Protect Foundations – Documentation Handover

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 - Fundamentals**
- **Protect Foundations - Best Practices**
- **Protect Foundations - Integration Guide**
- **Protect Foundations - PingAM / AIC Integration Guide**
- **Protect Foundations - Output Checklist Template**
- **Protect Foundations - Evidence Matrix Template**

Table of Contents

Protect Foundations – Documentation Handover Template

Use this template as the customer-facing handover document at the end of a PingOne Protect engagement. It summarises what was built, how it behaves, how to operate it, and what comes next. Populate one version per customer and per production rollout (with references to lower environments where relevant).

This document should be completed as part of the Delivery Playbook handover phase and provided to the customer as the final summary of the implementation.

---

1. Engagement Overview

1.1 Customer & Project Details

- Customer name:
- Project / engagement name:
- Sponsor / business owner:
- Technical owner:

1.2 Objectives & Outcomes

Business objectives

Provide a short summary of the key business goals for this implementation (e.g., reduce fraud, improve login success rates, introduce adaptive MFA).

Protect Outcomes

Provide a summary of what this rollout delivers from a Protect perspective (e.g., risk-based authentication, bot detection, adaptive step-up flows).

1.3 Scope

In-scope user journeys

Provide a list of user journeys included in this implementation (e.g., login, registration, account recovery), including where Protect is applied.

Out-of-scope journeys

List any journeys intentionally excluded from this phase, including those planned for future rollout.

---

2. Architecture & Design Summary

2.1 High-Level Architecture

Provide a concise overview of how PingOne Protect is integrated into the existing IAM architecture, including where risk evaluation occurs in the user journey.

2.2 Integration Surfaces Implemented

Summarise where Protect has been integrated (e.g., PingFederate, DaVinci, PingAM/AIC), including key flows or journeys and how Protect is used.

---

3. Environments & Configuration

3.1 Environments

List all environments where Protect is configured (e.g., DEV, TEST, PROD), including region and purpose.

Environment	Purpose (DEV/TEST/PROD)	Region	Notes

3.2 PingOne Configuration

Summarise key Protect configuration per environment, including worker applications, active risk policies, and any custom predictors or attributes.

- Protect service: enabled (Y/N)
- Worker application(s): name(s) and purpose
- References to:
    - Risk policies (IDs/names)
    - Custom predictors (names/IDs)
    - Custom attributes used for third-party risk data

3.3 Integration Configuration References

Provide references or locations for key integration configurations (e.g., flows, journeys, adapters), without including sensitive information.

- PingFederate:
  - Adapter / provider names:
  - Policy trees / connections:
  - Export / backup location (if applicable):

- DaVinci:
  - Flow names & IDs:
  - Library templates used (if any):

- PingAM / AIC:
  - Journeys / trees:
  - Worker Service configuration name:

4. Risk Policies & Tuning Summary

4.1 Policies in Use

Summarise the risk policies active in production, including their purpose and where they are applied.

Policy Name	Purpose (Auth/Reg/Recovery/Tx)	Key Predictors	Enforcement Mode (observe/partial/full)	Notes

4.2 Key Tuning Decisions

Highlight the most important tuning decisions made during the engagement (e.g., threshold adjustments, predictor changes, allow lists).

- Training window and date(s) of main tuning cycles:
- Changes made (high-level):
  - Thresholds / scores:
  - Allow lists / composite predictors:

- Predictors disabled (if any) and rationale:

4.3 Known Limitations / Assumptions

Document any known data gaps (e.g., missing device data, limited training data, or incomplete integration coverage) may impact risk accuracy and enforcement decisions.

Risk behaviour may evolve over time as Protect models learn from real-world activity, particularly in early stages of deployment:

Early-stage deployments may show elevated medium/high risk rates due to limited historical data; this should stabilise as models learn over time.

5. Operations, Monitoring & Support

5.1 Day-2 Operations

Describe how Protect should be monitored and operated, including where to access dashboards and key views.

5.2 KPIs & Alerts

Summarise agreed success metrics and any alerts or thresholds used to monitor performance and risk:

5.3 Runbooks & Playbooks

Provide references to operational runbooks and guidance for handling common scenarios (e.g., fraud spikes, false positives).

---

6. Testing & Evidence Summary

6.1 Evidence Matrix Reference

Provide links or references to supporting evidence demonstrating that Protect is functioning as expected:

6.2 Key Scenarios Demonstrated

Summarise the main scenarios validated during testing (e.g., low-risk login, high-risk challenge, bot detection).

- Authentication (examples):
- Registration:
- Account recovery:
- High-risk transactions:

6.3 Outstanding Testing / Deferred Items

List any scenarios not yet tested and any agreed follow-up actions.

7. Open Risks, Issues & Backlog

7.1 Open Risks

Capture any known risks that could impact production behaviour or future rollout.

ID	Description	Impact	Likelihood	Owner	Mitigation / Next Step

7.2 Open Issues / Defects

List unresolved issues or defects, including status and ownership.

ID / Ticket	Summary	Environment	Priority	Owner	Status / ETA

7.3 Future Enhancements / Backlog

Summarise planned improvements, additional journeys, or enhancements for future phases:

8. Next Steps & Recommendations

Provide prioritised, practical recommendations to improve coverage, optimise performance, and expand Protect usage.

- Short-term (0–3 months):

- Medium-term (3–12 months):

- Longer-term (beyond 12 months):

Include any PS package / partner follow-up opportunities if appropriate (e.g., extended tuning, additional journey coverage).

9. Sign-Off

Capture formal acceptance of the solution, confirming readiness for production use and handover to operations.

Role	Name	Signature / Date
Customer Technical Owner		
Customer Security / Risk		
Customer Project Manager		
Partner / Ping Delivery Lead		

Comments: