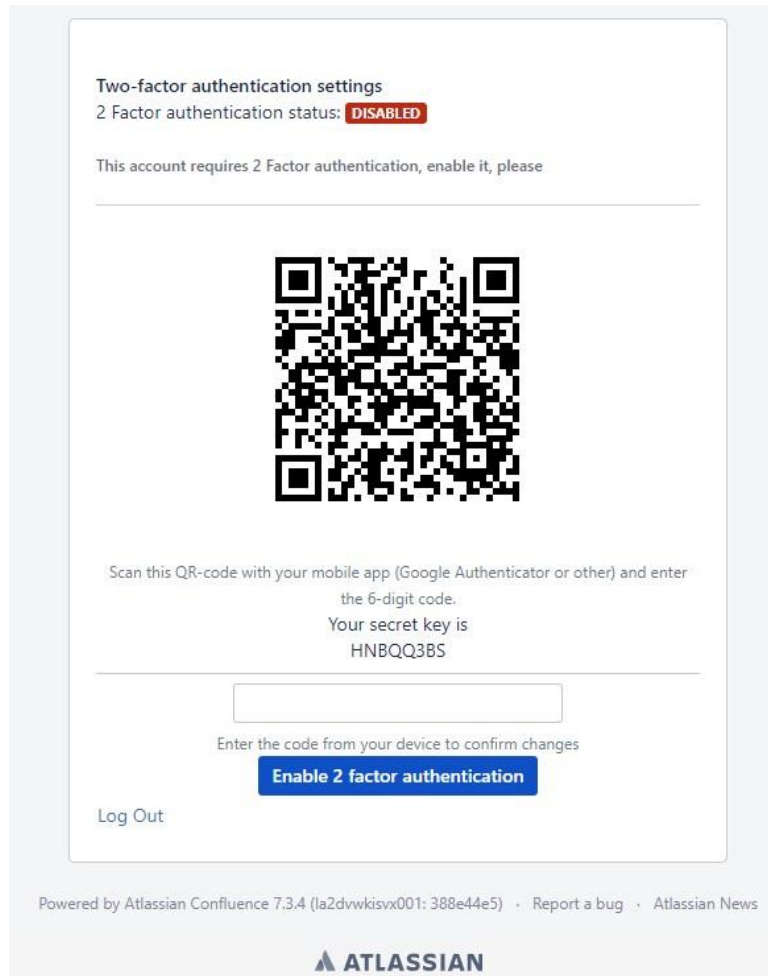
Supported Authentication Applications

Prior to beginning this process, download and install one of the approved authentication apps on your smartphone. Deluxe has chosen the following authentication apps as our standard:

- Google Authenticator
- Microsoft Authenticator

Initial Two-Factor Authentication

After two factor authentication has been enabled for your user group, the following pop-up will be presented after login.



Scan the QR Code with your Google or Microsoft Authentication App and once activated,

1. write down the secret code
2. enter the six digit PIN code in the Confluence or Jira section of the authenticator.

Click "Enable 2 factor authentication" to confirm.

A pop-up will appear with the Backup Codes aka Recovery Codes.

VERY IMPORTANT – Download the recovery codes to a local file on your computer.

1. Should you ever lose your phone or access to your one time secret password, we provide secure backup (recovery) codes that can be used to regain access to your account.
2. Click "Download codes" to download file with codes to your computer .
3. Click "Continue" to finish registration process.

Backup codes

i In case you lose your phone or access to your one-time password, each of these recovery codes can be used once to regain access to your account. Please save them in a secure place, otherwise you will lose access to your account.

AKZQFRVY4RW4KFN6
SXDMHIY4OP4T4KAV
BQ4GJPPKBHXVQQHL
AMUHRZNI5GTXD7WB
22O6ZH64O2QVWJLQ
Z4M4ZCXBJBCTUBOL
KL52GIGTIBENL324
PKB6LKVYCRXSXSFPR
YPTHX7PMIUR3O2V6
OHYJL7RFG7JGQNJ

Download codes Continue

Powered by Atlassian Confluence 7.3.4 (la2dvwkisvx001:388e44e5) · Report a bug · Atlassian News

ATLASSIAN

After registration, you will see a configuration page where you can manage your devices.

Configuration

i **As U2F devices are only supported by a few browsers.**
We require you to set up a two-factor authentication app before a U2F device. Thus you'll always be able to log in, even when you use an unsupported browser.

Two-factor authentication settings

2 Factor authentication status: **ENABLED**

Deactivate 2FA Protection

Increase security of your account by enabling 2FA.

Register U2F Hardware Security Keys

U2F Hardware Security keys can be used as your second factor of authentication instead of a verification code.

Add U2F Device

#	Name	Added	Delete
---	------	-------	--------

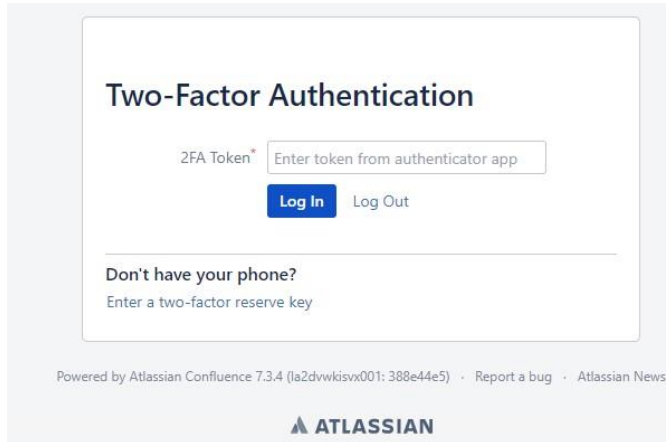
i **2FA is already enabled.**
Additionally you may add U2F devices as an alternative to TOTP, or you may **skip adding U2F devices** at all or add them later.

Powered by Atlassian Confluence 7.3.4 (la2dvwkisvx001:388e44e5) · Report a bug · Atlassian News

ATLASSIAN

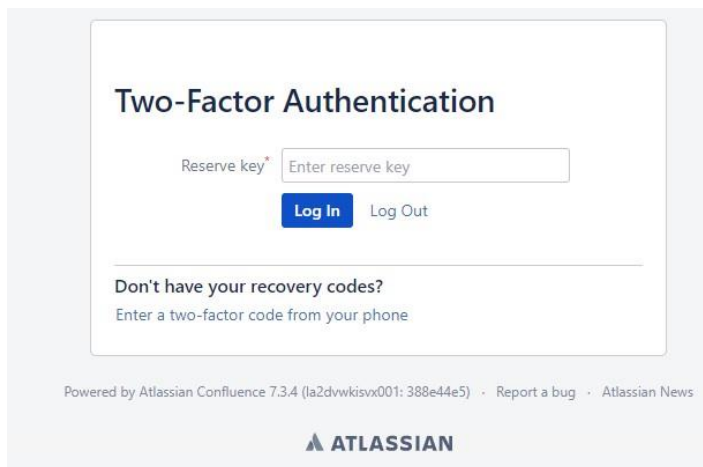
Subsequent Logins

Once enabled, the following pop-up will be presented after login as part of the Two-Factor Authentication.



The screenshot shows a login window titled "Two-Factor Authentication". It features a text input field labeled "2FA Token*" with the placeholder text "Enter token from authenticator app". Below the input field are two buttons: a blue "Log In" button and a "Log Out" link. A horizontal line separates this section from the next. Below the line, there is a section titled "Don't have your phone?" with the text "Enter a two-factor reserve key". At the bottom of the window, there is a footer that reads "Powered by Atlassian Confluence 7.3.4 (la2dvwkivx001: 388e44e5) · Report a bug · Atlassian News" and the Atlassian logo.

If you do not have your authentication app available, one of the recovery codes can be used for access instead.



The screenshot shows a login window titled "Two-Factor Authentication". It features a text input field labeled "Reserve key*" with the placeholder text "Enter reserve key". Below the input field are two buttons: a blue "Log In" button and a "Log Out" link. A horizontal line separates this section from the next. Below the line, there is a section titled "Don't have your recovery codes?" with the text "Enter a two-factor code from your phone". At the bottom of the window, there is a footer that reads "Powered by Atlassian Confluence 7.3.4 (la2dvwkivx001: 388e44e5) · Report a bug · Atlassian News" and the Atlassian logo.