POWER BI SECURITY

Power BI Authentication & Identity Types.

Every time you open a report, an invisible exchange happens.

Here's what it is and why your business depends on getting it right.

ProtoComet

THE HIDDEN EXCHANGE

Every time your dashboard loads, your data source asks one question:

"Who are you, and do you have permission to see this?"

This moment -- Power BI presenting its identity to a data source -- is called authentication. It happens silently, in milliseconds, every single refresh.

Most people never think about it. Until something breaks. And when it does, the consequences are real.

WHY THIS MATTERS TO YOUR BUSINESS

Authentication isn't IT's problem. It's yours.

Report Reliability

Wrong setup = refreshes that silently fail. Decisions made on stale data that nobody knew was stale.

Data Security

The wrong authentication method can expose sensitive data to the wrong people -- without any visible error.

Operational Risk

If your dashboards depend on one person's login, what happens when they go on holiday or leave?

THINK OF IT THIS WAY

It's Like Showing ID at a Security Checkpoint.

Your data source is the security checkpoint. Power BI is trying to get in.

The authentication type is the ID card it shows -- and different ID cards carry very different levels of trust, security, and risk.

Choosing the wrong ID card doesn't always cause an immediate failure. Sometimes it creates a ticking clock -- working fine today, breaking catastrophically tomorrow.

THE 8 AUTHENTICATION TYPES

Power BI offers 8 ways to prove who it is.

Anonymous

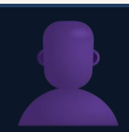
No ID shown

Basic

Username + password

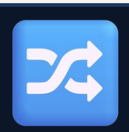
Windows

Corporate login



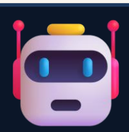
Org Account

Your M365 login



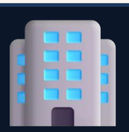
OAuth2 + SSO

Per-user passthrough



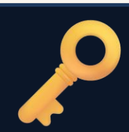
Service Principal

App identity



Workspace ID

Platform-managed



API Key

Shared secret string

⚠ PROCEED WITH CAUTION

Two types you should almost never use for internal data.

Anonymous -- No ID required

If a system lets anyone in without identifying themselves, it has no security. Using anonymous auth for internal data means your data is unprotected by design.

Basic (Username & Password) -- The old padlock

Simple and static. Passwords don't change unless someone actively updates them. Ex-employees' credentials can linger in your systems long after they've moved on.

MOST COMMON · DAILY USE

Organisational Account -- Your everyday badge

- ✓ Uses the same login as Outlook, Teams & SharePoint
- ✓ Multi-factor authentication applies automatically
- ✓ When an employee leaves, their access stops too
- ✓ Perfect for personal reports and early development

⚠ **The catch most businesses miss**

The credentials stored belong to one specific person. If they go on holiday or leave the company, every report relying on their login stops refreshing.

No warning. Just silence.

REAL-WORLD SCENARIO

The Key Person Trap

It's Monday morning. Your weekly KPI dashboard hasn't updated since Friday. The finance team is waiting for numbers.

The analyst who set up the connection? On a two-week vacation.

The report is tied to her personal login. Nothing refreshes until she's back.

I've seen this happen in organisations with multi-million dollar analytics investments. The fix takes five minutes once you know about it -- but first, you need to know it's a problem.

✅ PRODUCTION STANDARD

Service Principal
-- The company vehicle

🚗 Org Account

Personal Car

Used for company trips. Works fine -- until the person leaves, goes on holiday, or forgets the keys.

VS

🚙 Service Principal

Company Vehicle

Purpose-built. Tracked. Managed. Doesn't disappear when staff change.

If your dashboards drive business decisions, this is how they should be connecting -- not through anyone's personal account.

🚀 THE FUTURE STANDARD

Workspace Identity -- Zero-hassle security

No credentials to manage

The Azure platform handles all cryptographic identity -- automatically, behind the scenes.

No rotation anxiety

No secrets to expire at 2am on a Sunday. No emergency password resets.

The workspace IS the identity

Grant access to data once. Power BI connects automatically, forever.

📌 *Best for Azure-native environments on Microsoft Fabric or Premium. Verify connector support for your specific data sources before committing.*

QUICK REFERENCE

Which type should you use? Start here.

Personal reports / early development	→	**Org Account**
Production dashboards the business relies on	→	**Service Principal**
Azure-first environment on Fabric / Premium	→	**Workspace Identity**
On-premises SQL / corporate network data	→	**Windows + Gateway**
External SaaS APIs (marketing, CRM tools)	→	**API Key**

THE BOTTOM LINE

Authentication is a Business Decision.

- Never rely on a personal login for production reports
- Use Service Principal for anything the business depends on
- Treat API keys and passwords as the sensitive credentials they are
- Ask your team: whose login is your dashboard using right now?