Actifile QuickStart Deployment Guide (A/NZ)

Actifile Data Privacy Platform is as easy as 1, 2, and 3:

1. Your **MSP** trial account setup: https://my.actifile.com/sign-up-partner?partnerkey=BV4X-C9CC-IICW-OWV8
2. Set up Actifile in your AV/EDR Allow List. THIS IS CRITICAL.
3. Log into your Actifile Account: my.actifile.com > [**Add Customer – "Internal"** – if you are an MSP] > [**Deployment**] > [**Device Setup**] > [**Installation**] and then Download the Actifile Sentry Agent/MSI [**copy agent key**] and install the Actifile Sentry Agent (about 2 min) on your laptop/test machine.

It is that easy. The rest is **fully** autonomous. Discovery, quantify, monitor, identify your data risk exposure, and value your sensitive data without **any** additional effort. Introduction to Actifile.

What is Actifile

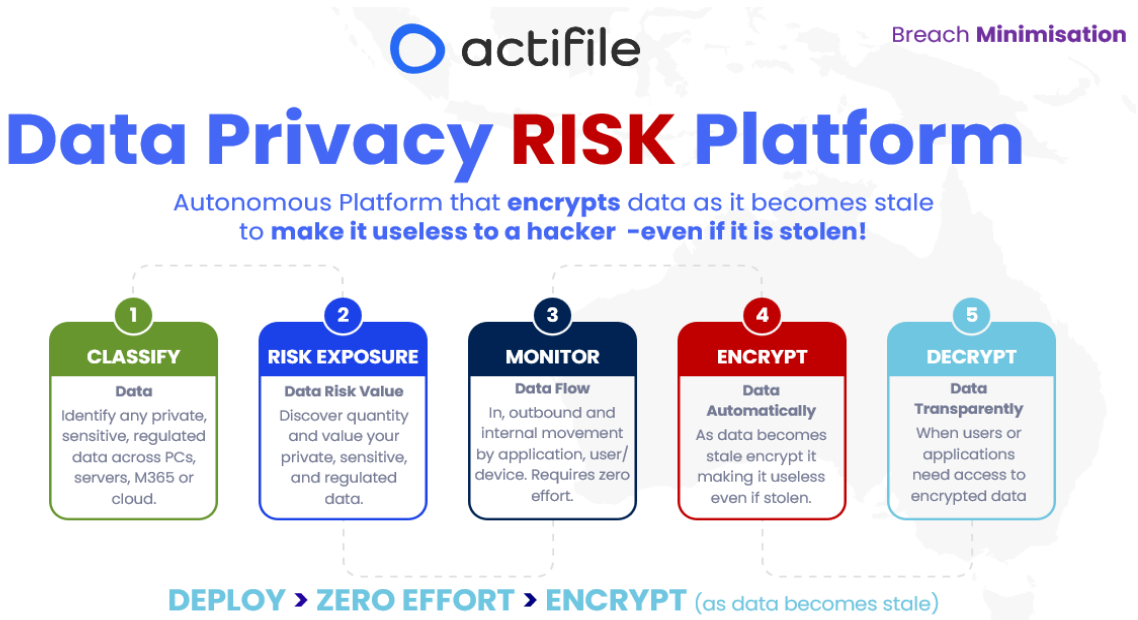
- **Outcome**: Actifile can automatically make your stale sensitive data useless to a hacker – even if it is stolen.
- **Deploys in minutes** and with zero effort: discover, classify and even value your data.

Quick Links:

- Login (new interface): my.actifile.com
- Book a Live Demo: Calendly - Greg Wyman
- Allow Listing in your AV/EDR/MDR/XDR product and Deployment options.

Questions:

1. *How much private and sensitive data do you have – and how much is inactive or stale?*
2. *If a hacker got hold of those inactive sensitive files – would they still be of value to them?*
3. *What would be reputational damage and financial impact if those sensitive records were exposed because they weren't encrypted?*

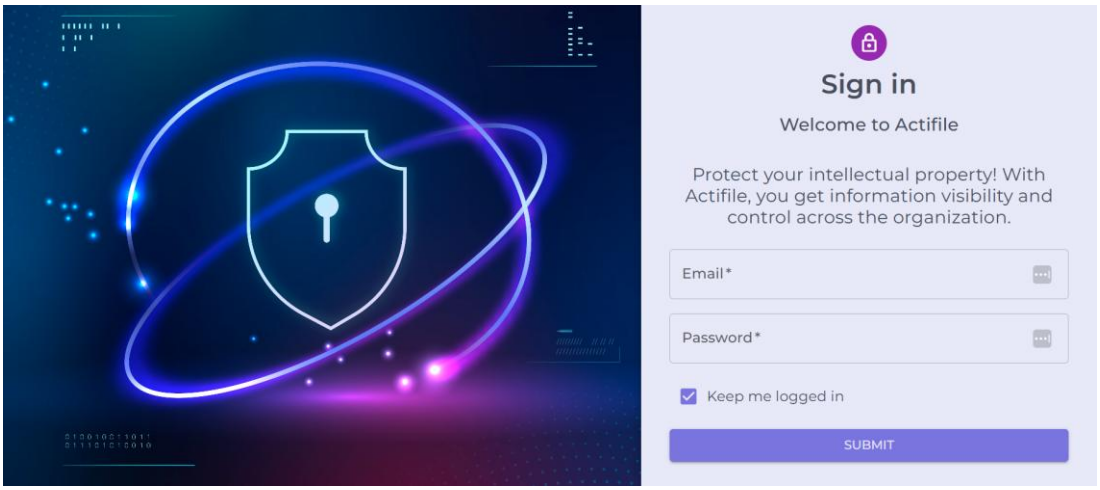


Actifile Deployment Guide

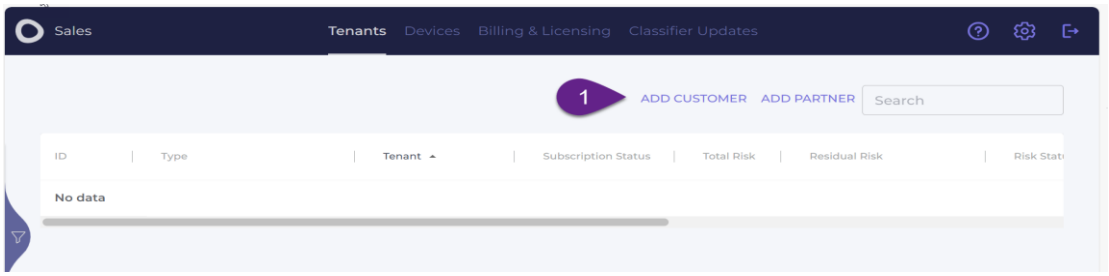
Welcome to Actifile! This guide will help you quickly and efficiently deploy Actifile in your organisation, to identify, quantify, classify, monitor and value your sensitive data with minimal effort. Follow the steps below to get started.

Step 1: Log into your Actifile Account

1. Create your full working trial: https://my.actifile.com/sign-up-partner?partnerkey=BV4X-C9CC-IICW-OWV8
2. Login: https://my.actifile.com/ - Sign in with your email and your password.



Step 2: Add [Your Company Name] as the First Customer

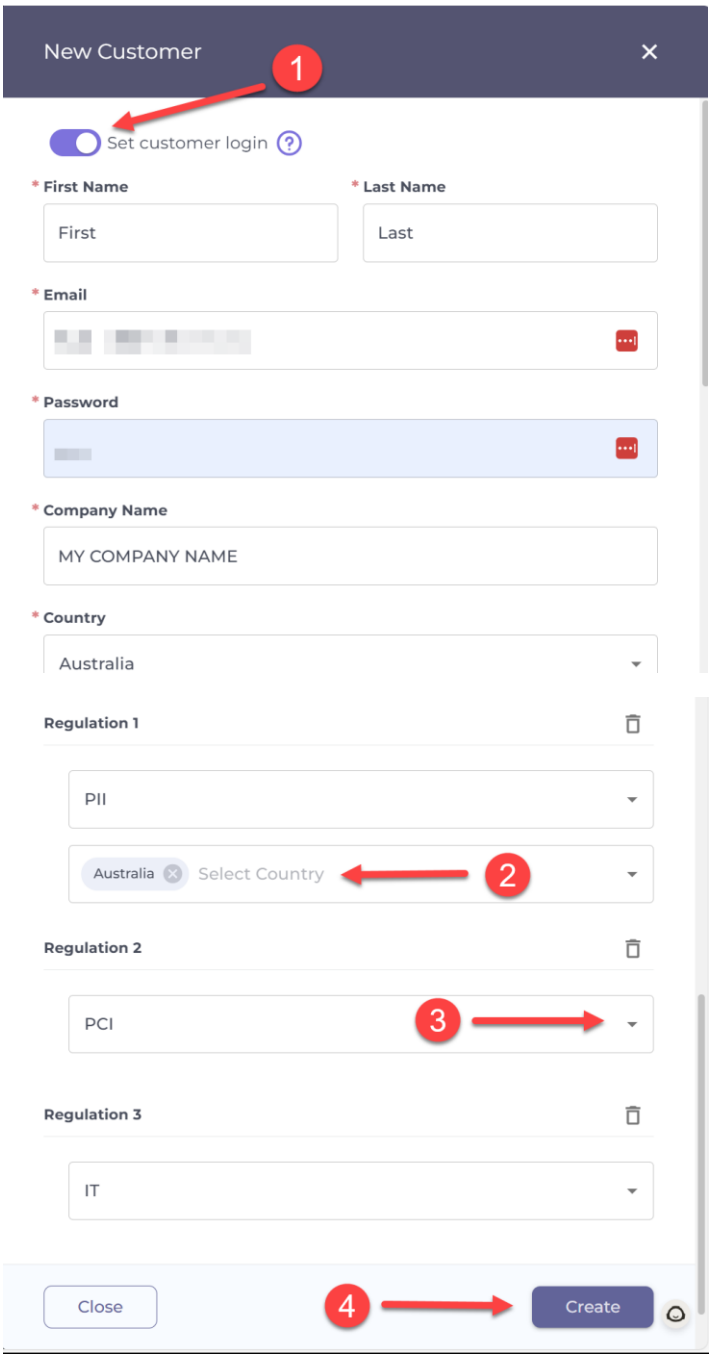


If you are End Client – your will log directly into your account.

If you are an MSP – you will be able to create Clients (see below) in your tenancy.

Supported environments: Windows, Mac, Linux PC/laptops and servers. Options are available for SharePoint, OneDrive, M365 (final beta), NAS and various cloud. Some may require additional fees or implementation processes.

This Trial License only allows installation of our endpoint agent. To perform a one time audit of your machine. Soon, we will be able to use the GRAPH API access into your M365 account and with zero physical deployment, you will be able to audit your complete M365 environment – including M365 mailbox attachments. **Note**: today – Actifile does not 'read" the body of emails, and it cannot encrypt M365 email attachments.



Activate: Customer Login, so they can login to their own portal and view their data.

No emails are sent.

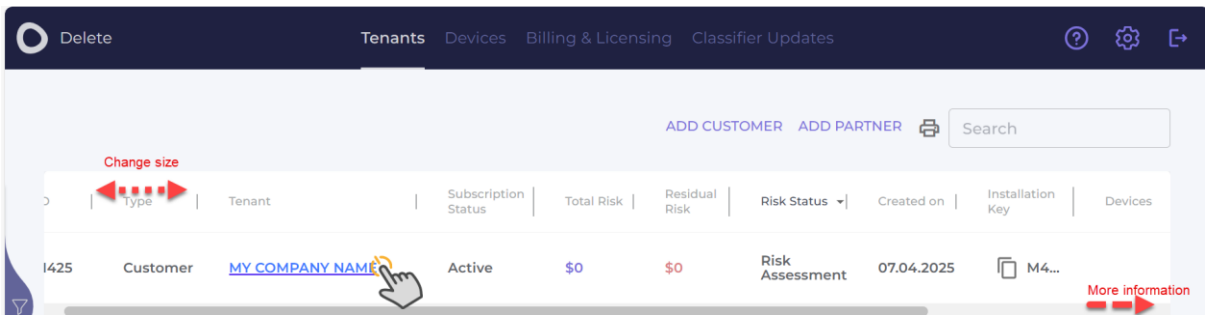
Select [Australia] or your country.

Leave defaults initially.

Add or delete [Regulated Classifications] of data (this can be changed in the future).

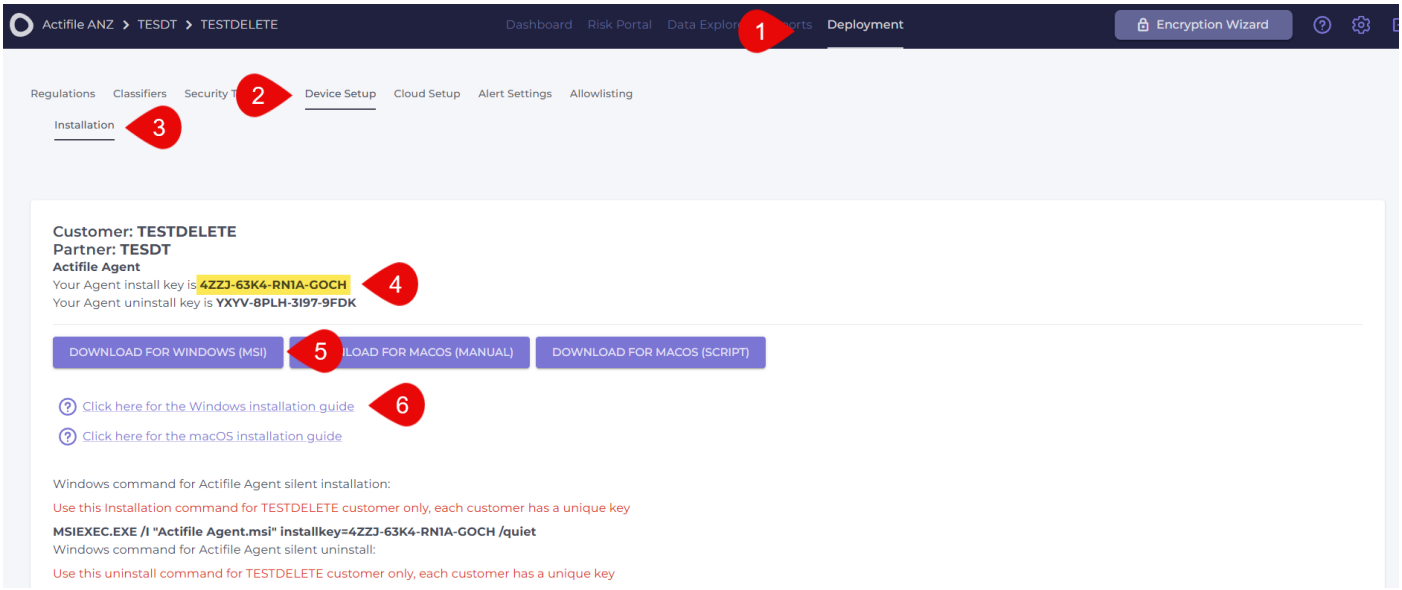
Click [Create] – your account will now be created.

Then Click [MY COMPANY NAME]



Step 3: Deploy the Actifile Agent

1. Place Actifile in your AV/EDR/MDR/XDR Allow list – **CLICK HERE**. THIS IS A CRITICAL STEP.
2. Download the Actifile Sentry agent directly from the portal.

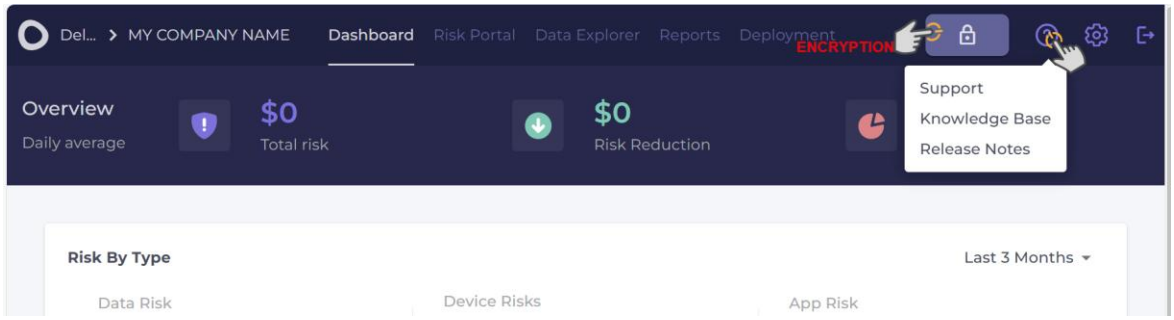


2. Deploy the agent across all endpoints/servers in your organisation (trial it on up to 10 pc's/laptops).
3. For multiple machine deployments, ensure the "path" includes the Fully Qualified Domain Name (FQDN) to the installer package that can be accessed by those machines.
4. Once installed, Actifile will automatically begin auditing your environment with **ZERO EFFORT** required from your team. Book a meeting with us to walk through your initial results

Now relax and explore Actifile while audit completes on your laptop (typically 20 – 90 mins).

- At the bottom right of moist screens are quick tutorials on Actifile.
- Browse through the various sections in the Actifile portal to understand how your data is being monitored.
- *Important: **Avoid saving changes** unless you fully understand the impact of those settings.*

CRITICAL: DO NOT TURN ON ENCRYPTION - TALK TO US BEFORE ENCRYPTING YOUR DATA. Consider running Actifile in monitoring mode for 1–3 months before turning on encryption. This way, we can identify applications and websites that may need access to encrypted data. This can be reduced to a few days if required. **Book a meeting here.**



Frequently Asked Questions (FAQ)

Q1. We don't have private or sensitive data. Why should we use Actifile?

You'd be surprised! Many organisations unintentionally have/store more sensitive, regulated, or private data than they realise. Common examples include:

- Downloaded reports from ERP, CRM, cloud, or finance systems.
- Email attachments, spreadsheets, or customer information.
- Folders or files containing passwords – for hackers, these are the 'keys to the kingdom'.

Actifile helps uncover and secure this data. Contact us for a complimentary Data Risk Assessment to discover and quantify sensitive data at risk in your organisation. Almost all businesses hold regulated data but may not realise it until it is too late and that data is stolen.

Q2. Why do we need Actifile if we only use cloud applications?

Even with cloud-based applications, endpoints like laptops can inadvertently store sensitive data from downloads, email attachments, or offline activities. These endpoints often become prime targets for hackers.

Actifile identifies and secures these hidden risks, helping ensure you:

- Minimise exposure to regulatory fines and penalties.
- Protect your organisation's reputation in the event of a data breach.

Cloud security isn't enough on its own if endpoint and network vulnerabilities aren't addressed.

Q3. What if we don't have a budget for additional tools?

Good news! Actifile offers a **free initial data risk assessment** for a limited number of devices. This assessment helps you determine:

- Whether your endpoints store sensitive or regulated data and its value.
- Which devices pose the highest risk for data exposure.
- If you are breached, what your risk exposure is in dollar terms.

Plus, implementing Actifile's Breach Minimisation solution is highly cost-effective, typically requiring just **1–3%** of your total estimated data risk value. It's a small investment for significant peace of mind.

Next Steps:

1. Install and discover how easy Actifile is.
2. **Book a Demo** to learn more about how Actifile works for your organisation. Schedule here: Book a Demo.
3. For questions or support, reach out to the Actifile team anytime: support@actifile.com

Reach out to our local Australian team with any sales questions or assistance during deployment:

- Greg Wyman (sales, demo, and technical): 0402 259 359
- Actifile Knowledgebase or log a technical support (tell them your account name (top left) and that you are in the AU region and explain the issue and include screen shots to help explain your issue – or just call me Greg 0402 259 359).