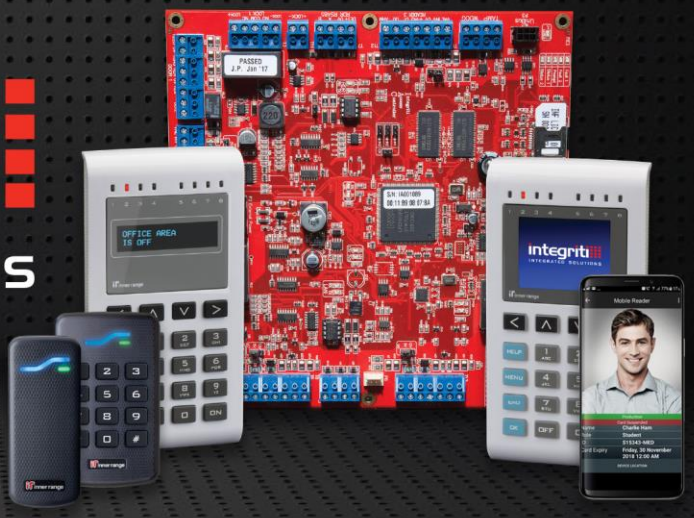
integriti
INTEGRATED SOLUTIONS



Two-Factor Authentication (2FA) Guide

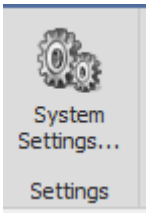
Introduction

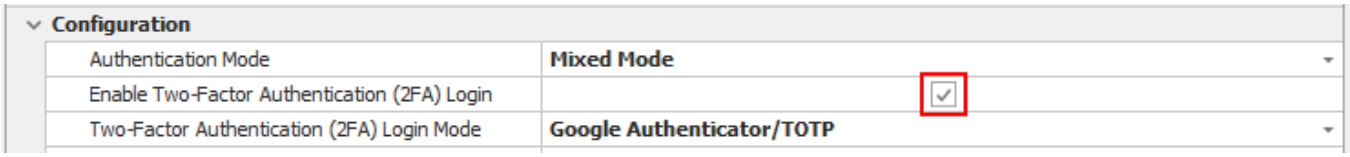
Two Factor Authentication (2FA) provides an additional level of security for users logging into the Integriti system by requiring them to enter an extra security code generated by a registered device such as a smartphone or tablet, in addition to their username and password. Integriti implements 2FA through Time-based One-time Password (TOTP) codes, which can be generated 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.

2FA login can be enabled in Integriti by enrolling specific operators, or by setting up a Security Policy that enforces 2FA enrolment so that 2FA enrolment is made mandatory for newly logged in operators. 2FA login is supported for Integriti System Designer & Gatekeeper, as well as the Integriti Web Interface. 2FA login is also supported for use with Integriti's Active Directory Integration and Single Sign-On (SSO) features.

Setting up 2FA

To enable 2FA login for the Integriti system, open the System Settings window from the System tab in Integriti System Designer and enable the "Enable Two-Factor Authentication Login" option under the Configuration category. **NOTE:** The logged in operator must have permission to edit the system settings.





You should now be able to enrol operators for 2FA access.

Enrolling an Operator for 2FA

Downloading an authentication app

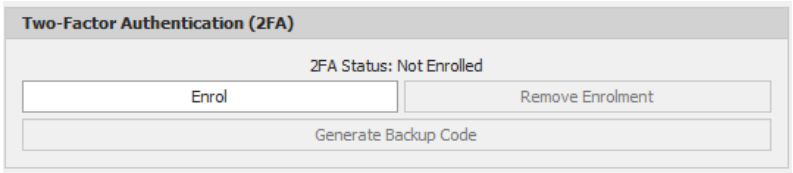
Integriti uses time-based TOTP codes for verification, which can be generated by several freely available compatible smartphone apps. For ease of setup, Inner Range recommends using the Google Authenticator app, which can be downloaded from the Google Play Store or Apple App Store for Android and iOS devices respectively:

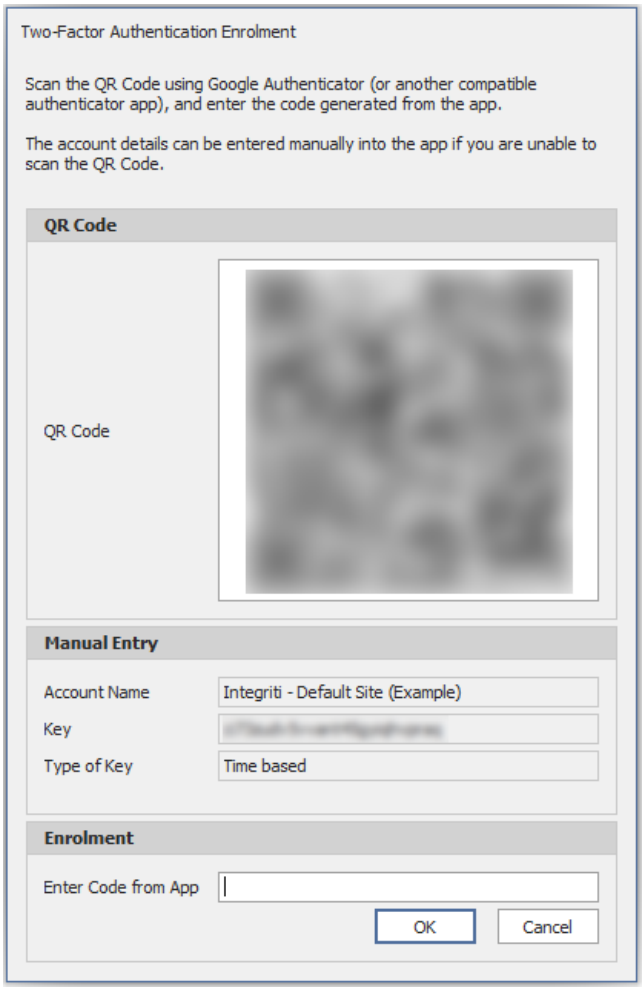
GET IT ON Google Play

Download on the App Store

Enrolling the operator by scanning a QR code

Open the Operators panel from the Administration tab in System Designer and edit the operator you wish to enrol for 2FA login. Click the Enrol button to bring up the 2FA enrolment dialog.



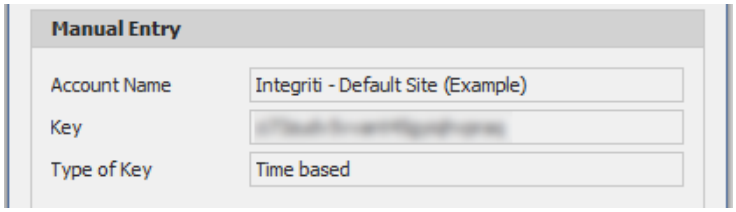


Scan the QR code with your device's camera and it should prompt you to open the link with the authenticator app you installed earlier. If you are using Google Authenticator, a newly created Integriti 2FA account should now be visible in the main app window. Enter the 6-digit code from the authenticator app into the Integriti 2FA Enrolment

dialog and click OK to continue. The operator should now be successfully set up for 2FA and will be prompted for a 2FA code the next time they log into Integriti. **NOTE:** Make sure to scan the QR code with all the personal devices you plan to use for 2FA login before confirming the code and clicking OK. Once the enrolment dialog is complete, you will not be able to enrol other personal devices unless you delete the existing enrolment data and re-enrol.

Enrolling the operator manually (without a QR code)

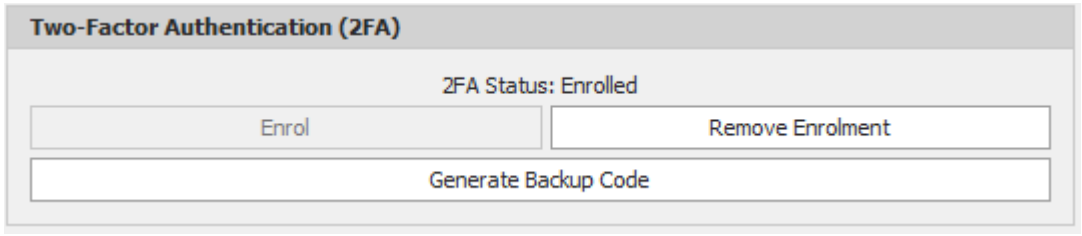
If you are unable to enrol by scanning the QR code, you can enter the 2FA account key into your authentication app manually instead. In Google Authenticator, select the "Enter a setup key" option and enter the Account name, Key and Type of key given by the enrolment dialog. Press the Add button to create the account and enter the 6-digit code from the app into the Enrolment dialog to proceed.



Generating an Emergency Backup Code (optional)

An emergency backup code can be generated to allow an operator to login in the case that they lose access to the phone or smart device they use for 2FA access. The backup code only allows the operator to log in once before the code expires forever, so the operator will need to fix any 2FA enrolment issues during their login session or generate another backup code if they wish to be able to log in again. It is recommended that backup codes are stored in a secure place (e.g. a password-protected file, or written on a note stored in a safe) where they can be retrieved in an emergency if needed.

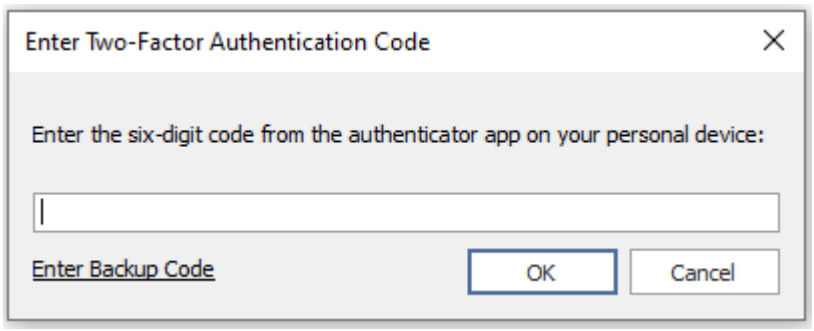
From the Edit Operator window, click the Generate Backup Code button to generate a new backup code. Make sure to store this code in a safe place. **NOTE:** Generating a backup code if one already exists will cause the old backup code to expire.



Logging in with 2FA

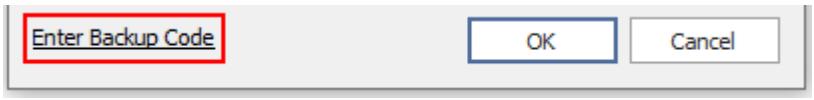
Logging in with a 2FA Code

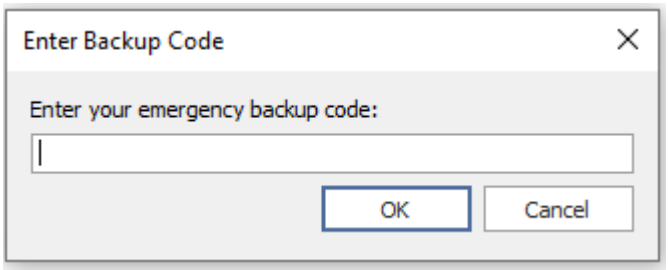
After you log into Integriti with your username and password, you should now see another dialog prompt asking for a 2FA code. Open the authenticator app on your personal device and enter the 6-digit code from the app and click OK.



Logging in with an Emergency Backup Code

To login with a backup code, click the “Enter Backup Code” link on the “Enter Two-Factor Authentication Code” dialog that appears when you log into Integriti, and enter your backup code. **NOTE:** The backup code expires after a single use.

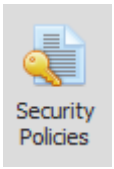


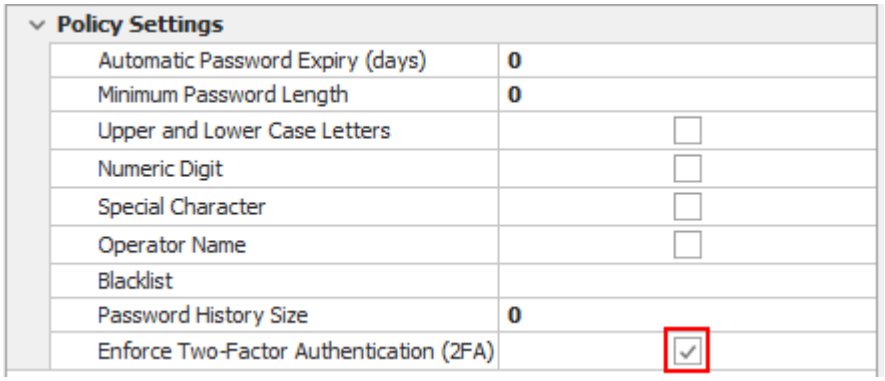


Enforcing 2FA with Security Policy

Setting up 2FA Enforcement

Open the Security Policies panel from the Administration tab and open the policy you wish to enforce 2FA for. Tick the “Enforce 2FA” checkbox in the policy settings and save the policy.





All operators covered by the security policy should now receive a prompt to register for 2FA the next time they log into Integriti if they are not already enrolled.

Logging in while 2FA Enforcement is enabled

When an operator logs into Integriti while 2FA enforcement is enabled, they will see the 2FA enrolment dialog pop up and prompt them to enrol before they can access the system. If the dialog is cancelled, the program will close and the operator will not be able to proceed.

Troubleshooting

My 2FA code is rejected when I try to log in

The TOTP codes generated by your authentication app are time-based and rely on the system time being synchronised between the Integriti server and your personal authentication device. Ensure that your device's system time is accurate, and that the Integriti server's system time is kept accurate with synchronisation with an NTP server.

If your device clock is properly synchronised and the problem persists, the account on your 2FA app may be incorrectly configured. Contact a system administrator to remove your existing Integriti 2FA enrolment data so you can re-enrol the account and try again.

I've lost my personal 2FA device, how do I log in?

If you generated an emergency backup code when you enrolled for 2FA, you can use this code at the login screen by clicking "Enter Backup Code" on the 2FA code prompt that appears after you submit your username & password.

NOTE: The backup code can only be used once before it expires, so make sure you fix any 2FA enrolment issues while you are logged into the system.

If you have lost your backup code or did not generate one, you will need to contact an administrator to reset your 2FA enrolment data so that you can log in and re-enrol for 2FA with another device.

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

If all operators are locked out of the system, contact Inner Range Technical Support for assistance in regaining access to the system..