Protect Foundations - Delivery Playbook

PingOne Protect

Field	Value
Version	1.0
Date	2026-04-01
Owner	Partner Delivery Architects
Intended Audience	Technical Consultants/Project Managers
Distribution	Internal/Partner

Related Delivery Kit Assets

- **Protect Foundations – Getting Started**
- **Protect Foundations – Best Practices**
- **Protect Foundations – Fundamentals**
- **Protect Foundations – PingFederate Integration Guide**
- **Protect Foundations – DaVinci Integration Guide**
- **Protect Foundations – PingAM / AIC Integration Guide**
- **Protect Foundations – Delivery Roadmap Template**

Table of Contents

Protect Foundations - Delivery Playbook

This playbook provides a structured, phase-based approach for partners and PS teams to deliver PingOne Protect Foundations.

It focuses on what to do, in what order, and which Delivery Kit assets to use to successfully deliver PingOne Protect Foundations - not on product-level configuration (covered in **Protect Foundations - Fundamentals** and **Integration Guides**).

This playbook assumes a basic understanding of PingOne Protect concepts. If you are new to Protect, review the **Protect Foundations - Fundamentals** guide before starting delivery.

---

1. Recommended Delivery Approach

This section provides a simplified view of the delivery flow before diving into detailed phase-by-phase guidance.

For most engagements, partners and PS teams should follow this approach:

1. Define scope and target journeys
   → Use the **Protect Foundations - Scoping Guide**
2. Prepare the environment
   → Use the **Protect Foundations - Getting Started**
3. Understand core concepts and capabilities
   → Use the **Protect Foundations - Fundamentals**
4. Select and implement the integration approach (PingFederate, DaVinci, or AIC)
   → Use the relevant **Protect Foundations - Integration Guide**
5. Validate behaviour and outcomes
   → Use the **Protect Foundations - Evidence Matrix Template**
6. Tune policies and predictors
   → Use the **Protect Foundations - Best Practices**
7. Deploy and hand over to the customer
   → Use the **Protect Foundations - Solution Handover Template**

This approach represents the minimum recommended delivery path for a successful Protect Foundations implementation.

2. Key Delivery Decisions

This section highlights the key decisions partners and PS teams must make when delivering PingOne Protect Foundations. These decisions should be made early in the engagement and guide the overall delivery approach.

2.1 Choosing the Integration Approach

Select the integration method based on the customer's existing architecture and use case:

- **PingFederate**
  → Best for workforce environments with existing authentication policies
- **DaVinci**
  → Best for CIAM use cases requiring orchestration and flexible flows
- **PingOne Advanced Identity Cloud (AIC / PingAM)**
  → Best for customers already using PingAM or AIC

2.2 Choosing the Initial Journey

Start with a single, high-value journey:

- **Login / Authentication**
  → Fastest path to value and easiest to validate
- **Registration**
  → Best for fraud prevention and bot detection use cases
- **Transaction / Approval**
  → More advanced use case, typically delivered after initial rollout

2.3 Defining the Risk Strategy

Start with a simple and explicit risk response model before implementation:

Low Risk → Allow access

Medium Risk → Step-up authentication (e.g. MFA)

High Risk → Block, challenge, or require additional verification

This model should be agreed with the customer early and refined during tuning based on observed behaviour and business requirements.

3. Minimum Recommended Delivery

This section defines the minimum recommended scope for a successful Protect Foundations implementation.
Partners and PS teams should prioritise delivering a simple, working solution before expanding into additional use cases or advanced configurations.

3.1 Minimum Scope

For most engagements, the following is sufficient:

- One in-scope journey (e.g. login or registration)
- A single integration approach (PingFederate, DaVinci or PingAM/AIC)
- Basic risk evaluation integrated into the selected journey
- A simple Low / Medium / High response model
- Avoid over-engineering early in the engagement. Start with a simple implementation (single journey, default policy, minimal branching) and expand based on observed risk patterns and business requirements.

3.2 Minimum Technical Implementation

- PingOne Protect enabled and configured in the target environment
- Risk evaluations successfully generated and visible in the Protect dashboard
- Integration logic responding to risk levels (Low / Medium / High)
- No advanced tuning or custom predictors required initially

3.3 Validation Expectations

- At least one end-to-end journey validated using the Evidence Matrix
- Expected vs actual outcomes aligned
- No critical defects impacting the primary journey

3.4 What to Avoid

- Implementing multiple journeys in the initial phase
- Over-tuning policies before sufficient data is collected
- Introducing complex custom or composite predictors too early
- Overriding risk levels globally (e.g. forcing High → Low)

4. Delivery Phases at a Glance

This playbook organises delivery into six phases, aligned with the internal Protect Foundations Delivery playbook (Pre-Engagement, Design, Implementation, Predictor Evaluation, Monitoring, Delivery) and the Delivery Kits framework roadmap.

Phase	Objective	Primary Roles	Key Kit References
1. Scoping & Pre-Engagement	Shape scope, journeys, and success criteria; confirm prerequisites	SE, TC, PM, Customer owner	Scoping Guide; Datasheet; SOW
2. Initiation & Design	Kick off, confirm scope, choose integration surface, design flows	PM, TC, Customer IAM/Security	Getting Started; Fundamentals; Delivery Playbook
3. Build & Integrate	Configure Protect, implement integration patterns, get first evaluations	TC	Fundamentals; Integration Guides (PF/DaVinci/AIC);
4. Tune & Validate	Let predictors train, tune policies, validate journeys & UX	TC, Customer IAM/Sec, PM	Best Practices; Delivery Playbook; Evidence Matrix
5. Deploy & Handover	Go-live, confirm runbooks, hand over ownership & evidence	PM, TC, Customer Ops	Output Checklist; Evidence Matrix; Solution Handover
6. Run & Optimise	(Optional) Ongoing monitoring, optimisation, and follow-on scope	Customer Ops/IAM, Partner/PS (advisory)	Best Practices;

Subsections below give inputs, core activities, and outputs for each phase.

5. Phase 1 – Scoping & Pre-Engagement

This phase should focus on defining a clear and achievable scope aligned to a Protect Foundations implementation, avoiding over-scoping additional journeys or advanced use cases.

5.1 Objective

- Understand business drivers, target journeys, and risk appetite.
- Decide what is in scope for the Protect Foundations Project vs follow-on work.
- Confirm prerequisites and dependencies before scheduling delivery.

5.2 Inputs

- PingOne Protect Datasheet
- Protect Foundations Scoping Guide
- Draft SOW / proposal.

5.3 Core Activities

- Discovery workshop (60–90 mins):
    - Capture drivers and outcomes (ATO, new account fraud, bots, MFA fatigue reduction, transaction protection).
    - Inventory candidate journeys (Auth, Reg, Recovery, Tx) and prioritise them.
    - Discuss volumes and risk appetite (tolerance for friction, desired actions per risk level).
    - Choose the primary integration surface (PF, DaVinci or AIC/PingAM).
- Confirm technical prerequisites:
    - PingOne tenant & target environments.
    - Network egress to PingOne APIs.
    - Admin roles and logging/monitoring capabilities.

5.4 Outputs

- Completed **Protect Foundations - Scoping Guide** (journeys in/out, risk appetite, integration choice, assumptions).
- Updated Work Plan / schedule
- Draft SOW and commercial alignment.

✓ This phase is complete when:

- ☐ In-scope journeys are clearly defined
- ☐ Integration approach is agreed
- ☐ Success criteria are documented
- ☐ Key prerequisites and dependencies are confirmed

6. Phase 2 – Initiation & Design

6.1 Objective

- Kick off the engagement, confirm scope and roles, and agree on design for how Protect will be used in the selected journeys.
- Move from “we want Protect” to “we know where and how Protect will evaluate risk in flows.”

6.2 Inputs

- Signed or near-final SOW.
- Completed **Protect Foundations - Scoping Guide** (Phase 1).
- **Protect Foundations – Delivery Playbook** (for consultant reference).

6.3 Core Activities

- **Project Kickoff**
  - Confirm in-scope journeys, timelines, and success criteria.
  - Introduce roles and responsibilities (customer IAM, SecOps, apps, PS/partner team).

- **Design Workshops** (leveraging Protect Foundations “Design Phase” and “Information Gathering”).
  - Re-validate:
    - Primary integration surface (PF, DaVinci or AIC/PingAM).
    - Whether we’re inserting Protect into existing flows or building new ones.
  - Identify for each in-scope journey:
    - Where Protect will evaluate (login, pre-MFA, registration submit, transaction confirm, recovery step).
    - High-level actions by risk level (Low/Medium/High).
  - Confirm predictors of interest and initial policy coverage (workforce vs CIAM hints, as per **Protect Foundations - Best Practices**).

- **Environment & Access Prep**
  - Use **Protect Foundations - Getting Started** + **Fundamentals** to:
    - Enable Protect on the correct environment.
    - Ensure admin roles and basic dashboard access exist.

6.4 Outputs

- Engagement overview / design summary (can be a short section in the Solution Handover doc, started early):

    - In-scope journeys, integration surfaces, risk actions by level.
- Updated Work Plan with phases and sessions (align with Protect Foundations Work Plan).
- Confirmed list of technical owners and environment access.

✓ **This phase is complete when:**

- ☐ Target journeys and flows are clearly defined
- ☐ Risk evaluation points are agreed within each journey
- ☐ High-level risk response model (Low/Medium/High) is aligned
- ☐ Roles, timelines, and delivery plan are confirmed

---

7. Phase 3 – Build & Integrate

This phase should focus on implementing a single working journey using the selected integration approach. Additional journeys and advanced configurations can be added after initial validation.

7.1 Objective

- Prepare the PingOne environment for Protect.
- Implement the chosen integration pattern (PF, DaVinci, AIC/PingAM, or API).
- Achieve end-to-end risk evaluations visible in the Protect dashboard.

7.2 Inputs

- **Protect Foundations - Getting Started** (environment-ready checklist).
- **Protect Foundations - Fundamentals** (detailed steps for service, worker app, policies, dashboard, SDK).
- Selected Integration Guide:
    - Protect Foundations - PingFederate Integration Guide
    - Protect Foundations - DaVinci Integration Guide
    - Protect Foundations - PingAM/AIC Integration Guide

7.3 Core Activities

7.3.1 PingOne Preparation (per Fundamentals guide)

- Enable PingOne Protect in the target environment and confirm the default risk policy exists.
- Create and configure a worker application (Worker type, correct roles, client ID/secret, env ID).

- Perform a quick dashboard sanity check (sample app or simple flow) to confirm events appear.

7.3.2 Integration Build (pattern-specific)

- PingFederate pattern – follow Protect Foundations - PingFederate Integration Guide:
  - Deploy integration kit JARs and assets.
  - Configure PingOne Protect IdP Adapter and optional Protect Provider for device profiling.
  - Wire adapter into PF authentication policies with branches for Low/Medium/High.

- DaVinci pattern – follow Protect Foundations - DaVinci Integration Guide
  - Configure PingOne Protect connector (Create/Update Risk Evaluation).
  - Implement device collection via Forms/HTTP + skrisk or SDK.
  - Create flows that call Protect and branch on `result.level`/`recommendedAction`.

- PingAM / AIC pattern – follow Protect Foundations - PingAM/AIC Integration Guide
  - Configure PingOne Worker Service and secret mapping.
  - Add Protect Initialise → Evaluate → Result nodes into journeys.
  - Branch based on risk outcomes and ensure results update evaluations.

7.4 Outputs

- Working integration in at least one non-prod environment:
  - Protect receives evaluations.
  - PF/DaVinci/AIC can branch on risk.
- First version of config baselines (snapshots or exports) captured for handover:
  - PF policies / DaVinci flows / AIC journeys.
  - Risk policies and key configuration notes.

✓ **This phase is complete when:**

- ☐ PingOne Protect is configured in the target environment
- ☐ Integration is working for at least one journey
- ☐ Risk evaluations are visible in the Protect dashboard
- ☐ Authentication or flow logic responds to Low/Medium/High outcomes

8. Phase 4 – Tune & Validate

Initial tuning should remain lightweight and focused on validating expected behaviour. Advanced tuning can be performed during ongoing optimisation.

Tuning is a required phase of every Protect implementation. Initial configurations should be treated as a starting point and must be refined based on observed behaviour, risk patterns, and business requirements.

Initial deployments may produce higher than expected medium or high-risk outcomes due to limited historical data. This is expected behaviour and should be refined during tuning as Protect models learn from real-world activity.

8.1 Objective

- Let predictors train on real traffic.
- Tune risk policies and predictors to a sensible operating point.
- Validate each in-scope journey using the **Protect Foundations - Evidence Matrix**.

8.2 Inputs

- **Protect Foundations - Best Practices** guide (policy patterns, training windows, tuning workflow).
- **Protect Foundations - Delivery Playbook** sections on Predictor Evaluation & Policy Design and Tuning & Monitoring.
- **Protect Foundations - Evidence Matrix Template** and **Output Checklist**.

8.3 Core Activities

8.3.1 Training Period

- Run Protect in observe / non-blocking mode for the recommended window:
    - Workforce: **1–3 weeks** of production traffic.
    - CIAM: **2–4 weeks** of traffic.

8.3.2 Policy & Predictor Tuning

- For each journey/policy:
    - Use the dashboard and audit logs to identify:
        - Predictors driving most High outcomes.
        - Obvious false positives (legitimate users flagged High).
    - Apply the tuning order from Best Practices:
        1. Fix data/integration issues (user IDs, IP, SDK payloads).
        2. Use allow lists and custom/composite predictors for known good patterns.

3. Adjust scores/thresholds where necessary.
4. Disable predictors only as a last resort and only for specific policies.

- Avoid global overrides that downgrade High → Low; instead, refine inputs and policy logic.

8.3.3 Scenario-Based Validation

- Define test scenarios per journey (Auth, Reg, Recovery, Tx) using the **Protect Foundations - Evidence Matrix Template**.
- For each scenario:
  - Run the journey, record:
    - Expected Protect behaviour (risk level, action).
    - Actual behaviour and Protect evidence (dashboard, audit, policy).
  - Mark Pass / Fail / N/A and capture any defects or follow-ups.

8.4 Outputs

- Tuned risk policies per use case, documented in Solution Handover.
- Completed **Evidence Matrix** for the environment.
- Updated **Output Checklist** confirming tuning and validation artefacts are in place.

✓ This phase is complete when:

- ☐ Predictors have been trained on real traffic
- ☐ Policies have been tuned to reduce false positives
- ☐ All defined scenarios have been tested using the Evidence Matrix
- ☐ Expected and actual outcomes are aligned

---

9. Phase 5 – Deploy & Handover

9.1 Objective

- Move from validated non-prod to production deployment.
- Ensure customer operations and support have the artefacts and ownership needed to run Protect safely.

9.2 Inputs

- Completed **Output Checklist**.
- Completed **Evidence Matrix**.
- Draft **Solution Handover Template** (partially filled during earlier phases).

9.3 Core Activities

- **Production Cutover Plan**
    - Decide whether to start with:
        - Learn mode / non-blocking, or
        - Partial enforcement (e.g., strong actions only for very clear High).
    - Align cutover timing with business windows and comms plans.

- **Runbook & Monitoring Setup**
    - Confirm:
        - Protect dashboard bookmarks and filters.
        - Any SIEM/SOC integrations and alerts.

- **Formal Handover**
    - Complete the **Protect Foundations - Solution Handover Template**:
        - Architecture and integration summary.
        - Environments and risk policies in use.
        - Operations, monitoring, and tuning responsibilities.
        - Evidence and test coverage summary.
        - Open risks and follow-on backlog.

9.4 Outputs

- Signed-off **Solution Handover** (customer-safe).
- Signed **Output Checklist** and **Evidence Matrix**.
- Agreed **ownership and support model** (who monitors, who tunes, who responds to incidents).

✓ **This phase is complete when:**

- ☐ Solution is deployed to production (or agreed target environment)
- ☐ Solution Handover document is completed and shared
- ☐ Evidence Matrix and Output Checklist are signed off
- ☐ Customer teams understand monitoring and ownership

10. Phase 6 – Run & Optimise (Post-Protect Foundations)

Following initial delivery, partners and PS teams should position:

- Regular tuning cycles (monthly/quarterly) based on evolving traffic and fraud patterns.
- Additional journeys or integration surfaces as follow-on work (e.g., new mobile apps, additional B2B flows).
- Deeper integration with SOC/fraud teams
- Playbook and Best Practices for monitoring and predictor quick cards.

These activities can be captured as backlog items in the **Protect Foundations - Solution Handover** and, where appropriate, scoped as separate PS/partner packages.

✓ **This phase is complete when:**

- ☐ Monitoring and alerting are in place
- ☐ Initial tuning adjustments have been completed
- ☐ Follow-on opportunities or backlog items are identified
- ☐ Ownership has fully transitioned to the customer or agreed support model

11. Roles & RACI (High-Level)

Use this as a starting point; adapt per customer.

Phase	Activity Cluster	Customer	Partner / PS	Notes
Scoping	Business drivers, journeys, risk appetite	Lead	Support	Use Scoping Guide and datasheet
Scoping	Technical prerequisites & dependencies	Lead	Advise	Customer confirms environments, access, egress
Initiation & Design	Kickoff, design workshops	Shared	Shared	PM + TC lead sessions
Build & Integrate	PingOne prep, integration build	Support	Lead	Use Fundamentals + Integration Guides
Tune & Validate	Training, tuning, scenario testing	Shared	Lead	Customer provides traffic and test cases
Deploy & Handover	Cutover, handover, acceptance	Lead	Support	Partner/PS presents outputs, customer signs off
Run & Optimise	Ongoing tuning and optimisation	Lead	Optional	Potential follow-on services

This RACI should be refined and captured explicitly in the **Protect Foundations - Solution Handover** and/or SOW.