



Intelligent Ally

Frequently asked questions

Date: September 2026 Version: 1.0

Transvault is a trademark of Transvault Software Ltd

This document contains proprietary and confidential information and may not be shared with any 3rd party without the express written permission of Transvault.

IMPORTANT: The information in this document is to act as a guide only. Transvault shall not be liable for technical or editorial errors or omissions contained herein. No warranties of any kind are made, including the accuracy of the information contained herein, or whether this information reflects the latest capability of the technology referenced.

Contents

1. General Overview	3
1.1. What is Intelligent Ally?	3
1.2. Why would my company need Intelligent Ally?	3
1.3. Which Sources and Targets are supported?	3
1.4. Do you have a SaaS version of Intelligent Ally?	4
1.5. What compliance standards does Intelligent Ally support?	4
2. Architecture & Deployment	4
2.1. What are the technical requirements for Intelligent Ally?	4
2.2. What is Intelligent Ally Shield?	5
2.3. What permissions and access are required to deploy and use Intelligent Ally?	5
2.4. Can you deploy Intelligent Ally on a non-Windows based environment?	5
2.5. Can you deploy Intelligent Ally on Cloud-based servers?	5
2.6. Can Intelligent Ally use Active Directory in Azure (Entra ID) when installed in an On-premises environment?	5
2.7. How long does end to end deployment typically take?	6
2.8. Do I need Services to deploy and use Intelligent Ally?	6
3. Data Handling & Privacy	6
3.1. What data does Intelligent Ally process?	6
3.2. How is captured data used and stored?	6
3.3. When using Intelligent Ally, will any of our data leave our secure environment?	7
3.4. How long is the captured data held for?	7
3.5. Who can access the captured data?	7
3.6. Does Intelligent Ally capture the source of the AI generated data?	7
3.7. If images and files are generated as part of the prompt response, are these also captured by Intelligent Ally?	7
3.8. How can I see the data that is being captured?	8
3.9. How do I verify the software is capturing correctly?	8
3.10. What information is stored in the Intelligent Ally database?	8
4. Integration & Compatibility	9

4.1.	Are Generative-AI prompts and responses still captured when working remotely? (For example, when using a VPN)	9
4.2.	Are Microsoft 365 Copilot interactions in Word, Excel and other Microsoft 365 applications captured?	9
4.3.	Can we export data for analysis?	9
4.4.	In what format is the captured data presented in the target mailbox?	9
5.	Administration and Monitoring	10
5.1.	Does Intelligent Ally have the ability to block access to a chatbot that is not on your supported list?	10
5.2.	If you use a personal Generative-AI subscription on your corporate device, will your usage be tracked by Intelligent Ally?	10
5.3.	Is an individual message generated for each prompt and each response? 10	
6.	Licensing & Support.....	10
6.1.	How much does it cost to use Intelligent Ally?	10
6.2.	How do we increase our Intelligent Ally licensing quota?	10
6.3.	How does Intelligent Ally licensing work?	11
6.4.	How do I get technical support for Intelligent Ally?	11
6.5.	What are the SLA's for Incident response and resolution?	11
6.6.	Where can I find your product documentation?	11
6.7.	How do I request a demonstration of Intelligent Ally?	12
6.8.	How can we make product feature or improvement suggestions?	12
6.9.	Do you have a public roadmap available?	12

1. General Overview

1.1. What is Intelligent Ally?

Transvault Intelligent Ally is a secure AI-governance platform that gives companies complete visibility and control over how generative AI is used across their workforce. As employees increasingly turn to AI tools to perform their roles, businesses face mounting risks — sensitive data leaving the perimeter, regulatory exposure, and a lack of insight into what data is being shared with which services, by whom, and how frequently.

Purpose-built for regulated industries and suitable for companies of all sizes, Intelligent Ally delivers the oversight needed to meet legal, audit and regulatory obligations, supporting compliance with ISO 42001, GDPR, FINRA and HIPAA.

1.2. Why would my company need Intelligent Ally?

Intelligent Ally can help your company deliver:

- Regulatory compliance requiring audit trails of AI interactions
- Data loss prevention and sensitive information monitoring
- Understanding AI usage patterns across teams
- Cost attribution and chargeback for AI services
- Training and quality assurance purposes
- Incident investigation and forensics

1.3. Which Sources and Targets are supported?

Intelligent Ally currently supports prompts/responses from:

- Anthropic Claude
- Google Gemini
- Microsoft Copilot (consumer)
- Microsoft 365 Copilot
- Mistral AI
- OpenAI ChatGPT

And the retention of that data with direct ingestion into:

- Arctera Enterprise Vault (Exchange Journal)
- Microsoft 365 (Primary or Archive mailboxes)
- Proofpoint

1.4. Do you have a SaaS version of Intelligent Ally?

Currently, Intelligent Ally is only available as an On-premises solution; however a SaaS version is under active consideration. If you would be interested in using a SaaS version, please send us an expression of interest to: Products@Transvault.com

1.5. What compliance standards does Intelligent Ally support?

Intelligent Ally is designed to support organisations in meeting a range of regulatory and compliance obligations. The platform provides the governance controls, audit trails and data handling capabilities needed to demonstrate adherence to frameworks including:

- ISO 42001 (AI Management Systems)
- UK GDPR and EU GDPR
- FINRA (Financial Industry Regulatory Authority)
- HIPAA (Health Insurance Portability and Accountability Act)
- EU AI Act
- FCA requirements for financial services firms
- SRA Code of Conduct for legal practices

Intelligent Ally does not itself hold a compliance certification, but it is built to provide the controls and evidence that organisations need to satisfy their own compliance obligations under these frameworks.

2. Architecture & Deployment

2.1. What are the technical requirements for Intelligent Ally?

Whilst dependent on the volume of your Generative AI interactions, currently the minimum requirement to run Intelligent Ally is a single Microsoft Windows Server (version 2019 and above).

The specification for this server will again vary depending on the volume of your daily AI interactions, but as a minimum we recommend the following, alongside a 1Gbps network connection:

- **CPU:** 4 vCPU
- **Memory:** 16GB RAM
- **Disk Space:** 150GB (OS + Application + Database)

In our current release, all components (application services and databases) are installed on a single server, in future releases, database components will optionally be deployable on a separate server to support scale-out and larger environments.

Additional components or features (such as Intelligent Ally Shield) may have separate or enhanced infrastructure requirements, which are covered in the relevant implementation guidance.

2.2. What is Intelligent Ally Shield?

Intelligent Ally Shield is an add-on module that provides PII (Personally Identifiable Information) detection capabilities. It scans prompts and responses in real time to identify sensitive personal data, helping organisations to enforce data loss prevention policies and meet regulatory requirements such as GDPR and HIPAA.

Shield focuses on text-based interactions and integrates with the wider Intelligent Ally platform to enhance visibility and control over AI usage.

For further details, please refer to the Intelligent Ally product documentation or contact your Account Manager.

2.3. What permissions and access are required to deploy and use Intelligent Ally?

Please see our **Pre-requisites** and **Implementation** Guides for detailed information on all requirements to deploy and use Intelligent Ally within your environment.

2.4. Can you deploy Intelligent Ally on a non-Windows based environment?

Currently, Intelligent Ally is only supported on Windows-based systems, however, our product team are reviewing the potential to extend support to non-Windows systems.

2.5. Can you deploy Intelligent Ally on Cloud-based servers?

Yes, Intelligent Ally can be deployed on cloud-based virtual machines (e.g. Azure), provided they meet the documented system requirements.

2.6. Can Intelligent Ally use Active Directory in Azure (Entra ID) when installed in an On-premises environment?

Yes. Intelligent Ally can integrate with Microsoft Entra ID (formerly Azure Active Directory) in hybrid environments. This allows organisations to use cloud-based identity services alongside an

on-premises deployment of Intelligent Ally, depending on their configuration and identity management approach.

2.7. How long does end to end deployment typically take?

Typically one day for initial setup, depending on environment complexity.

2.8. Do I need Services to deploy and use Intelligent Ally?

Whilst of course you could look to use 3rd party services to support the deployment and use of Intelligent Ally, there is no specific requirement to do so. Transvault has developed a package of product resources to support the successful delivery of those activities by your own IT personnel. However, should you wish to procure professional services to undertake those tasks, our Sales team would be happy to discuss that with you.

3.Data Handling & Privacy

3.1. What data does Intelligent Ally process?

When you use Intelligent Ally, we may process the following data:

- Messages you send to supported Gen AI tools and the responses you receive.
- Basic metadata such as timestamps, application name, and user identifiers.
- Files or attachments you upload, where capture is enabled.

Intelligent Ally does not modify the content of your messages.

3.2. How is captured data used and stored?

Your data is processed to:

- Capture and archive Gen AI interactions for compliance and audit purposes.
- Apply policy controls such as content filtering or data loss prevention.
- Support investigations, reporting, and operational troubleshooting.

Intelligent Ally does not use your data to train AI models.

Captured data is stored securely within your organisation's configured environment or approved storage location.

Access to stored data is restricted to authorised users and systems only.

3.3. When using Intelligent Ally, will any of our data leave our secure environment?

Intelligent Ally processes and stores captured interactions within your organisation's configured environment. It does not send captured prompt or response content to Transvault as part of normal operation. Users' prompts and other data submitted to AI services are still sent to those providers in accordance with your organisation's configuration.

The only outbound communication is to the Transvault licensing server, which transmits encrypted licence validation metadata (such as licence status and usage counts). No message content or personally identifiable information is included in this communication.

3.4. How long is the captured data held for?

Captured data is typically stored in your configured target systems (such as archive mailboxes or external platforms), where retention is fully controlled and managed by your organisation.

Intelligent Ally also maintains a temporary internal recovery store to support processing and resilience. Data in this store is retained for a configurable period of up to 90 days, after which it is automatically removed.

3.5. Who can access the captured data?

Access is limited to authorised administrators, compliance teams, or systems acting on behalf of your organisation. Transvault staff do not access client data, unless explicitly authorised for support or operational purposes.

3.6. Does Intelligent Ally capture the source of the AI generated data?

Intelligent Ally captures the source application used for each interaction (for example, ChatGPT, Microsoft Copilot, Claude, or Gemini), along with associated metadata such as timestamps and user context.

It largely will not determine or verify the underlying sources used by the AI model to generate its responses, as this information is not typically exposed by the AI providers.

3.7. If images and files are generated as part of the prompt response, are these also captured by Intelligent Ally?

Yes. For supported Generative AI tools, Intelligent Ally captures files, images, and generated artefacts alongside relevant metadata, supporting compliance, investigation, and audit requirements.

Any known limitations in capture are documented in the release notes available in the support portal.

3.8. How can I see the data that is being captured?

The data being captured will be stored in your target archive mailbox, accessible using an appropriate email client.

3.9. How do I verify the software is capturing correctly?

You can verify that Intelligent Ally is capturing data correctly by reviewing captured interactions in your configured target system (such as archive mailboxes or external platforms), where prompts and responses are stored.

In addition, system logs and monitoring tools can be used to confirm that processing is occurring as expected and to identify any errors or interruptions.

We recommend validating capture during initial deployment and after any configuration changes to ensure expected behaviour.

3.10. What information is stored in the Intelligent Ally database?

The Intelligent Ally database stores operational and configuration data required for the platform to function. This includes system configuration, processing state, audit logs, and metadata related to captured interactions (such as timestamps, application identifiers, and user context).

Captured prompt and response content is also temporarily stored within Intelligent Ally as part of its internal recovery store, for a configurable period of up to 90 days, to support processing and resilience.

Where applicable, Intelligent Ally may also store detection-related data (for example, policy matches or identified sensitive information) to support monitoring, reporting, and governance features.

Captured prompt and response content is primarily stored in your configured target systems. Intelligent Ally does not use client data to train AI models.

4. Integration & Compatibility

4.1. Are Generative-AI prompts and responses still captured when working remotely? (For example, when using a VPN)

Yes, provided traffic is routed via the configured Intelligent Ally deployment.

If your organisation's VPN or remote access solution directs web traffic through your corporate network, interactions with supported AI tools will continue to be captured as normal.

If traffic bypasses this route (for example, due to split tunnelling), some interactions may not be captured. We recommend reviewing remote access configuration to ensure relevant traffic is routed through Intelligent Ally.

4.2. Are Microsoft 365 Copilot interactions in Word, Excel and other Microsoft 365 applications captured?

Intelligent Ally captures supported Microsoft 365 Copilot chat interactions, including chats accessed within Microsoft 365 applications. This does not mean every Copilot action or generated result within those applications is captured. The release notes for the installed version describe the supported experiences and any known limitations.

4.3. Can we export data for analysis?

Captured data can be accessed and exported for analysis via your configured target systems (such as archive mailboxes or external platforms), where the data is stored in standard formats.

This allows organisations to use their existing tools for search, eDiscovery, reporting, and analysis. Additional export and reporting capabilities within Intelligent Ally may vary depending on configuration and feature set.

4.4. In what format is the captured data presented in the target mailbox?

Archived chatbot interactions are output as HTML-based MSG items.

5. Administration and Monitoring

5.1. Does Intelligent Ally have the ability to block access to a chatbot that is not on your supported list?

Yes. Administrators can add third-party AI providers to a blocking list to prevent access to those providers through the configured Intelligent Ally controls. A provider does not need to be supported for conversation capture to be blocked.

Blocking an unsupported provider does not enable capture of its prompts and responses. Capture remains limited to the supported AI experiences.

5.2. If you use a personal Generative-AI subscription on your corporate device, will your usage be tracked by Intelligent Ally?

Yes, activity may still be captured when using supported tools on a corporate-managed device. Intelligent Ally captures interactions based on traffic routed through its proxy, regardless of whether the user is signed into a personal or corporate AI account.

5.3. Is an individual message generated for each prompt and each response?

By default, Intelligent Ally generates a single message containing both the prompt and the corresponding response for each interaction.

Configuration options are available to control this behaviour, allowing organisations to capture prompts only, responses only, or both, depending on their requirements.

6. Licensing & Support

6.1. How much does it cost to use Intelligent Ally?

Pricing for Intelligent Ally is tailored to each organisation's requirements. Please contact your Transvault Sales representative or email: sales@transvault.com for a detailed quote.

6.2. How do we increase our Intelligent Ally licensing quota?

Please contact your Transvault Sales representative who will be happy to discuss and arrange any additional requirements with you.

6.3. How does Intelligent Ally licensing work?

Intelligent Ally is licensed on a per-user subscription basis. Licences are typically billed annually and cover the features included in your subscription tier.

The Intelligent Ally application communicates with a Transvault licensing server to validate your licence.

This communication is encrypted and transmits only licence validation metadata (such as licence status and usage counts). No client data, prompts, responses, or personally identifiable information is sent to the licensing server.

Licence validation is performed during normal operation. In the event that the licensing server is temporarily unavailable, Intelligent Ally is designed to allow continued operation for a defined grace period. Please refer to your licence agreement for specific details.

6.4. How do I get technical support for Intelligent Ally?

As a Transvault client, you will be provided with access to our Support Centre. The Support Centre offers a knowledge base, product documentation, software downloads, and ticket management, available 24 hours a day, 7 days a week.

Our technical support team is available Monday to Friday, between 09:00 and 20:30 (GMT/BST). Reduced hours may apply during UK public holidays (excluding the Christmas and New Year period, when our offices are closed).

If further assistance is required, our support team will work with you to investigate and resolve any issues. [Visit the Transvault Intelligent Ally Support Centre](#)

6.5. What are the SLA's for Incident response and resolution?

Transvault operates a five-tier priority system (P1 to P5) for support tickets, ranging from critical service outages to general enquiries and feature requests.

The priority level assigned to a ticket should reflect the business impact of the issue.

Response and resolution targets for each priority level are defined in your Support Agreement. Please refer to your agreement documentation or contact your Account Manager for further details.

6.6. Where can I find your product documentation?

All Intelligent Ally product documentation is available via the customer support portal:

[Visit the Transvault Intelligent Ally Support Centre](#)

6.7. How do I request a demonstration of Intelligent Ally?

Please contact our sales team at sales@transvault.com or visit: <https://www.transvault.com/software/transvault-intelligent-ally/> to schedule a demonstration.

6.8. How can we make product feature or improvement suggestions?

Should you have a suggestion for a new product feature or an improvement to an existing feature, please let us know at: product@transvault.com and we will only be too happy to hear your feedback.

6.9. Do you have a public roadmap available?

We do not currently publish a public product roadmap. However, we actively gather feedback from clients and partners to inform our development priorities. If you would like to discuss upcoming features or share input on the product direction, please contact your Account Manager or email: product@transvault.com.