IDENTITY & ACCESS SECURITY

FactorShield

Add stronger sign-in approval without making access harder to understand

Protect workforce and application access with number matching, authenticator approval, TOTP and policy-led identity controls.

The value for your team

01

Clear approvals

Use number matching and explicit user confirmation to reduce blind approvals.

02

Flexible factors

Support authenticator approval and standards-based TOTP where appropriate.

03

Auditable access

Keep enrolment, challenge and outcome events visible to authorised teams.

Product overview

FactorShield adds a clear second-factor decision to supported authentication journeys. It is designed for tenant-controlled enrolment, visible approval prompts and auditable outcomes, with RADIUS and RadSec integration available for compatible network-access environments.

FactorShield is designed for organisations protecting employee portals, business applications and compatible network-access workflows. It connects number-match approval, tenant-controlled enrolment and authentication audit events so teams can move from input to accountable action without losing the decision trail.

The product supports the operating workflow; it does not remove professional judgement, statutory responsibility or customer ownership. Final controls, integrations and commercial scope are confirmed during discovery and recorded in the implementation plan.

Customer challenges it addresses

01 Information about number-match approval, authenticator and totp factors and tenant-controlled enrolment often lives in separate tools, inboxes or spreadsheets, making the operating picture difficult to trust.

02 When teams need to challenge supported sign-in attempts, manual hand-offs can hide ownership, delay decisions and make exceptions harder to resolve.

03 Leaders need a clearer way to achieve auditable access while preserving human approval, role boundaries and an understandable record of what happened.

Value created in practice

Clear approvals

Use number matching and explicit user confirmation to reduce blind approvals.

Flexible factors

Support authenticator approval and standards-based TOTP where appropriate.

Auditable access

Keep enrolment, challenge and outcome events visible to authorised teams.

Detailed capabilities

Six connected capabilities shape the core FactorShield operating experience.

01 Number-match approval

Bind the approval decision to the sign-in attempt so the user must confirm the intended authentication rather than approve blindly.

02 Authenticator and TOTP factors

Support appropriate second-factor methods with clear enrolment and verification boundaries for the protected application.

03 Tenant-controlled enrolment

Keep factor enrolment under the organisation's tenant and authorised administrator process.

04 Access policy controls

Apply defined access rules to supported authentication journeys and record the resulting policy outcome.

05 RADIUS and RadSec integration

Extend supported identity decisions into compatible network-access environments through assessed RADIUS or RadSec integration.

06 Authentication audit events

Organise readiness and review information so leaders can see what is complete, what remains open and who owns the next action.

Connected operating model

The capabilities are designed to work together. Number-match approval establishes context, tenant-controlled enrolment moves the work forward, and authentication audit events supports review and accountability.

How teams use the product

The workflow is intentionally simple to understand, while retaining visible owners, review points and evidence.

01

Enrol the user and approved device

Authorised users combine number-match approval and authenticator and totp factors to enrol the user and approved device. The workflow keeps the responsible owner, review point and resulting action visible.

02

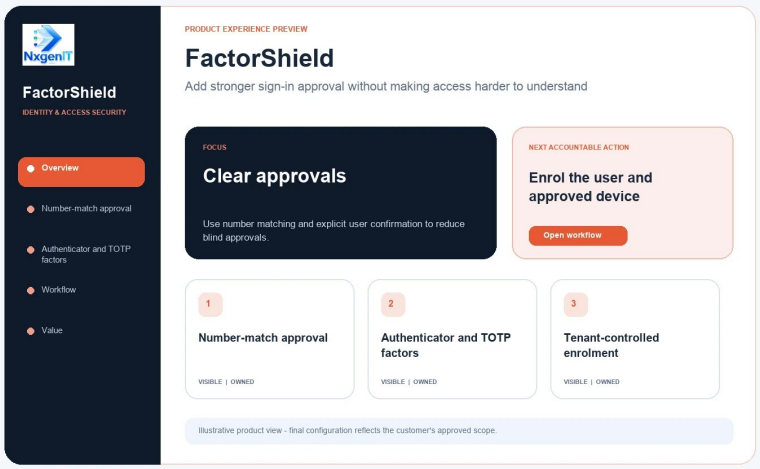
Challenge supported sign-in attempts

Authorised users combine tenant-controlled enrolment and access policy controls to challenge supported sign-in attempts. The workflow keeps the responsible owner, review point and resulting action visible.

03

Record approval, denial and policy outcome

Authorised users combine radius and radsec integration and authentication audit events to record approval, denial and policy outcome. The workflow keeps the responsible owner, review point and resulting action visible.



Illustrative product preview. Final screens and configuration reflect the customer's approved scope.

Rollout, governance and success

A controlled rollout keeps the product aligned to customer ownership, real operating roles and measurable outcomes.

PHASE 01

Discover and scope

Confirm the users, operating boundaries, source data and decisions that FactorShield must support.

PHASE 02

Configure roles and controls

Define authorised roles, approval points, protected information and escalation paths before customer data is introduced.

PHASE 03

Prepare data and connections

Map the required inputs for number-match approval and authenticator and totp factors, including migration or integration needs.

PHASE 04

Pilot, validate and scale

Run a controlled pilot, review outcomes with responsible users, adjust the workflow and expand only after acceptance.

Roles, ownership and control

FactorShield is configured around named users, authorised roles and explicit approval points. Customer data remains customer-owned, protected information is limited to appropriate roles, and important actions retain an understandable history.

What success can look like

- Shorter cycle time across 'Enrol the user and approved device'.
- Fewer unresolved exceptions around tenant-controlled enrolment.
- Clearer ownership of approvals, follow-ups and closure evidence.
- Stronger adoption among the intended users and responsible reviewers.

Best for

Organisations protecting employee portals, business applications and compatible network-access workflows.

See how this product fits your operation

www.nxgenit.co.za/products/factorshield | info@nxgenit.co.za