

inception

WEB POWERED SECURITY

Simple & Easy Installation
Integrated Security - Access Control



Two-Factor Authentication (2FA)

Overview

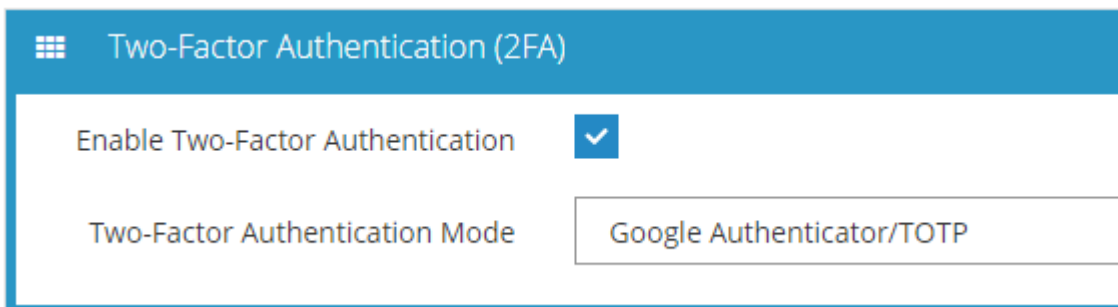
This technical note details how to configure the Inner Range Inception controller to support Two-Factor Authentication (2FA) for users logging into the Inception web interface.

Introduction

Two-Factor Authentication (2FA) provides an additional level of security for users logging into the Inception web interface by requiring them to enter an extra security code generated by a registered device such as a smartphone or tablet, in addition to their username and password. Inception firmware 4.0 adds support for Time-based One-time Password (TOTP) 2FA which is supported by many freely available 2FA apps. Google Authenticator is used as the example app in this guide, but any 2FA app that supports TOTP code generation should also work.

Enabling 2FA in the Controller Settings

2FA functionality is enabled by default in firmware version 4.0, but it can be enabled or disabled on a controller-wide basis by using the Two-Factor Authentication (2FA) options on the **[Configuration > General > System]** page. You can disable and re-enable 2FA on the controller without affecting user 2FA enrolment data; users will not have to be re-enrolled if you need to temporarily disable 2FA functionality.



Setting up NTP Synchronisation

The TOTP codes generated for Inception 2FA login rely on the internal clocks of both the Inception controller and the user's personal device to be synchronised with each other, since the codes are time-sensitive and will not be accepted outside of the timeframe they were generated in. Due to this technical requirement, we highly recommend that NTP synchronisation is enabled on the Inception controller when 2FA login is being used, in order to minimise the risk of users being locked out of the system when using 2FA.

To enable NTP time sync, go to the **[Configuration > General > Date and Time]** page and tick the "Enable NTP Syncing" checkbox if it is not already enabled. The default NTP servers are set to ntp.org's NTP server pool, but you can specify your own server(s) by entering their URLs in the "NTP Server(s)" field, with spaces separating each individual server URL.

Current Server Time


31/08/2020 12:22:11 PM

Time	
Enable NTP Syncing	<input checked="" type="checkbox"/>
NTP Server(s)	0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org 3.pool.ntp.org
Time Zone	Australia/Melbourne

Enrolling Users for 2FA Login

By default, users will not be prompted for a 2FA code on login unless they have been successfully enrolled for 2FA first. To enrol a User for 2FA, go to the **[Configuration > Users > Manage Users]** page and find the "Two-Factor Authentication (2FA) Configuration" field in the Credentials section.


Two-Factor Authentication (2FA) Configuration	Not Enrolled	
---	--------------	--


Click the  icon to bring up a dialog box that will take you through the user 2FA enrolment process on your personal device. You will first need to download Google Authenticator (or another compatible 2FA app) from the App store on your device.

User 2FA Configuration

Inception supports Two-Factor Authentication (2FA) with a smartphone or tablet using the Google Authenticator app or another compatible Time-based One-time Password (TOTP) authenticator app.

The Google Authenticator app can be downloaded from the Apple App store and Google Play store.

 GET IT ON Google Play

 Download on the App Store

Using your authenticator app, scan the QR code using your smartphone's camera, or manually enter the authentication key to add a new 2FA account.

After installing Google Authenticator on your personal device, press the + button in the bottom-right corner of the screen and select “Scan a QR code”. Using your device’s camera, point it at the QR code on the screen and the app should create a new 2FA account for your Inception user login. Alternatively, if you are not able to use your device’s camera, enter the Account Name and Key details as shown in the Manual Key entry section and create a new account.

The screenshot shows the Google Authenticator app interface. At the top, there is a section labeled "QR Code" with a blurred QR code. Below it is a section labeled "Manual Key Entry" with the following fields: "Account Name:" followed by a blurred input field, "Key:" followed by a blurred input field, and "Type of Key: Time based".

Optionally, click the “Get Backup Code” button to generate a one-time emergency backup code that can be used if you cannot use your personal device to log in. Keep in mind that your emergency backup code can only be used to login once, and you will have to remove your existing 2FA enrolment data and re-enrol if you want to get a new backup code.

The screenshot shows a dialog box with the text: "Your emergency backup 2FA login code is: [blurred code]. Please store this code safely, as it can only be used once." There is a close button (X) in the top right corner and an "OK" button in the bottom right corner.

After you have created a new 2FA account for Inception in the Google Authenticator app, enter the 6-digit code shown by your device and click Enrol to finish the process.

NOTE: Before clicking the Enrol button, it is recommended that the account creation process is repeated for any other user devices that will be used for logging in, since the registration dialog will no longer be accessible once the enrolment code has been successfully entered.

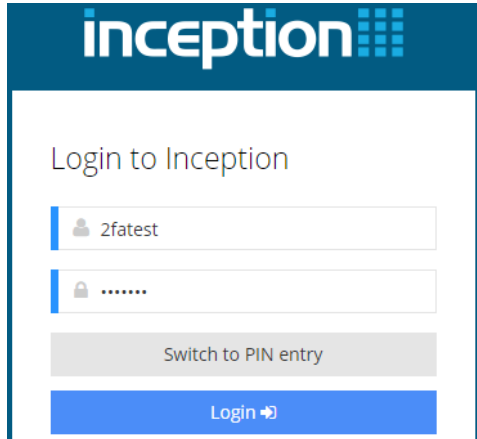
The screenshot shows a web interface for 2FA enrolment. It contains the text: "Once you have created an account, enter the 6-digit code from the authenticator app and click the Enrol button to confirm your 2FA enrolment." Below this is a text input field labeled "Enter Code". At the bottom, there are three buttons: "Enrol", "Get Backup Code", and "Cancel".

The 2FA enrolment process is now complete, and you should now receive an additional prompt for the 6-digit 2FA code the next time you log into the Inception web interface with your username and password.

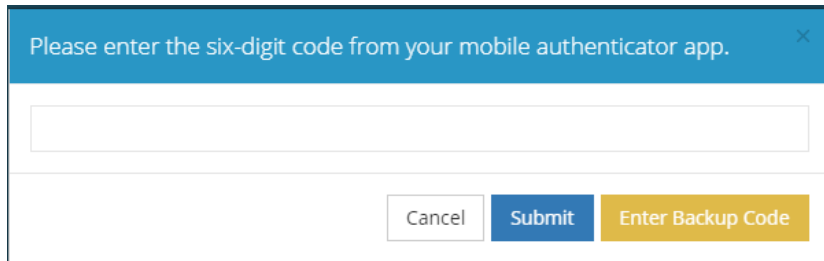
Logging into Inception with a 2FA code

When logging into Inception with a 2FA-enabled user account, you will receive an additional prompt asking you to type the 6-digit code shown in Google Authenticator on your registered personal device.

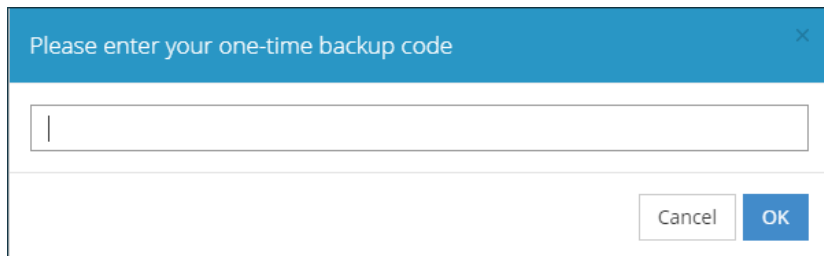
Open a web browser and go to the login page for the Inception controller. Enter your username and password/PIN as usual, then click the Login button.



A prompt will appear asking you to enter the additional security code from the authentication app on your device. Enter the code and click OK in order to complete the login and access the Inception web interface.

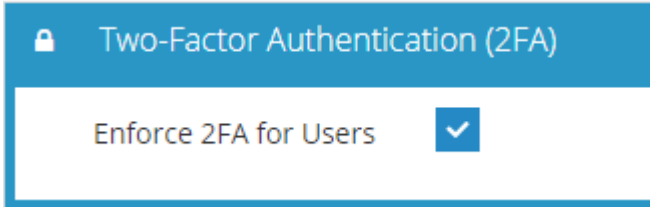


You can also click the “Enter Backup Code” button to log in with an emergency backup code if you generated one during the 2FA enrolment process. The backup code will only work once, so make sure only to use it in an emergency.



Enforcing 2FA for Web Page Profiles (optional)

For increased security, 2FA can be made compulsory for certain groups of users by editing the 2FA settings on the **[Configuration > Users > Web Page Profiles]** page. For example, you may want to enforce 2FA for users with high levels of permission such as installers or system administrators. To enforce 2FA for users associated with a certain web page profile, tick the “Enforce 2FA for Users” checkbox.



The next time a user in the group logs into the web interface, they will be redirected to a special 2FA enrolment page before being allowed to access the rest of the web interface. Enrolment can be done by scanning a QR code image with Google Authenticator or entering the account details manually, similar to the enrolment dialog on the Manage Users page.

Two Factor Authentication (2FA) Enrolment

The security policy for this user account requires that two-factor authentication (2FA) is configured before you can access the Inception web interface.

Download the Google Authenticator app (or another compatible 2FA app) onto your smartphone or tablet device.



Scan the QR code using the authenticator app on your phone, or manually enter the authentication key to add a new 2FA account.

QR Code



Manual Key Entry

Account Name:

Key:

Type of Key: Time based

Optionally, the user can choose to generate an emergency backup code for 2FA login to be used if they have lost access to their device or cannot log in for another reason. To generate the backup code, click the “Generate Backup Code” button. The backup code should be stored securely by the user and used in the event when the user cannot log in with 2FA through normal means, e.g. due to system problems or loss of device.

Emergency Backup Code

Click the Generate Backup Code button to generate an emergency backup code that can be used to log into Inception if you lose your registered personal device.

Generate Backup Code

Once a 2FA account has been created on the user's device, they can enter the 6-digit code from their authenticator app into the text box and click the Enrol button to finish enrolling. Once successfully enrolled, they will be taken to the Dashboard page and allowed to access the web interface as normal.

Enter the 6-digit code from your authenticator app and click the Enrol button to confirm your 2FA enrolment.

Troubleshooting

My 2FA login code isn't working

The TOTP codes used for 2FA login require that Inception's system time be kept in sync with the system time on your personal device used to generate codes. Ensure that your device's time is accurate, and that Inception's system time is kept accurate with synchronisation from an NTP server.

You can also use an emergency backup code to login if you generated one at the time you enrolled for 2FA. Keep in mind that your emergency backup code can only be used to login once, and you will have to remove your existing 2FA enrolment data and re-enrol if you want to get a new backup code.

I've lost my device, how do I log in?

You can ask someone with user administration privileges to log in and remove your 2FA enrolment data, or help you enrol a new device for 2FA.

No one can log into the system, how can we access the device?

If no one can log into the system due to 2FA login codes, the system time on the Inception controller is likely incorrect (enabling NTP time sync is highly recommended when using 2FA login for this reason).

To fix the problem, you can reset the Installer user details on the controller in order to log in without 2FA, which requires physical access to the controller. Consult the Inception installation manual for the reset procedure. Log in with the defaulted Installer user details and go the **[Configuration > General > Date and Time]** page to fix the Date and Time settings, or temporarily disable 2FA login from the **[Configuration > General > System]** page.