AiX Enterprise Platform Documentation

v2026.3

DDX Business Solutions Limited

Customer Reference

Table of Contents

Home

title: AiX Documentation product: AiX owner: DDX Business Solutions Limited

AiX Documentation

Welcome to the official product documentation for **AiX**, the enterprise AI and automation platform from **DDX Business Solutions Limited**.

AiX helps organizations apply AI to business processes, documents, knowledge, and workflows while maintaining control over their data, infrastructure, and AI models.

Your AI. Your Data. Your Control.

Explore AiX

Whether you are a business user, administrator, AI specialist, or technical team member, this documentation provides the information you need to use, configure, deploy, and operate AiX.

Getting Started

Learn the fundamentals of AiX and get familiar with the platform, its capabilities, and key concepts.

User Guide

Learn how to use AiX features including Chat, Knowledge Base, Assistants, Smartflow, scheduling, and other business-user capabilities.

Administration

Configure users, access permissions, authentication, platform settings, and other administrative functions.

AI Model Management

Configure and manage the AI models used by AiX, including locally hosted and supported external models.

Operations & Maintenance

Guidance for operating, monitoring, maintaining, backing up, and supporting an AiX environment.

Architecture

Understand the AiX platform architecture, components, services, and how they work together.

Deployment

Learn about AiX deployment options for cloud, on-premises, hybrid, and local environments.

Integration

Learn how AiX connects with enterprise systems, data sources, identity providers, messaging platforms, and external services.

Security

Understand AiX security architecture, access controls, audit capabilities, data protection, and deployment security considerations.

Troubleshooting

Find guidance for diagnosing and resolving common configuration, deployment, integration, and operational issues.

Upgrade & Migration

Guidance for upgrading AiX installations and migrating between supported releases or deployment configurations.

Release Notes

Review new features, improvements, fixes, and other changes introduced in each AiX release.

Designed for Enterprise AI

AiX is designed to provide organizations with flexibility in how AI is deployed and used.

It supports:

- **Cloud, on-premises, hybrid, and local deployment**
- **Local and external AI models**
- **Enterprise knowledge and document processing**
- **No-code AI workflow automation with Smartflow**
- **Role-based access and governance**
- **Auditability of user and AI interactions**
- **Integration with enterprise systems and data sources**

AiX does not require organizations to train their own AI models. Instead, organizations can select and configure appropriate supported models according to their business, security, infrastructure, and governance requirements.

Documentation Versions

AiX documentation is maintained alongside product releases.

When working with a production environment, refer to the documentation version corresponding to the installed AiX release, as features and configuration options may change between versions.

Download Documentation

Prefer an offline or printable copy?

Download AiX Documentation (PDF)

The PDF contains the complete product documentation for this release and is generated from the same documentation source as this website.

About DDX Business Solutions

AiX is developed by **DDX Business Solutions Limited**.

Our goal is to make enterprise AI practical, affordable, governed, and sustainable — enabling organizations to adopt AI while maintaining control over their data, infrastructure, and technology choices.

1. Getting Started

1.1 Overview

■# Getting Started with AiX

Welcome to **AiX**, an enterprise AI and automation platform designed to make Artificial Intelligence practical and accessible for business users.

AiX brings AI models, organizational knowledge, reusable AI Assistants, workflow automation, and business processes together within a single platform.

This Getting Started guide introduces the main AiX capabilities and helps you understand where to begin.

What is AiX?

AiX enables organizations to use AI within their own business environment while maintaining control over their data, AI models, access, and business processes.

Rather than providing only a conversational AI interface, AiX allows AI to become part of everyday business activities.

With AiX, you can:

- Interact with AI models through **Chat**
- Ask questions using organizational information with **Knowledge Base**
- Use purpose-built AI experiences with **Assistants**
- Build and run automated business processes with **Smartflow**
- Automatically execute processes with **Scheduler**
- Work with documents, files, and enterprise information
- Incorporate human review and approval into AI-assisted processes

The capabilities available to you depend on your organization's AiX configuration and your access permissions.

AiX at a Glance

AiX provides several capabilities that work independently or together.

Chat

Chat is the simplest way to start using AiX.

Ask questions, generate content, analyze information, work with documents, and interact directly with the AI models available to you.

Start here if: you want to interact directly with AI.

Knowledge Base

Knowledge Base allows AI to work with organizational information.

AiX retrieves relevant information from approved documents and information sources and provides it to the AI model as context for answering your questions.

Start here if: you want answers based on your organization's information.

Assistants

Assistants provide reusable AI experiences designed for specific business purposes.

An Assistant can combine predefined instructions, an AI model, organizational knowledge, and other configured capabilities.

Start here if: you have a specific recurring task that benefits from a consistent AI experience.

Smartflow

Smartflow is AiX's no-code workflow and AI orchestration capability.

It allows AI, content, business rules, integrations, and human activities to be combined into repeatable business processes.

Start here if: you want to automate a multi-step business process.

Scheduler

Scheduler allows supported AiX processes to run automatically at defined times or intervals.

Start here if: you want an AiX process to execute automatically.

Understanding the AiX Approach

The AiX capabilities build on each other.

A simple way to think about them is:

Chat Ask AI.

↓

Knowledge Base Ask AI using organizational knowledge.

↓

Assistants Create a purpose-built AI experience.

↓

Smartflow Turn AI activities into a repeatable business process.

↓

Scheduler Run that process automatically.

You do not need to use every capability. Start with the feature that best matches what you want to accomplish.

A Simple Example

Consider a business process for reviewing incoming documents.

With **Chat**, you could upload a document and ask AI to summarize it.

With **Knowledge Base**, you could compare the document against your organization's policies or procedures.

With an **Assistant**, you could provide users with a predefined Document Review Assistant that follows consistent review instructions.

With **Smartflow**, you could create a process that automatically reads the document, extracts important information, performs an AI review, requests human review, and generates a standardized report.

With **Scheduler**, the process could be executed automatically at a defined time or interval where appropriate.

AiX allows organizations to start with simple AI interactions and progressively introduce structured automation as requirements develop.

Working with AI Models

AiX can support different AI models depending on your organization's environment and configuration.

The models available to you are managed by your organization.

As a user, you generally do not need to understand how an AI model is deployed. Simply select an available model where a choice is provided and use the model appropriate for your task.

For information about configuring and managing models, refer to **AI Model Management**.

Working with Enterprise Information

AiX can work with documents, files, and information made available by your organization.

Depending on your environment and permissions, this information may be used through Knowledge Bases, Assistants, Smartflows, or other AiX capabilities.

Access to information remains subject to the permissions and configuration established by your organization.

Human Oversight

AI can assist with analysis, content generation, information retrieval, and business process automation, but AI-generated results should be reviewed appropriately.

AiX supports human involvement within AI-assisted processes, including review and approval activities where required.

For important business activities, users should verify AI-generated information against authoritative sources and follow their organization's applicable policies and procedures.

Access and Permissions

What you see in AiX depends on your role and permissions.

Some users may primarily use existing Chats, Knowledge Bases, Assistants, and Smartflows.

Other users may have additional permissions to create, configure, publish, or manage these capabilities.

System administrators have additional responsibilities for platform configuration, users, access, integrations, and other administrative functions.

Refer to the **Administration** documentation for administrative activities.

Where to Go Next

If you are using AiX for the first time, continue with the remaining **Getting Started** topics to learn how to access and navigate the platform.

When you are ready to begin using individual AiX capabilities, continue to the **User Guide**.

The User Guide provides detailed instructions for:

- Chat
- Knowledge Base
- Assistants
- Smartflow
- Scheduler

For technical and operational topics, refer to the appropriate **Administration**, **AI Model Management**, **Operations & Maintenance**, **Architecture**, **Deployment**, **Integration**, or **Security** sections of the documentation.

Download Documentation

Prefer an offline or printable copy of this section?

Download Getting Started (PDF)

The PDF contains the complete Getting Started documentation for this release and is generated from the same documentation source as this website.

1.2 Quick Start

This Quick Start introduces the main AiX capabilities through a few simple activities.

You do not need to complete every activity. The features available to you depend on your organization's configuration and your access permissions.

1. Start a Chat

The quickest way to begin using AiX is with **Chat**.

1. Open **Chat** from the AiX navigation menu.
2. Select an available AI model if required.
3. Enter a question or instruction.
4. Select **Send** or press **Enter**.

For example:

> Summarize the key considerations when introducing AI into a business process.

You can continue the conversation with a follow-up question:

> Present this as five recommendations for management.

AiX uses the previous conversation as context when responding to follow-up questions.

For more information, see **User Guide** → **Chat**.

2. Work with a Document

Where file upload is available, you can provide a document as part of your conversation.

1. Start or open a Chat.
2. Add a supported document.
3. Enter an instruction describing what you want AiX to do.
4. Submit your request.
5. Review the response.

For example:

> Summarize this document and identify the key actions, dates, and decisions.

You can then continue with questions about the document:

> Which actions require management attention?

Always review important information against the original document before using AI-generated results for business decisions.

3. Ask a Knowledge Base

Use **Knowledge Base** when you want answers based on information provided by your organization.

1. Open **Knowledge Base**.
2. Select a Knowledge Base available to you.
3. Enter your question.
4. Submit the question.
5. Review the response and available source references.

For example:

> What is the approval process described in our procurement policy?

AiX searches for relevant information within the selected Knowledge Base and provides that information to the AI model as context.

Where references are available, review the original source when the information is important.

For more information, see **User Guide** → **Knowledge Base**.

4. Use an Assistant

Assistants provide AI experiences configured for a particular task or business purpose.

1. Open **Assistants**.
2. Select an Assistant available to you.
3. Enter your question or provide the requested information.
4. Submit your request.
5. Review the response.

Unlike general Chat, an Assistant already contains instructions that guide how the AI should perform its task.

For example, a Document Review Assistant might already know how your organization expects documents to be reviewed and how the results should be presented.

For more information, see **User Guide** → **Assistants**.

5. Run a Smartflow

Smartflow allows you to execute a predefined business process.

1. Open **Smartflow**.
2. Select a Smartflow available to you.
3. Review its description and required inputs.
4. Provide the requested information or files.
5. Select **Run**.
6. Monitor the execution.
7. Review the generated results.

A Smartflow may perform several activities automatically.

For example:

Document → Read Content → AI Analysis → Human Review → Generate Report

Some Smartflows may pause and wait for a user to review information or perform an action before continuing.

For more information, see **User Guide → Smartflow**.

6. Review Your Results

Whether you are using Chat, Knowledge Base, Assistants, or Smartflow, remember that AI-generated information should be reviewed appropriately.

For important business information:

- Verify facts against authoritative sources.
- Review important names, dates, figures, and calculations.
- Check source references where available.
- Confirm that the result addresses your intended task.
- Apply human review or approval where required.

AI should assist your business process rather than replace appropriate business judgement and controls.

Choosing the Right AiX Capability

If you are unsure where to start, use this simple guide:

| I want to... | Use | | ---------- | ---------- | | Ask AI a general question | **Chat** | | Analyze or summarize a document | **Chat** | | Ask questions using organizational information | **Knowledge Base** | | Perform a predefined conversational AI task | **Assistant** | | Execute a repeatable multi-step process | **Smartflow** | | Run a process automatically at a defined time | **Scheduler** |

What's Next?

You have now seen the main ways of working with AiX.

Continue to the **User Guide** for detailed instructions on each capability.

If you create or manage AiX capabilities, the User Guide also explains how to work with Knowledge Bases, Assistants, Smartflows, and Schedules according to your permissions.

Platform administrators and technical teams should refer to the **Administration**, **AI Model Management**, **Operations & Maintenance**, **Architecture**, **Deployment**, **Integration**, and **Security** sections.

2. User Guide

2.1 Overview

■# User Guide Overview

AiX is an enterprise AI and automation platform designed to help business users apply Artificial Intelligence to everyday business activities, documents, information, and processes.

AiX brings AI, enterprise knowledge, workflow automation, and business applications together within a single platform. Depending on the features enabled by your organization, you can use AiX to interact with AI models, work with organizational knowledge, automate business processes, and execute reusable AI-powered tasks.

What You Can Do with AiX

AiX provides several capabilities that can be used independently or combined to support business processes.

Chat

Use **Chat** to interact directly with available AI models.

You can ask questions, analyze information, generate or refine content, and work with documents made available during the conversation.

The AI models available to you are determined by your organization's AiX configuration.

Knowledge Base

A **Knowledge Base** allows you to ask questions using information provided by your organization.

Knowledge Bases can contain documents and other approved information sources. AiX retrieves relevant information from these sources and provides it to the AI model as context when answering your questions.

Where available, references to the source information can be included with the response to help you review and verify the answer.

Assistants

Assistants provide predefined AI experiences for particular tasks or business purposes.

An Assistant can combine instructions, AI models, Knowledge Bases, and other configured capabilities so that users can perform a task without repeatedly defining the same prompts or settings.

Smartflow

Smartflow is AiX's no-code workflow and AI orchestration capability.

Smartflows allow business processes to be represented as a sequence of connected steps. A Smartflow can combine AI processing with documents, data, business rules, integrations, and human review.

Depending on your permissions, you may be able to run existing Smartflows or create and modify your own.

Scheduler

The **Scheduler** allows supported AiX processes to run automatically at defined times or intervals.

For example, a Smartflow may be scheduled to process information every morning, generate a regular report, or perform another recurring business activity.

Working with AiX

A typical AiX activity may involve several capabilities working together.

For example, you might use a Knowledge Base to provide trusted organizational information, an AI model to analyze that information, and a Smartflow to automate the overall process.

AiX can also support human review and approval steps where business processes require additional oversight.

This allows AI to become part of a controlled business process rather than operating as a standalone tool.

Your Access

The features, AI models, Knowledge Bases, Assistants, Smartflows, and information available to you depend on the access permissions configured by your organization.

Some users may primarily use existing AI applications and workflows, while other users may have permission to create, configure, or manage them.

Administrative and platform configuration activities are covered separately in the **Administration** section of the AiX documentation.

Getting Started

If you are new to AiX, a good starting point is to become familiar with **Chat**, followed by **Knowledge Base**, **Assistants**, and **Smartflow**.

The following sections of this User Guide explain how to use each capability and provide examples of common tasks.

Download Documentation

Prefer an offline or printable copy of this section?

Download User Guide (PDF)

The PDF contains the complete User Guide documentation for this release and is generated from the same documentation source as this website.

2.2 Chat

Chat provides a conversational interface for interacting with AI models available within AiX.

You can use Chat to ask questions, analyze information, create and refine content, summarize documents, explore ideas, and perform other AI-assisted tasks using natural language.

The AI models available in Chat are determined by your organization's AiX configuration.

Starting a Chat

To start a new conversation:

1. Open **Chat** from the AiX navigation menu.
2. Select an available **AI Model**.
3. Enter your question or instruction in the message box.
4. Select **Send** or press **Enter** to submit your message.

AiX sends your request to the selected AI model and displays the response within the conversation.

You can continue asking questions within the same conversation. Previous messages provide conversational context that can help the AI understand follow-up questions.

Selecting an AI Model

Depending on your organization's configuration, more than one AI model may be available.

Different models may be suitable for different types of tasks, such as:

- General questions and content generation
- Reasoning and analysis
- Document understanding
- Coding and technical tasks
- Multilingual content

Select the model appropriate for your task before submitting your message.

The models available to you depend on your organization's configuration and access permissions.

Asking Questions

You can communicate with AiX using normal language.

For better results, provide clear instructions and include relevant context about what you want the AI to do.

For example:

> Summarize the key points from this document for a management audience.

Or:

> Review this text and identify the main risks, assumptions, and recommended actions.

You can also continue the conversation with follow-up instructions such as:

> Make the summary shorter.

> Explain the second point in more detail.

> Present the findings as a table.

Working with Files

Where enabled, you can provide files or documents as part of your conversation.

AiX can use the content of supported files together with your instructions to perform tasks such as:

- Summarizing a document
- Extracting important information
- Comparing documents
- Identifying key topics
- Answering questions about document content
- Creating or transforming content

The supported file types and maximum file sizes may depend on your organization's AiX configuration.

Conversation Context

Messages within the same Chat conversation provide context for subsequent messages.

For example, after asking AiX to summarize a document, you can continue with:

> What are the three most important findings?

AiX can use the preceding conversation when responding to the follow-up question.

For a different task or topic, consider starting a **New Chat** to avoid unrelated conversation context affecting the response.

Reviewing AI Responses

AI-generated responses should be reviewed before they are used for important business decisions or activities.

AI models can occasionally produce incomplete, inaccurate, or unexpected information.

When working with important business information, consider:

- Checking important facts against the original source
- Reviewing calculations and numerical information
- Verifying names, dates, and references
- Confirming that the response addresses your intended question

- Applying appropriate human review before using generated content

Chat and Enterprise Knowledge

Standard Chat interacts with the selected AI model using the information provided within the conversation.

When you need AI responses based on approved organizational documents or information, use an appropriate **Knowledge Base** or **Assistant** where available.

Knowledge Bases allow AiX to retrieve relevant organizational information and provide it to the AI model as additional context.

Chat History

AiX may retain your Chat conversations according to your organization's configuration and policies.

Previous conversations can be reopened where Chat history is available.

For a new or unrelated activity, start a new conversation rather than continuing an existing conversation.

Good Prompting Practices

You do not need to learn a special command language to use AiX. However, clear instructions generally produce better results.

A useful prompt usually explains:

Task — What you want AiX to do.

Context — Relevant background information.

Requirements — Any specific rules or constraints.

Output — How you want the result presented.

For example:

> Review the attached project update and prepare a management summary. Highlight the current status, major risks, outstanding decisions, and next actions. Keep the summary under 500 words and use headings for each section.

Next Steps

After becoming familiar with Chat, you may want to explore:

- **Knowledge Base** — Ask questions using organizational knowledge and documents.
- **Assistants** — Use predefined AI capabilities designed for particular tasks.
- **Smartflow** — Run or create AI-powered business workflows.

These capabilities extend Chat by combining AI with organizational information, reusable instructions, automation, and business processes.

2.3 Knowledge Base

Knowledge Base allows AiX to use your organization's documents and information when answering questions.

Instead of relying only on the general knowledge of an AI model, AiX can search the selected Knowledge Base for information relevant to your question and provide that information to the AI model as additional context.

This helps users work with organizational policies, procedures, manuals, reports, reference materials, and other business information through a conversational interface.

What is a Knowledge Base?

A Knowledge Base is a collection of information that AiX can search and use when responding to questions.

For example, an organization might create Knowledge Bases for:

- Human Resources policies
- Standard Operating Procedures (SOPs)
- Product documentation
- Customer service procedures
- Technical manuals
- Legal and compliance information
- Project documentation
- Internal policies and guidelines

Knowledge Bases can be created for a particular team, department, subject, or business purpose.

The Knowledge Bases available to you depend on your organization's configuration and your access permissions.

Using a Knowledge Base

To ask questions using a Knowledge Base:

1. Open **Knowledge Base** from the AiX navigation menu.
2. Select the Knowledge Base you want to use.
3. Enter your question.
4. Select **Send** or press **Enter**.
5. Review the response and any available source references.

AiX searches the selected Knowledge Base for information relevant to your question and uses the retrieved information as context for the AI model.

You can continue asking follow-up questions within the same conversation.

Asking Effective Questions

You can ask questions using normal language.

For example:

> What is the company's annual leave policy?

> What is the procedure for handling a customer complaint?

> Summarize the approval requirements described in the procurement policy.

> What documents are required before this process can be approved?

> Compare the requirements described in these procedures.

Specific questions generally help AiX identify the most relevant information.

If the initial response does not contain the information you need, you can refine your question or provide additional context.

For example:

> Only consider the requirements for permanent employees.

Or:

> Focus on the approval process described in the Finance Policy.

How Knowledge Base Answers Questions

When you submit a question, AiX identifies information within the Knowledge Base that may be relevant to your request.

The relevant information is then provided to the selected AI model as context for generating the response.

In simplified terms:

Your Question → **Search Knowledge Base** → **Retrieve Relevant Information** → **AI Model** → **Response**

This approach is commonly known as **Retrieval-Augmented Generation (RAG)**.

It allows the AI model to work with organizational information without requiring that information to be used to train the AI model.

Source References

Where available, AiX can provide references to the information used when generating a response.

References may identify information such as the source document, page, section, or other available source details.

Use these references to review the original information and verify important answers.

For business-critical activities, the original source document should remain the authoritative source.

Working with Multiple Documents

A Knowledge Base may contain many documents covering the same or related subjects.

When you ask a question, AiX searches across the available information to identify relevant content.

This allows you to ask questions that may require information from multiple documents.

For example:

> Summarize the approval requirements across these procedures.

Or:

> Are there any differences between the requirements described in the HR Policy and Employee Handbook?

The quality of the response depends on the information available within the Knowledge Base and the relevance of the information retrieved.

Creating a Knowledge Base

Depending on your permissions, you may be able to create and manage Knowledge Bases.

When creating a Knowledge Base, provide a clear name and description so that users understand its intended purpose.

For example:

Name: HR Policies

Description: Company policies and procedures relating to employees, leave, benefits, expenses, and workplace practices.

A clearly defined Knowledge Base makes it easier for users to select the appropriate source of information for their questions.

Adding Content

Depending on your organization's configuration, content can be added or made available to a Knowledge Base from supported information sources.

These may include documents and enterprise content locations configured for AiX.

When adding content, consider whether the information is:

- Relevant to the purpose of the Knowledge Base
- Current and authoritative

- Appropriate for the intended users
- Free from unnecessary duplicate or outdated versions
- Organized clearly enough for users to identify the original source

Maintaining good source information improves the usefulness of the Knowledge Base.

Updating Knowledge

Organizational information changes over time.

Policies may be revised, procedures may be replaced, and new documents may become authoritative.

Knowledge Base owners should periodically review the information available within their Knowledge Bases and ensure that outdated or superseded information is handled appropriately.

This helps reduce the possibility of users receiving answers based on information that is no longer current.

Access and Permissions

Access to Knowledge Bases is controlled by your organization's AiX configuration.

Depending on your permissions, you may be able to:

- Use a Knowledge Base
- Create a Knowledge Base
- Add or manage content
- Share a Knowledge Base with other users or teams
- Modify Knowledge Base settings

Users should only have access to Knowledge Bases and source information that they are authorized to use.

Knowledge Base and Chat

Chat provides a general-purpose conversation with an AI model using the information supplied within the conversation.

Knowledge Base adds organizational information that AiX can search and provide to the AI model when answering your question.

For example:

Chat

> Explain what an employee leave policy normally contains.

The AI model can provide a general answer based on its available knowledge.

Knowledge Base

> According

2.4 Assistants

Assistants provide reusable AI experiences designed for specific tasks, business functions, or areas of expertise.

An Assistant combines predefined instructions with an AI model and, where configured, organizational knowledge and other AiX capabilities. This allows users to perform common tasks consistently without having to recreate detailed prompts each time.

Examples of Assistants may include:

- HR Policy Assistant
- Customer Service Assistant
- Legal Document Assistant
- Sales Assistant
- Technical Support Assistant
- Internal Knowledge Assistant

The Assistants available to you depend on your organization's configuration and your access permissions.

Using an Assistant

To use an Assistant:

1. Open **Assistants** from the AiX navigation menu.
2. Select an Assistant available to you.
3. Enter your question or instruction.
4. Select **Send** or press **Enter** to submit your message.
5. Review the response and continue the conversation as required.

The Assistant automatically applies its configured instructions and other settings when processing your request.

You do not need to enter these instructions each time you use the Assistant.

Assistants and Chat

Chat provides a general-purpose interface for interacting directly with an available AI model.

An **Assistant** provides a more structured experience for a particular purpose.

For example, when using Chat you might need to provide detailed instructions explaining how a document should be reviewed.

An Assistant designed for document review can already contain those instructions, allowing you to simply provide the document and ask the Assistant to perform the review.

This makes Assistants useful for tasks that are performed repeatedly or where users should follow a consistent approach.

Assistant Instructions

Each Assistant can contain predefined instructions that guide how the AI should perform its task.

Instructions may define:

- The Assistant's purpose
- How information should be analyzed
- Business rules or guidelines to follow
- The expected tone or style
- Required response structure
- Restrictions or boundaries
- How results should be presented

These instructions are automatically applied when you interact with the Assistant.

Using Knowledge with an Assistant

An Assistant can be connected to one or more **Knowledge Bases** where configured.

This allows the Assistant to use approved organizational information when responding to questions.

For example, an HR Assistant could use an organization's HR policies and procedures to help answer employee questions.

When organizational knowledge is used, AiX retrieves relevant information and provides it to the AI model as additional context.

Where available, source references may also be provided so that users can review the information used to generate the response.

Working with Files

Where enabled, you can provide files to an Assistant as part of your request.

For example, you might provide a document and ask an Assistant to:

- Summarize the document
- Review its contents
- Extract specific information
- Identify issues or risks
- Compare information
- Prepare a structured response

The way files are processed depends on the purpose and configuration of the Assistant.

Conversation Context

An Assistant can maintain conversational context within the current conversation.

This allows you to ask follow-up questions without repeating all of the information from your previous messages.

For example:

> Summarize the key issues in this document.

You could then continue with:

> Which three issues require the most immediate attention?

Or:

> Present those issues in a table with recommended actions.

For a different task or topic, consider starting a new conversation with the Assistant.

Creating an Assistant

Depending on your permissions, you may be able to create your own Assistants.

When creating an Assistant, you can define its purpose and configure the capabilities required for the task.

Typical configuration may include:

- **Name** — A clear name describing the Assistant.
- **Description** — A short explanation of what the Assistant is designed to do.
- **AI Model** — The model used by the Assistant.
- **Instructions** — The rules and guidance provided to the AI.
- **Knowledge Base** — Organizational knowledge available to the Assistant.
- **Access** — Users or teams that can use the Assistant.

The configuration options available may vary depending on your organization's AiX configuration and your permissions.

Designing Effective Assistants

An effective Assistant should have a clearly defined purpose.

Rather than creating an Assistant that attempts to perform every possible task, consider creating Assistants for specific business activities.

For example:

General Assistant

> Help users with business questions.

This provides little guidance about how the Assistant should behave.

A more focused Assistant could be:

Contract Review Assistant

> Review business contracts and identify key obligations, important dates, commercial terms, risks, and items requiring further review. Present the findings using a consistent structured format.

Clear instructions help produce more predictable and reusable results.

Sharing Assistants

Depending on your permissions, Assistants may be private or shared with other users or teams.

Before sharing an Assistant, consider whether:

- Its purpose is clearly described
- Its instructions have been tested
- The appropriate AI model has been selected
- Required Knowledge Bases are connected
- Users have access to the required information
- Responses have been reviewed using representative examples

Shared Assistants can help organizations provide consistent AI capabilities across teams and business functions.

Reviewing Assistant Responses

Assistant responses are generated by AI models and should be reviewed appropriately before being used for important business activities or decisions.

Predefined instructions and organizational knowledge can improve consistency and relevance, but they do not guarantee that every response will be complete or accurate.

Important facts, calculations, dates, references, and business decisions should be verified where appropriate.

Assistants and Smartflow

Assistants and Smartflows serve different purposes.

Assistants are primarily conversational. They provide a reusable AI experience where users interact with AI through questions and follow-up messages.

Smartflows are process-oriented. They allow multiple steps, AI operations, business rules, integrations, document processing, and human activities to be combined into a workflow.

Use an Assistant when the activity is primarily conversational.

Use a Smartflow when the activity requires a repeatable sequence of processing steps or business actions.

Next Steps

You may also want to explore:

- **Chat** — Interact directly with available AI models.
- **Knowledge Base** — Work with organizational documents and information.
- **Smartflow** — Create and run AI-powered business workflows.
- **Scheduler** — Run supported processes automatically at defined times or intervals.

2.5 Smartflow

Smartflow is AiX's no-code workflow and AI orchestration capability.

It allows business users to create and run repeatable processes that combine AI, documents, data, business rules, integrations, and human activities within a visual workflow.

Instead of performing a series of AI tasks manually, Smartflow allows those activities to be organized into a controlled and reusable business process.

What is a Smartflow?

A Smartflow represents a business process as a sequence of connected steps.

Each step performs a specific activity and can pass its results to subsequent steps.

A Smartflow might:

- Read a document
- Extract information
- Ask an AI model to analyze the content
- Search a Knowledge Base
- Apply business rules
- Generate a report
- Request human review
- Send a notification
- Save or distribute the result

Simple Smartflows may contain only a few steps, while more advanced Smartflows can automate larger business processes.

How Smartflow Works

A Smartflow typically starts with an input, performs a series of processing steps, and produces one or more outputs.

For example:

Document → Read Content → AI Analysis → Human Review → Generate Report → Output

The output of one step can be used as the input to another step.

This allows complex processes to be built from smaller, reusable activities.

Running a Smartflow

To run an existing Smartflow:

1. Open **Smartflow** from the AiX navigation menu.
2. Select the Smartflow you want to use.
3. Review the description and any required inputs.
4. Provide the requested information or files.
5. Select **Run**.
6. Monitor the execution status.
7. Review the results when processing is complete.

Depending on the Smartflow, execution may complete automatically or pause while waiting for a user action, review, or approval.

The Smartflows available to you depend on your organization's configuration and your access permissions.

Smartflow Inputs

A Smartflow may require information before it can be executed.

Inputs can vary depending on the purpose of the Smartflow and may include:

- Documents or files
- Text
- User selections
- Parameters
- Dates or other values
- Information retrieved from configured systems

The Smartflow determines which inputs are required before execution can begin.

Smartflow Steps

Each Smartflow consists of one or more connected steps.

A step represents an activity performed during the workflow.

Depending on the capabilities configured by your organization, steps may perform activities such as:

- Reading content
- Processing documents
- Calling an AI model
- Asking questions about content
- Searching organizational knowledge
- Transforming information
- Applying business logic
- Creating documents or reports
- Interacting with external systems
- Sending messages or notifications
- Requesting human action

Each step can use information produced by earlier steps in the Smartflow.

Using AI in a Smartflow

AI processing can be included at different points within a Smartflow.

For example, an AI step might:

- Summarize a document
- Classify information
- Extract important details
- Identify risks or issues
- Compare information
- Generate recommendations
- Create structured content
- Prepare a report

Different AI models may also be used for different steps where appropriate.

The models available to Smartflow depend on your organization's AiX configuration.

Working with Content

Smartflow can process content as part of a business workflow.

For example, a Smartflow could receive a document, read its contents, analyze the information using AI, and generate a new document containing the results.

Content can therefore move through different stages of a workflow as it is processed.

A Smartflow may produce outputs such as:

- Documents
- Spreadsheets
- Presentations
- PDF files
- Structured data
- Text
- Reports
- Notifications

The available input and output formats depend on the tools and capabilities used by the Smartflow.

Human Review and Approval

Not every business process should operate entirely automatically.

Smartflow can include human activities within a workflow so that users can review information or make decisions at appropriate stages of the process.

Depending on the Smartflow and your permissions, you may participate as a reviewer or approver.

A workflow might, for example:

Receive Document → **AI Review** → **Human Review** → **Approval** → **Generate Final Output**

This allows AI-assisted processing to be combined with appropriate human oversight.

Smartflow Status

While a Smartflow is running, AiX tracks its execution status.

Depending on the workflow, you may be able to see:

- Current execution status
- Completed steps
- Processing steps
- Steps waiting for user action
- Errors or problems
- Generated outputs

This helps users understand where a process is within its execution.

Smartflow Outputs

A Smartflow can produce one or more outputs.

Outputs may include information displayed directly within AiX or files generated by the workflow.

For example, a Smartflow could produce:

- A management summary
- A document review report
- A classification result
- A completed Word document
- An Excel workbook
- A PowerPoint presentation
- A PDF report
- Structured information for another process

Outputs can also be used by subsequent Smartflow steps.

Creating a Smartflow

Depending on your permissions, you may be able to create your own Smartflows.

Smartflows are created using the visual Smartflow designer.

You build a workflow by adding steps and connecting them in the order required by the business process.

A typical design process is:

1. Define the purpose of the Smartflow.
2. Identify the required inputs.
3. Add the processing steps.
4. Connect the steps.
5. Configure each step.
6. Define the required outputs.
7. Test the Smartflow.
8. Review the results.
9. Publish the Smartflow for use.

This allows business processes to be designed without developing a traditional software application.

Designing a Smartflow

Before creating a Smartflow, consider the business process you want to automate.

Start by identifying:

Input — What information starts the process?

Process — What needs to happen to that information?

AI — Where can AI assist the process?

Business Rules — What conditions or decisions need to be applied?

Human Review — Where should a person review or approve the result?

Output — What should the process produce?

For example, a document review process might be designed as:

Upload Document

↓

Read Document

↓

Extract Key Information

↓

AI Review

↓

Verify Results

↓

Human Review

↓

Generate Report

This provides a clear structure before individual Smartflow steps are configured.

Testing a Smartflow

A Smartflow should be tested before it is made available for regular business use.

Testing should include representative inputs and business scenarios.

When testing, consider whether:

- The correct information is being processed
- AI instructions produce the expected results
- Business rules behave correctly
- Required human review steps occur

- Errors are handled appropriately
- Generated outputs contain the required information
- The complete process produces a useful business result

AI-based steps should also be tested with different examples because AI responses may vary depending on the input and selected model.

Publishing and Versions

Smartflows can be updated as business requirements change.

Where versioning is enabled, changes can be maintained separately from published versions.

This allows a Smartflow to be modified and tested before a new version is made available for operational use.

Published versions also help organizations maintain consistency and traceability when Smartflows are used for business processes.

Smartflow Execution History

AiX records Smartflow executions to support operational tracking and auditability.

Depending on your permissions, execution information may include:

- Smartflow version
- Execution status
- Execution time
- Processing steps
- Inputs and outputs
- User activities
- AI interactions
- Errors or exceptions

This information can help users understand how a result was produced and assist with troubleshooting when required.

Smartflow and Assistants

Smartflow and Assistants support different types of AI activities.

Assistant

Designed primarily for conversational interaction.

Smartflow

Designed primarily for repeatable business processes and automation.

For example, an Assistant might help a user interactively review a contract.

A Smartflow might automatically read the contract, extract key terms, perform an AI review, verify selected information, request human review, and generate a standardized report.

Use an **Assistant** when the activity is primarily conversational.

Use a **Smartflow** when the activity follows a repeatable process.

Smartflow and Scheduler

Smartflows can also be used with **Scheduler** where supported.

Instead of requiring a user to manually start a Smartflow, Scheduler can execute supported Smartflows automatically at defined times or intervals.

For example:

Every morning → **Retrieve Information** → **Analyze** → **Generate Summary** → **Send Notification**

This allows Smartflow to support recurring business processes as well as user-initiated activities.

Good Practices

When working with Smartflows:

- Start with a clearly defined business objective.
- Keep each step focused on a specific activity.
- Use meaningful names for steps and outputs.
- Test with representative business scenarios.
- Include human review where appropriate.
- Verify important AI-generated information.
- Handle exceptions and unexpected inputs.
- Review changes before publishing a new version.
- Keep workflows understandable for other users who may need to maintain them.

A well-designed Smartflow should make the business process easier to understand, execute, and maintain.

Next Steps

You may also want to explore:

- **Chat** — Interact directly with available AI models.
- **Knowledge Base** — Use organizational information with AI.
- **Assistants** — Create reusable conversational AI experiences.
- **Scheduler** — Run supported Smartflows automatically.

2.6 Projects

2.7 Scheduler

Scheduler allows AiX processes to run automatically at a defined date, time, or recurring interval.

Instead of manually starting the same process each time it is required, you can create a schedule and allow AiX to execute it automatically.

Scheduler is particularly useful for recurring business activities such as daily reports, periodic document processing, information monitoring, and regular notifications.

What is Scheduler?

Scheduler controls **when** an AiX process should run.

For example, you might create schedules to:

- Run a Smartflow every morning
- Generate a weekly management report
- Process documents every evening
- Check for new information at regular intervals
- Produce a monthly summary
- Send scheduled notifications

A schedule can be associated with a supported AiX process and configured to execute automatically.

The scheduling options available to you depend on your organization's configuration and your access permissions.

Scheduler and Smartflow

Scheduler and Smartflow work together to automate business processes.

Smartflow defines what should happen.

Scheduler defines when it should happen.

For example, a Smartflow might define the following process:

Retrieve Information → Analyze with AI → Generate Summary → Send Notification

Scheduler can then automatically run that Smartflow every weekday morning.

This separates the business process from its execution schedule, allowing the same Smartflow to be run manually or automatically.

Viewing Schedules

Open **Scheduler** from the AiX navigation menu to view schedules available to you.

Depending on your permissions, you may be able to see information such as:

- Schedule name
- Description
- Scheduled process
- Frequency
- Next execution
- Last execution
- Status

Schedules can typically be enabled or disabled without removing their configuration.

Creating a Schedule

Depending on your permissions, you may be able to create schedules.

To create a schedule:

1. Open **Scheduler**.
2. Select **New Schedule**.
3. Enter a name and description.
4. Select the process or Smartflow to execute.
5. Define when the process should run.
6. Configure any required parameters.
7. Review the schedule.
8. Save and enable the schedule.

Once enabled, AiX will automatically execute the scheduled process according to the defined schedule.

Schedule Types

Depending on your organization's configuration, schedules may be configured to run once or repeatedly.

One-Time Schedule

A one-time schedule runs a process at a specific date and time.

For example:

> Run the Year-End Report Smartflow on 31 December at 6:00 PM.

Recurring Schedule

A recurring schedule runs repeatedly according to a defined frequency.

Examples include:

Daily

> Run every day at 8:00 AM.

Weekly

> Run every Monday at 9:00 AM.

Monthly

> Run on the first day of every month.

Interval

> Run at a defined recurring interval.

The scheduling options available may vary depending on the AiX configuration.

Schedule Parameters

A scheduled process may require information or parameters when it runs.

For example, a reporting Smartflow might require:

- Reporting period
- Input location
- Output location
- Recipient
- Processing options

Where supported, these values can be configured as part of the schedule so that the process can execute without requiring manual input each time.

Example: Daily News Summary

A Smartflow could be designed to retrieve and analyze relevant news.

The process might be:

Retrieve News → **Filter Relevant Articles** → **AI Analysis** → **Generate Summary** → **Send Notification**

Scheduler could then be configured to run the Smartflow:

> Every weekday at 7:00 AM.

The process runs automatically and produces the required output without a user having to start the Smartflow manually.

Example: Monthly Management Report

A Smartflow could collect information and generate a management report.

The Smartflow might perform:

Retrieve Data → Analyze Results → Generate Charts → Create PowerPoint → Save Output

Scheduler could run the Smartflow automatically on the first business day of each month.

This allows recurring reporting processes to be automated while maintaining a consistent workflow.

Enabling and Disabling a Schedule

A schedule can be enabled or disabled where your permissions allow.

Enabled

The schedule is active and will execute according to its configured timing.

Disabled

The schedule remains configured but will not automatically execute.

Disabling a schedule can be useful when an automated process needs to be temporarily suspended without deleting its configuration.

Editing a Schedule

Depending on your permissions, you may be able to modify an existing schedule.

For example, you might change:

- Execution time
- Frequency
- Scheduled process
- Input parameters
- Start or end date
- Schedule status

Review schedule changes carefully before enabling the updated schedule.

Execution History

AiX maintains execution information for scheduled processes.

Depending on your permissions, you may be able to review information such as:

- Scheduled execution time

- Actual execution time
- Process or Smartflow executed
- Execution status
- Completion time
- Generated outputs
- Errors or exceptions

Execution history can help confirm that scheduled activities have completed successfully and assist with troubleshooting when a scheduled process fails.

Failed Scheduled Runs

A scheduled process may fail if a problem occurs during execution.

For example:

- Required information is unavailable
- A source system cannot be reached
- A file cannot be accessed
- An AI service is unavailable
- A Smartflow step encounters an error

Where available, review the execution details to identify the step or activity that caused the problem.

After resolving the issue, the process may be run again manually or allowed to execute at its next scheduled time.

Scheduling Considerations

Before scheduling a process, consider how frequently it needs to run and whether all required resources will be available at the scheduled time.

For example, consider:

- How long the process normally takes
- Whether required source systems will be available
- Whether required files or information will be ready
- Whether multiple scheduled executions could overlap
- Whether the process uses external AI services or APIs
- Whether human review is required
- Who should review failures or exceptions

Avoid scheduling processes more frequently than required.

Human Activities

A scheduled Smartflow can include human activities.

For example:

Scheduled Start → Retrieve Documents → AI Review → Human Review → Generate Final Report

Scheduler can automatically start the process, but the Smartflow may pause when it reaches a step requiring human action.

The workflow can continue after the required user completes their activity.

This allows scheduled automation to be combined with appropriate human oversight.

Good Practices

When using Scheduler:

- Use clear and descriptive schedule names.
- Schedule processes only as frequently as required.
- Confirm that required inputs will be available.
- Consider the expected execution time.
- Avoid unnecessary overlapping executions.
- Review execution history periodically.
- Investigate failed executions.
- Disable schedules that are temporarily not required.
- Review schedules when the associated Smartflow changes.
- Include human review where appropriate for important business processes.

Scheduler, Smartflow, and Assistants

AiX provides different capabilities for different types of activities.

Assistant

Provides a reusable conversational AI experience.

Smartflow

Defines a repeatable business process.

Scheduler

Determines when a supported process should execute automatically.

Together, these capabilities allow AiX to support both interactive AI use and automated business processes.

For example:

Knowledge Base

Provides the organizational information.

↓

Smartflow

Defines how the information should be processed.

↓

Scheduler

Determines when the process should run.

↓

Human Review

Provides oversight where required.

This allows recurring AI-assisted activities to operate as controlled business processes rather than isolated AI interactions.

Next Steps

You may also want to explore:

- **Smartflow** — Create and run AI-powered business workflows.
- **Knowledge Base** — Use organizational information with AI.
- **Assistants** — Create reusable conversational AI experiences.

3. Administration

3.1 Overview

■# Administration Overview

The Administration section provides guidance for users responsible for configuring and managing the AiX platform.

AiX administration includes managing users and access, platform settings, shared resources, integrations, and other capabilities required to make AiX available securely and consistently across an organization.

The administrative functions available to you depend on your assigned role and permissions.

Administration Responsibilities

Depending on your organization's deployment and your administrative permissions, responsibilities may include:

- Managing users and access
- Managing roles and permissions
- Configuring authentication and Single Sign-On (SSO)
- Managing teams and shared resources
- Configuring platform settings
- Managing integrations and connectors
- Managing access to Knowledge Bases, Assistants, and Smartflows
- Reviewing platform activity and audit information

AI model configuration and operational infrastructure are covered separately under **AI Model Management** and **Operations & Maintenance**.

Users

AiX users represent individuals who are authorized to access the platform.

Administrators may be responsible for activities such as:

- Viewing users
- Creating or provisioning users
- Enabling or disabling access
- Assigning roles and permissions
- Managing team membership
- Reviewing user status

How users are created and authenticated depends on your organization's identity configuration.

AiX may use locally managed accounts or integrate with an organization's existing identity provider.

Authentication and Single Sign-On

AiX supports integration with enterprise identity and authentication environments.

Depending on the deployment, users may authenticate using:

- AiX-managed authentication
- Enterprise Single Sign-On (SSO)
- Microsoft Entra ID
- Other supported identity providers

Organizations may also use an identity bridge or federation service to integrate AiX with existing identity infrastructure.

Authentication determines **who the user is**, while authorization determines **what the user is permitted to access or perform** within AiX.

Roles and Permissions

AiX uses roles and permissions to control access to platform capabilities and resources.

Permissions can determine whether a user can perform activities such as:

- View a resource
- Use or execute a resource
- Create a resource
- Modify a resource
- Share a resource
- Review or approve activities
- Perform administrative functions

Administrators should follow the principle of least privilege by granting users only the permissions required for their responsibilities.

Teams

Teams allow users to be grouped for collaboration and access management.

Depending on the resource and configuration, teams can be used to share access to capabilities such as:

- Knowledge Bases
- Assistants
- Smartflows
- Business content

Using teams can simplify access management compared with assigning permissions individually to every user.

Managing AiX Resources

AiX includes several resources that may be created and shared across an organization.

These include:

Knowledge Bases Collections of organizational information that can be used as context for AI.

Assistants Purpose-built conversational AI experiences.

Smartflows Reusable AI-powered business processes.

Schedules Configurations that automatically execute supported processes.

Resource owners and administrators can control who can access and use these capabilities according to their assigned permissions.

Detailed instructions for creating and using these resources are provided in the **User Guide**.

Integrations and Connectors

AiX can integrate with enterprise systems and information sources.

Depending on your organization's environment, integrations may provide access to services such as:

- Enterprise document repositories
- File and network storage
- Email services
- Databases
- Messaging platforms
- External business applications
- AI services

Administrators may be responsible for configuring or authorizing these integrations.

Detailed technical configuration is covered under **Integration**.

AI Models

AiX can provide access to locally deployed or externally hosted AI models.

Administrators may control which configured models are available to users and AiX capabilities.

Detailed model installation, configuration, routing, and management are covered separately under **AI Model Management**.

Audit and Activity

AiX records platform and user activities to support operational visibility, governance, and audit requirements.

Depending on your permissions, administrative information may include:

- User activities
- Resource changes
- Smartflow executions
- AI interactions
- Authentication activities
- Administrative actions
- Errors and exceptions

Audit information can help organizations understand how AiX is being used and investigate activities when required.

Detailed logging, monitoring, and operational procedures are covered under **Operations & Maintenance**.

Administrative Access

Administrative access should be limited to authorized personnel.

Administrators should:

- Use individual administrator accounts
- Avoid sharing credentials
- Apply least-privilege access
- Review administrative permissions periodically
- Disable access when it is no longer required
- Follow organizational security policies
- Review important administrative changes where appropriate

For additional security guidance, refer to the **Security** section.

Administration and Operations

Administration and Operations & Maintenance have different responsibilities within the AiX documentation.

Administration focuses on configuring and managing how the platform is used.

Examples include users, roles, permissions, authentication, teams, resources, and platform settings.

Operations & Maintenance focuses on keeping the platform running reliably.

Examples include service health, monitoring, logging, backup and recovery, patching, maintenance, and troubleshooting.

Technical deployment and infrastructure configuration are covered under **Deployment** and **Architecture**.

Related Documentation

Refer to the following sections for additional information:

- **User Guide** — Using Chat, Knowledge Base, Assistants, Smartflow, and Scheduler
- **AI Model Management** — Configuring and managing AI models
- **Operations & Maintenance** — Monitoring and maintaining the AiX environment
- **Architecture** — Understanding AiX components and system architecture
- **Deployment** — Installing and deploying AiX
- **Integration** — Connecting AiX with enterprise systems and services
- **Security** — Authentication, authorization, data protection, auditing, and security controls
- **Troubleshooting** — Diagnosing and resolving common issues

Download Documentation

Prefer an offline or printable copy of this section?

Download Administration (PDF)

The PDF contains the complete Administration documentation for this release and is generated from the same documentation source as this website.

3.2 User Management

User management controls who can access AiX and provides the identity used to determine each user's access to platform capabilities and resources.

Depending on your organization's authentication configuration, users may be managed directly within AiX or provisioned through an external identity provider.

Administrators can use user management to review accounts, manage user status, and assign the appropriate roles, teams, and access permissions.

User Accounts

Each AiX user has an account that identifies the individual accessing the platform.

A user account may contain information such as:

- Username
- Display name
- Email address
- Authentication method
- Account status
- Assigned roles

- Team membership
- User profile information
- Last login information

The information available depends on your organization's configuration and authentication method.

Viewing Users

Administrators with the appropriate permissions can view users registered with AiX.

The user list may provide information such as:

- Username
- Name
- Email
- Authentication method
- Status
- Roles
- Last login

Use search and filtering options, where available, to locate a particular user or group of users.

Select a user to view additional account and access information.

Creating Users

How users are created depends on the authentication method configured for your AiX environment.

Locally Managed Users

Where local authentication is enabled, authorized administrators may create users directly within AiX.

Typical information may include:

- Username
- Display name
- Email address
- Authentication method
- Initial access settings
- Role assignments
- Team membership

Required fields may vary depending on your organization's configuration.

Enterprise Identity Users

Where AiX is integrated with an enterprise identity provider, users may be created or recognized through the organization's existing identity system.

Examples may include environments using:

- Microsoft Entra ID
- Active Directory
- LDAP
- OpenID Connect
- SAML
- Other supported identity providers

In these environments, identity information may be managed by the organization's identity provider rather than directly within AiX.

AiX maintains the information required to associate the authenticated identity with the appropriate AiX user and permissions.

Authentication Method

A user's authentication method determines how their identity is verified when accessing AiX.

Depending on your environment, authentication may be provided through:

Local Authentication The user's credentials are managed through AiX.

Single Sign-On (SSO) The user authenticates through an approved enterprise identity provider.

When SSO is used, password policies, Multi-Factor Authentication (MFA), account lockout, and other authentication controls may be managed by the external identity provider.

For detailed configuration information, see **Authentication & SSO**.

User Status

User accounts can have a status that determines whether the account can access AiX.

Common states may include:

Active The user is permitted to access AiX according to their assigned permissions.

Inactive or Disabled The account remains registered but cannot access the platform.

Disabling an account is generally preferred when access needs to be removed while retaining the user's historical activities and audit information.

Available status values may depend on your AiX version and configuration.

Roles and Permissions

Creating a user does not necessarily give that user access to every AiX capability.

Roles and permissions determine what the user is authorized to do after authentication.

Depending on their assigned permissions, a user may be able to:

- Use Chat
- Access Knowledge Bases
- Use Assistants
- Run Smartflows
- Create or modify resources
- Review or approve activities
- Manage other users
- Perform administrative functions

Administrators should assign only the access required for the user's responsibilities.

For detailed information, see **Roles & Permissions**.

Teams

Users can be assigned to teams to simplify collaboration and resource access.

For example, an organization might create teams for:

- Human Resources
- Finance
- Legal
- Operations
- Information Technology
- Project teams

Resources such as Knowledge Bases, Assistants, and Smartflows can then be shared with the appropriate teams rather than individually with each user.

A user may belong to more than one team where permitted.

For more information, see **Teams**.

User Profile

User profiles contain information associated with the user within AiX.

Depending on your organization's configuration, profile information may be used to support:

- Display information

- Organizational information
- Department or business unit
- Regional settings
- AI or processing preferences
- Resource access
- Processing or service routing

Some profile information may be maintained directly within AiX, while other information may originate from an enterprise identity provider.

Editing a User

Authorized administrators may modify user information that is managed by AiX.

Depending on the authentication method and permissions, editable information may include:

- Display information
- Account status
- Roles
- Team membership
- User profile settings

Information managed by an external identity provider may need to be changed in the source identity system rather than within AiX.

Disabling User Access

When a user should no longer access AiX, their account should be disabled according to your organization's access management procedures.

For example, access may need to be disabled when:

- An employee leaves the organization
- A contractor's engagement ends
- A user changes responsibilities
- Access is temporarily suspended
- An account is identified as no longer required

Disabling access preserves the relationship between the user and their previous platform activities.

Historical Smartflow executions, approvals, audit records, and other activities should remain attributable to the original user.

Deleting Users

Where user deletion is available, administrators should consider the impact on historical and audit information before permanently removing a user.

In many enterprise environments, disabling an account is preferable to deleting it because historical activities may need to remain associated with the original user.

Follow your organization's information retention and identity management policies when determining whether an account should be disabled or deleted.

User Lifecycle

A typical AiX user lifecycle is:

User Created or Provisioned

↓

Identity Authenticated

↓

Roles and Teams Assigned

↓

User Accesses AiX

↓

Access Changes as Responsibilities Change

↓

Account Disabled When Access Is No Longer Required

This lifecycle helps maintain controlled access while preserving accountability for activities performed within AiX.

Authentication and Authorization

Authentication and authorization serve different purposes.

Authentication answers:

> Who is this user?

Authentication is performed by AiX or an approved identity provider.

Authorization answers:

> What is this user allowed to do?

Authorization is controlled through AiX roles, permissions, teams, and resource access.

A successfully authenticated user does not automatically have access to every AiX capability or resource.

External Identity Management

When AiX is connected to an enterprise identity provider, the identity provider should normally remain the authoritative source for user identity.

For example, the identity provider may manage:

- Username
- Password
- Multi-Factor Authentication
- Account lockout
- Authentication policies
- Identity lifecycle

AiX manages the application-level information required to determine what the authenticated user can access and perform within the platform.

This separation allows organizations to continue using their established identity and security controls while managing AiX-specific authorization within AiX.

User Management Good Practices

Administrators should follow their organization's identity and access management policies when managing AiX users.

Recommended practices include:

- Create individual accounts for each user.
- Do not share user accounts.
- Use enterprise SSO where required by organizational policy.
- Apply the principle of least privilege.
- Use teams to simplify access management.
- Review user access periodically.
- Remove unnecessary roles and permissions.
- Disable accounts promptly when access is no longer required.
- Preserve user identity for historical and audit records.
- Review administrative privileges regularly.

Audit Information

User-related activities are recorded by AiX where applicable.

Audit information may include:

- User creation
- User changes
- Account status changes
- Authentication activities
- Role or permission changes
- Team membership changes
- Administrative actions

Audit records support operational investigation, security review, and organizational governance requirements.

For more information, see **Audit & Activity** and **Security**.

Related Documentation

Refer to the following sections for additional information:

- **Roles & Permissions** — Configure what users are authorized to do.
- **Teams** — Organize users and manage shared access.
- **Authentication & SSO** — Configure user authentication and enterprise identity integration.
- **Resource Access** — Control access to AiX resources.
- **Audit & Activity** — Review user and administrative activities.
- **Security** — Understand AiX security and access-control mechanisms.

3.3 Roles & Permissions

Roles and permissions control what users are authorized to access and perform within AiX.

AiX uses role-based access control to provide users with the capabilities required for their responsibilities while restricting access to functions and resources they do not require.

Authentication determines **who the user is**.

Roles and permissions determine **what the user is allowed to do**.

Role-Based Access Control

Role-Based Access Control (RBAC) assigns permissions to roles rather than managing every permission separately for every user.

A simplified model is:

User → Role → Permissions → Actions

For example, a standard user may have permission to use Chat and execute shared Smartflows, while an administrator may have additional permissions to manage users and platform configuration.

Using roles helps organizations apply access controls consistently across groups of users.

Roles

A role represents a collection of permissions associated with a particular responsibility.

Depending on your organization's AiX configuration, roles may be used to distinguish between users who:

- Use AiX capabilities
- Create and manage resources
- Review business activities
- Approve business activities
- Manage users and access
- Configure the platform
- Perform administrative functions

The roles available to you depend on your AiX version and organizational configuration.

Permissions

Permissions define individual actions that a user is authorized to perform.

Permissions may control activities such as:

- View
- Create
- Modify
- Delete
- Execute
- Share
- Review
- Approve
- Publish
- Manage

A role can contain multiple permissions.

Users receive the permissions associated with their assigned roles together with any applicable resource-level access controls.

Platform and Resource Access

AiX access can be considered at two levels:

Platform Access

Controls whether a user can access or manage a capability within AiX.

For example, a user may have permission to access Smartflow or administer users.

Resource Access

Controls what the user can do with a particular resource.

For example, a user may have access to one Smartflow but not another.

This separation allows organizations to provide access to a capability without automatically providing access to every resource within that capability.

Resource Roles

AiX resources may use additional roles to control how individual users participate in a particular resource or business process.

Depending on the resource, these may include:

Creator

The **Creator** is the owner or creator of the resource.

The Creator typically has the permissions required to configure and manage the resource, subject to organizational access policies.

Team

A **Team** member is a user who has been given access to a shared resource.

Depending on the resource and assigned permissions, Team members may be able to view or use the resource without being permitted to modify its configuration.

Assignee

An **Assignee** is a user responsible for completing an activity or providing information as part of a business process.

For example, an Assignee may be asked to provide information, upload a document, or submit a response before a Smartflow can continue.

Reviewer

A **Reviewer** participates in the review stage of a process.

Depending on the workflow configuration, a Reviewer may be able to:

- Review information
- Execute an assigned activity
- Add comments

- Update review status

A Reviewer does not automatically have approval authority.

Approver

An **Approver** is authorized to perform an approval activity within a configured business process.

Depending on the workflow, an Approver may review the available information and update the approval status so that the process can continue.

Reviewer and Approver responsibilities should be assigned according to the organization's business controls.

Example

Consider a Smartflow used to review a business document.

The Smartflow may have the following participants:

Creator

Creates, configures, and publishes the Smartflow.

↓

Team

Uses the published Smartflow.

↓

Assignee

Provides the document or information required by the process.

↓

Reviewer

Reviews the AI-generated analysis and provides comments or a review status.

↓

Approver

Performs the required approval action.

These roles allow different responsibilities to be separated within the same business process.

Assigning Roles

Administrators with the appropriate permissions can assign roles to users.

Before assigning a role, consider:

- The user's business responsibilities
- The AiX capabilities they require
- The resources they need to access
- Whether they need creation or modification rights
- Whether they require review or approval authority
- Whether administrative access is required

Users should be assigned only the permissions necessary to perform their responsibilities.

Multiple Roles

A user may have more than one role where required.

For example, a user could be a standard AiX user while also acting as an Approver for a particular Smartflow.

Access is therefore determined by the combination of:

User Identity + Platform Permissions + Resource Access + Process Role

This allows AiX to support different responsibilities without requiring separate user accounts.

Teams and Permissions

Teams can simplify permission management by allowing resources to be shared with groups of users.

For example, instead of sharing a Knowledge Base individually with every member of the Finance department, an administrator or resource owner may provide access to the Finance team.

Users who join or leave the team can then gain or lose the associated resource access according to the configured permissions.

For more information, see **Teams**.

Permissions and Shared Resources

Resources such as Knowledge Bases, Assistants, and Smartflows may be private or shared.

Sharing a resource does not necessarily give every user permission to modify it.

For example, a user may have permission to:

- Use an Assistant without editing it
- Query a Knowledge Base without managing its content
- Run a Smartflow without modifying its design
- Review a Smartflow execution without approving it

This separation helps protect shared resources from unauthorized changes.

Least Privilege

AiX administrators should follow the principle of least privilege.

Users should receive only the access required to perform their responsibilities.

For example, a user who only needs to run an existing Smartflow should not require permission to modify or publish that Smartflow.

Similarly, administrative permissions should only be assigned to users responsible for managing the platform.

Separation of Duties

For business processes requiring additional controls, different responsibilities can be assigned to different users.

For example:

Submit → **Review** → **Approve**

The user submitting information does not necessarily need permission to approve it.

Similarly, a Reviewer and an Approver can represent separate responsibilities within the process.

Organizations should configure these roles according to their internal governance and business control requirements.

Changing Permissions

User responsibilities may change over time.

Administrators should update roles and permissions when:

- A user changes department or role
- Responsibilities change
- A project ends
- Temporary access is no longer required
- Administrative responsibilities change
- A user leaves the organization

Access changes should follow the organization's identity and access management procedures.

Permission Review

Organizations should periodically review user access.

A review may consider:

- Active users
- Assigned roles
- Administrative privileges
- Team memberships
- Shared resource access
- Reviewer and Approver assignments
- Users who no longer require access

Regular reviews help ensure that access remains appropriate as organizational responsibilities change.

Audit

Changes to roles, permissions, and resource access are recorded where applicable to support traceability and governance.

Audit information may include:

- User
- Action performed
- Role or permission changed
- Resource affected
- Date and time
- Result of the action

Business activities such as review and approval can also be associated with the user who performed the action.

For more information, see **Audit & Activity**.

Good Practices

When managing roles and permissions:

- Follow the principle of least privilege.
- Use roles rather than assigning permissions individually where possible.
- Use teams to simplify shared resource access.
- Keep administrative access limited.
- Separate submission, review, and approval responsibilities where required.
- Review access periodically.
- Remove access when it is no longer required.
- Avoid shared user accounts.
- Preserve user identity for auditability.
- Document organization-specific role definitions and responsibilities.

Related Documentation

Refer to the following sections for additional information:

- **Users** — Manage AiX user accounts.
- **Teams** — Organize users and shared access.
- **Authentication & SSO** — Configure how users authenticate.
- **Resource Access** — Manage access to Knowledge Bases, Assistants, Smartflows, and other resources.
- **Audit & Activity** — Review access changes and user activities.
- **Security** — Understand AiX authentication, authorization, and security controls.

3.4 System Settings

System Settings allow authorized administrators to configure platform-wide behavior and default settings for AiX.

These settings apply across the AiX environment and may affect multiple users, teams, and platform capabilities.

Because changes to system settings can affect the operation of the platform, access should be limited to authorized administrators.

Accessing System Settings

To access System Settings:

1. Sign in to AiX using an account with administrative permissions.
2. Open **Administration**.
3. Select **System Settings**.
4. Select the settings category you want to review or modify.

The settings available depend on your AiX version, deployment configuration, and administrative permissions.

General Settings

General settings define basic information and behavior for the AiX environment.

Depending on your configuration, these settings may include:

- Organization name
- Environment name
- Default language
- Regional settings
- Date and time format
- Time zone
- Default application behavior

These settings can help align the AiX environment with your organization's operating requirements.

Organization Settings

Organization settings identify the organization or business environment using AiX.

Depending on the deployment, administrators may configure information such as:

- Organization name
- Display name
- Organization information
- Default preferences

Organization settings may also be used by other AiX capabilities when presenting information to users or generating outputs.

Regional Settings

Regional settings control how locale-sensitive information is presented within AiX.

Depending on the available configuration, administrators may define settings such as:

- Default language
- Time zone
- Date format
- Time format
- Number format

Individual user preferences may override selected defaults where supported.

Administrators should ensure that the configured time zone is appropriate for scheduled processes and audit information.

Default Settings

AiX may provide platform-wide defaults for selected capabilities.

Defaults help provide a consistent starting configuration while allowing individual resources to use different settings where permitted.

For example, an organization may define defaults that are used when a new resource is created.

Changing a default setting does not necessarily change existing resources that already have their own configuration.

AI Defaults

Where available, administrators may define default AI-related preferences for the platform.

These may include settings such as:

- Default AI model
- Default response behavior
- Default language
- Other platform-level AI preferences

Only AI models that have already been configured and made available to the AiX environment can be selected.

Detailed model configuration, endpoints, credentials, deployment, and lifecycle management are covered under **AI Model Management**.

Content and File Settings

Depending on your organization's configuration, system settings may include default behavior relating to content and files.

These settings may control areas such as:

- Supported content behavior
- Default content locations
- File handling preferences
- Output handling
- Temporary or working content

Technical storage configuration, network shares, mounted volumes, and infrastructure-level file services are covered under **Deployment** and **Operations & Maintenance**.

Application Settings

Application settings control selected platform-wide behavior within AiX.

Depending on the version and configuration, these settings may include:

- Feature availability
- Default user experience
- Platform behavior
- Resource defaults
- Application-level options

Administrators should review the impact of a setting before changing it in a production environment.

Feature Availability

Some AiX capabilities may be enabled or disabled according to the organization's requirements, licensing, deployment, or configuration.

Depending on the environment, this may affect the availability of capabilities such as:

- Chat
- Knowledge Base
- Assistants
- Smartflow
- Scheduler
- Integrations
- Other optional capabilities

Disabling a capability may affect users or processes that depend on it.

Review dependencies before changing feature availability.

Authentication Settings

Some authentication-related settings may be visible through Administration.

These may identify the authentication methods available to the AiX environment or control application-level authentication behavior.

Detailed identity provider configuration, Single Sign-On, federation, and authentication integration are covered under **Authentication & SSO**.

Administrators should avoid changing authentication settings without understanding how users currently access the platform.

Incorrect authentication configuration may prevent users from signing in.

System Settings and Technical Configuration

System Settings are intended primarily for application-level configuration.

Technical infrastructure configuration is documented separately.

Use the following sections when managing the underlying AiX environment:

AI Model Management AI model endpoints, availability, configuration, and model management.

Deployment Servers, containers, databases, storage, networking, and deployment configuration.

Integration Enterprise systems, identity services, document repositories, messaging services, and external APIs.

Operations & Maintenance Monitoring, logs, backups, recovery, patching, service management, and routine maintenance.

Security Authentication, authorization, data protection, audit, and security controls.

Related Documentation

Refer to the following sections for additional information:

- **Users** — Manage AiX user accounts.
- **Roles & Permissions** — Control what users are authorized to do.
- **Authentication & SSO** — Configure enterprise authentication.
- **AI Model Management** — Configure and manage AI models.
- **Integration** — Configure external systems and services.
- **Operations & Maintenance** — Operate and maintain the AiX environment.
- **Security** — Configure and understand platform security controls.

3.5 Authentication & SSO

Authentication controls how users verify their identity when accessing AiX.

AiX supports local authentication and enterprise Single Sign-On (SSO). When enterprise SSO is required, **Keycloak is used as the SSO gateway between AiX and the organization's identity environment**.

If the organization already operates a compatible Keycloak environment, AiX can connect to the organization's existing Keycloak deployment.

If Keycloak is not already available, an **AiX SSO Gateway based on Keycloak** can be deployed as part of the AiX solution.

This provides AiX with a consistent authentication interface while allowing organizations to continue using their existing enterprise identity infrastructure.

Authentication and Authorization

Authentication and authorization perform different functions.

Authentication determines:

> Who is the user?

Authentication verifies the identity of the person accessing AiX.

Authorization determines:

> What is the user allowed to do?

After authentication, AiX uses its own roles, permissions, teams, and resource access controls to determine which capabilities and information the user can access.

A simplified model is:

Enterprise Identity → Keycloak → AiX User → Roles & Permissions → AiX Resources

This separates enterprise authentication from application-level authorization.

Authentication Methods

AiX supports two primary authentication approaches.

Local Authentication

With local authentication, users authenticate using credentials managed within the AiX environment.

Local authentication may be used for standalone environments, development and testing, or environments where enterprise SSO is not required.

Enterprise Single Sign-On

When enterprise SSO is required, AiX uses Keycloak as its SSO gateway.

Keycloak provides the integration layer between AiX and the organization's enterprise identity environment.

A typical authentication architecture is:

User

↓

AiX

↓

Keycloak

↓

Enterprise Identity Environment

The underlying enterprise environment may use technologies such as Active Directory, LDAP, SAML, or Kerberos.

AiX therefore does not need to implement separate authentication mechanisms for each customer identity environment.

AiX SSO Gateway

The **AiX SSO Gateway** is based on Keycloak.

It provides a standardized authentication interface between AiX and enterprise identity systems.

AiX communicates with Keycloak using a standard authentication protocol, while Keycloak handles integration with the organization's underlying identity infrastructure.

For example:

AiX → Keycloak → Active Directory / LDAP

or:

AiX → Keycloak → SAML Identity Provider

or, where applicable:

AiX → Keycloak → Active Directory / Kerberos

This architecture isolates the AiX application from differences between customer identity environments.

Deployment Options

There are two standard approaches for integrating Keycloak with AiX.

AiX SSO Gateway

If the organization does not already operate Keycloak, a dedicated Keycloak instance can be deployed as the **AiX SSO Gateway**.

The architecture is:

AiX

↓

AiX SSO Gateway (Keycloak)

↓

Customer Identity Environment

The AiX SSO Gateway is then configured to integrate with the organization's existing identity infrastructure.

Customer Keycloak

If the organization already operates Keycloak, AiX can connect to the customer's existing Keycloak environment where permitted by the organization's architecture and security policies.

The architecture becomes:

AiX

↓

Customer Keycloak

↓

Customer Identity Environment

In this scenario, a separate AiX Keycloak deployment may not be required.

The customer's identity and security teams remain responsible for the operation and policies of their Keycloak environment.

Enterprise Identity Integration

Keycloak provides the bridge between AiX and supported enterprise identity technologies.

Depending on the customer environment, this may include:

Active Directory and LDAP

Keycloak can connect to supported LDAP directory services, including Microsoft Active Directory.

A typical architecture is:

AiX → Keycloak → Active Directory / LDAP

The enterprise directory remains the authoritative source for the user's enterprise identity.

SAML

Where the organization provides a SAML Identity Provider, Keycloak can broker authentication between the SAML environment and AiX.

A typical architecture is:

AiX → Keycloak → SAML Identity Provider

This allows AiX to maintain a consistent authentication interface regardless of the customer's SAML implementation.

Kerberos

In Active Directory environments where Kerberos authentication is required, Keycloak can provide the appropriate integration with the enterprise authentication environment.

A typical architecture may be:

AiX → Keycloak → Active Directory / Kerberos

Kerberos configuration depends on the customer's Active Directory, DNS, browser, network, and security environment.

Detailed technical configuration is covered under **Integration → Identity & SSO**.

Authentication Flow

A typical enterprise SSO login follows this process:

1. The user accesses AiX.
2. AiX redirects the user to Keycloak for authentication.

3. Keycloak determines the appropriate enterprise authentication method.
4. The user authenticates using the organization's identity environment.
5. Keycloak validates the authenticated identity.
6. Keycloak returns the authenticated identity to AiX.
7. AiX associates the identity with the corresponding AiX user.
8. AiX applies the user's roles, permissions, teams, and resource access.
9. The user is granted access to the authorized AiX capabilities.

The user's enterprise password does not need to be managed by AiX.

Identity Mapping

After successful authentication, AiX associates the identity returned by Keycloak with an AiX user.

Identity information may include:

- Unique user identifier
- Username
- Display name
- Email address
- Enterprise groups
- Department
- Other approved identity attributes

A stable and unique identity identifier should be used when associating an enterprise ide

3.6 License Activation

4. AI Model Management

4.1 Overview

■# AI Model Management

AiX supports local and approved external AI models. This section documents the product-level model lifecycle, configuration principles, validation, operations, and troubleshooting.

Mermaid diagram source

```
flowchart LR
    Provider[Model Provider / Runtime] --> Register[Register Model]
    Register --> Configure[Configure Capabilities]
    Configure --> Test[Test]
    Test --> Enable[Enable]
    Enable --> Route[Assign / Route]
    Route --> Monitor[Monitor]
    Monitor --> Upgrade[Upgrade / Replace]
    Upgrade --> Disable[Disable / Remove]
```

Document only currently supported functionality as supported. Clearly identify roadmap or planned capabilities.

Download Documentation

Prefer an offline or printable copy of this section?

Download AI Model Management (PDF)

The PDF contains the complete AI Model Management documentation for this release and is generated from the same documentation source as this website.

4.2 Providers & Runtimes

Document the AI model providers and runtimes supported by the current AiX release.

| Type | Provider / Runtime | Deployment | Status | Notes | |---|---|---|---|---| | Local | Ollama | Customer environment | Supported / TBD | | | Local | vLLM | Customer environment | Supported / TBD | | | Local | vLLM-Ascend | Ascend environment | Supported / TBD | | | External | Approved API provider | External | Supported / TBD | |

Customer-specific endpoints, enabled models and credentials belong in the customer documentation. Never store API keys or tokens here.

4.3 Local Models

Purpose

Local models allow AiX deployments to execute approved AI workloads within customer-controlled infrastructure.

Record for Each Supported Model

- Model name and version

- Runtime
- Quantization, where applicable
- Context size
- Capabilities
- Minimum/recommended CPU, memory and accelerator requirements
- Installation or pull procedure
- AiX registration/configuration
- Health check
- Upgrade and rollback procedure
- Removal procedure

Lifecycle

Mermaid diagram source

```
flowchart TD
    Install[Install Runtime] --> Obtain[Obtain Approved Model]
    Obtain --> Register[Register with AiX]
    Register --> Validate[Validate]
    Validate --> Enable[Enable for Use]
    Enable --> Monitor[Monitor]
    Monitor --> Replace[Upgrade / Replace]
    Replace --> Retire[Retire Old Model]
```

4.4 External Models

Document supported external model/API integrations, required connectivity, supported authentication method, data-routing considerations, and validation procedures.

Do not include customer API keys, secrets or tokens. Customer-specific provider selections belong in `aix-docs-<customer>`.

4.5 Model Configuration

Document AiX model registration and configuration fields, including model identifier, endpoint/runtime, capabilities, context limits, defaults, timeout behavior, and any supported generation settings.

Where configuration differs between local and external models, document the differences explicitly.

4.6 Assignment & Routing

Document how AiX selects or assigns models to supported modules and workloads. Include default-model behavior, per-step overrides, local/external selection rules, and any location/department routing supported by the current release.

Avoid describing planned routing features as currently available.

4.7 Testing & Validation

Before enabling a model for production use, validate:

- Connectivity and health
- Authentication, where applicable
- Expected model identity/version
- Context/token limits
- Representative prompts
- Response latency
- Structured output behavior where used
- RAG/tool/function behavior where applicable
- Failure and timeout handling

Record customer-specific acceptance evidence in the customer documentation or approved evidence repository.

4.8 Upgrade & Replacement

Treat model changes as controlled changes. Record the old and new model/runtime versions, compatibility considerations, validation performed, rollback approach, and release/customer approval where required.

Prefer validating replacement models in UAT before enabling them in Production.

4.9 Troubleshooting

Check, in order:

1. Runtime/service health.
2. Network/DNS connectivity.
3. Model availability and identifier.
4. AiX endpoint/model configuration.
5. Authentication for external providers.
6. CPU/GPU/NPU memory and capacity.
7. Timeout/context-limit errors.
8. AiX and runtime logs.

Never paste secrets into troubleshooting records.

5. Operations & Maintenance

5.1 Overview

■# Operations & Maintenance Overview

This section defines product-level operating guidance for AiX. Customer-specific schedules, tools, responsibilities, retention periods, RPO/RTO values and infrastructure procedures belong in `aix-docs-<customer>`.

Core areas include service management, backup/recovery, data lifecycle and cleanup, health checks, monitoring, performance, logging, audit, patching and disaster recovery.

Download Documentation

Prefer an offline or printable copy of this section?

Download Operations & Maintenance (PDF)

The PDF contains the complete Operations & Maintenance documentation for this release and is generated from the same documentation source as this website.

5.2 Service Management

Document supported procedures for starting, stopping, restarting and checking AiX components. Include dependency/order considerations and safe maintenance procedures for the current deployment architecture.

Customer-specific container/service names and infrastructure commands should be recorded in the customer repository.

5.3 Backup & Recovery

A complete AiX backup strategy should consider the database, file storage, configuration, customer-managed integrations, and any other state required to restore service.

Mermaid diagram source

```
flowchart LR
    DB[(Database)] --> Backup[Backup Set]
    Files[File Storage] --> Backup
    Config[Configuration] --> Backup
    Backup --> Verify[Verify / Test Restore]
    Verify --> Recovery[Recovery Procedure]
```

Document what must be backed up, supported recovery sequence, consistency considerations, and restore validation. Customer-specific frequency, retention and backup technology belong in customer documentation.

5.4 Data Lifecycle & Cleanup

AiX deployments may accumulate multiple classes of operational and business data. Cleanup must be deliberate and must not remove records required for audit, recovery or customer retention requirements.

| Data Area | Examples | Cleanup Consideration | |---|---|---| | Database | application, execution, interaction records | retention and referential integrity | | Audit | user/actions/AI interaction audit | compliance retention | | File Storage | input, working, output, temporary files | business retention and active jobs | | Knowledge Base | source files, chunks, vectors | KB lifecycle and re-index requirements | | Logs | application/service logs | rotation and retention | | Cache | temporary/cache data | safe expiry/invalidation | | AI Worker | temporary processing artifacts | active-job safety |

Cleanup Principles

- Define retention before automated deletion.
- Separate temporary/cache cleanup from business-record deletion.
- Preserve required audit/provenance records.
- Validate backups where recovery may be required.
- Record customer-specific retention policies in the customer repository.

5.5 Health Checks

Define health checks for AiX web/application services, database, storage, AI Worker, AI Engine/model runtime, scheduler and required integrations.

Health checks should distinguish service availability from deeper functional readiness where practical.

5.6 Monitoring

Document availability and operational monitoring for AiX services and dependencies. See also Health Checks and Performance Monitoring.

Customer-specific monitoring products, alert thresholds, recipients and escalation procedures belong in the customer documentation.

5.7 Performance Monitoring

Monitor both infrastructure and application/model behavior. Relevant measures may include CPU, memory, disk, accelerator utilization, service response time, worker queue/load, model response latency and database/storage performance.

AiX may rely on customer/infrastructure monitoring tooling for metrics not exposed by the application. Document that boundary explicitly.

5.8 Logging

Document log locations/sources, log levels, rotation, retention, access control and safe diagnostic handling for AiX components.

Do not intentionally log secrets. Customer-specific forwarding/SIEM configuration belongs in the customer repository.

5.9 Audit

This section defines product-level operating guidance for AiX. Customer-specific schedules, tools, responsibilities, retention periods, RPO/RTO values and infrastructure procedures belong in `aix-docs-<customer>`.

Core areas include service management, backup/recovery, data lifecycle and cleanup, health checks, monitoring, performance, logging, audit, patching and disaster recovery.

5.10 Patching & Maintenance

Document the supported maintenance lifecycle for AiX application releases and relevant runtime dependencies. Coordinate OS, container runtime, database and infrastructure patching with the responsible customer/infrastructure teams.

Validate significant changes in UAT before Production where applicable and maintain an explicit rollback/recovery path.

5.11 Disaster Recovery

Document the standard DR planning framework, recovery sequence, validation, and customer-specific RTO/RPO considerations.

6. Architecture

6.1 Overview

■# AiX Platform Architecture

Overview

AiX is a modular enterprise AI platform designed to support business applications, AI-assisted workflows, knowledge processing, document processing, and automation across cloud, on-premises, hybrid, and local deployment environments.

The platform separates application services, AI orchestration, task execution, AI model services, data persistence, authentication, and platform management into independent service components.

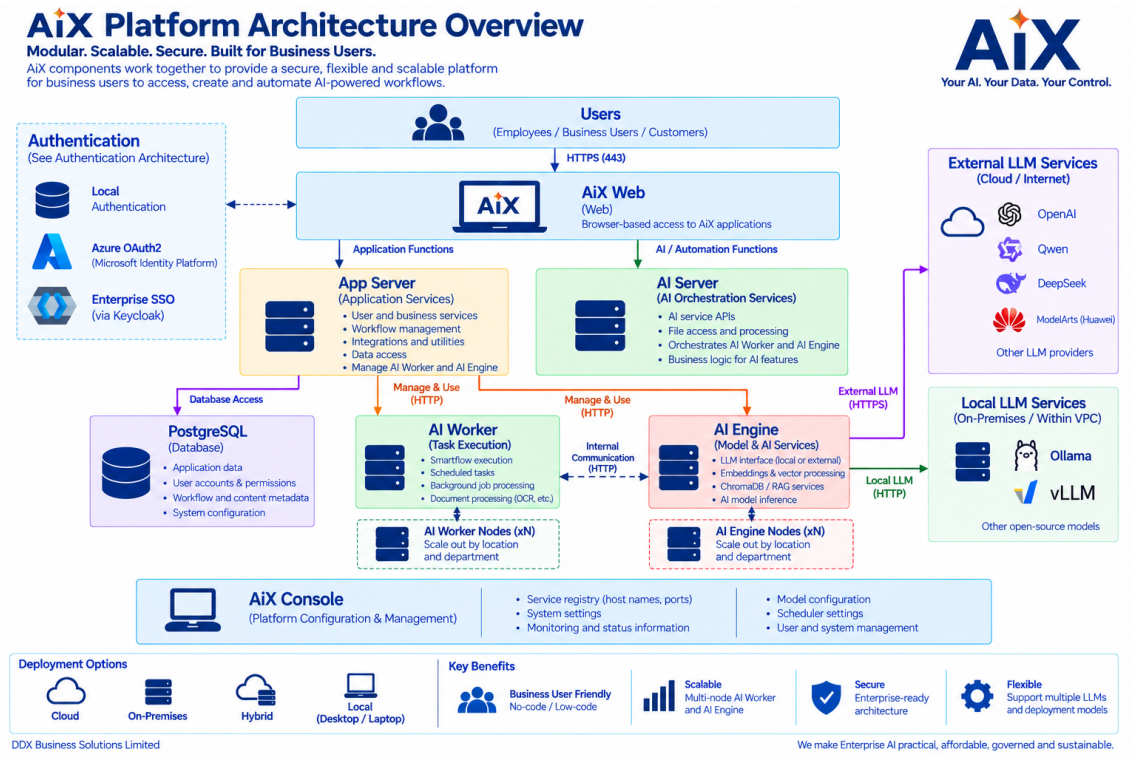
This modular architecture allows AiX to operate as a compact single-host deployment or scale across multiple infrastructure nodes according to workload, organizational, security, and availability requirements.

AiX supports both external and locally hosted AI models while allowing application data, user access controls, workflow execution, and platform configuration to remain within the designated deployment environment.

Platform Architecture Overview

The following diagram illustrates the primary AiX platform components and their logical relationships.

<figure markdown="span">



AiX platform architecture overview

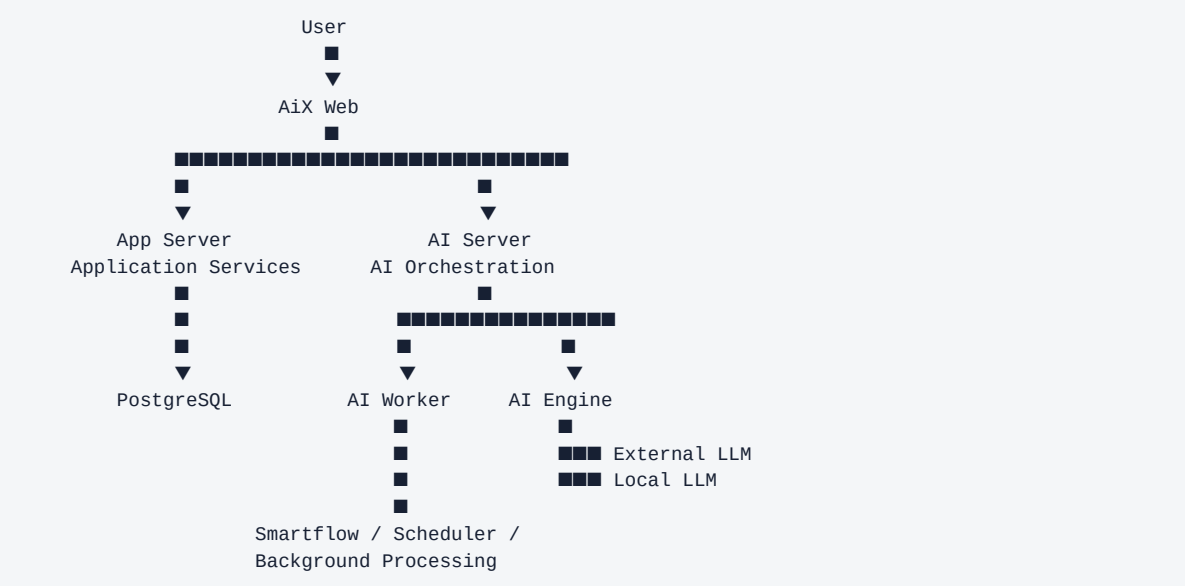
<figcaption>Figure: AiX Platform Architecture Overview</figcaption>

</figure>

Users access the platform through **AiX Web**. Depending on the requested function, AiX Web communicates directly with either the **App Server** or the **AI Server**.

The two backend paths provide a logical separation between application functions and AI or automation functions:

text



The **App Server**, **AI Server**, **AI Worker**, and **AI Engine** operate as separate services with defined responsibilities. This allows individual components to be maintained and scaled independently.

Core Platform Components

AiX Web

AiX Web provides the browser-based user interface for the AiX platform.

Users connect to AiX Web through HTTPS. AiX Web then communicates with the appropriate backend service depending on the requested operation:

- **App Server** for application and business functions
- **AI Server** for AI and automation functions

AiX Web therefore does not depend on a single backend gateway for all platform operations.

App Server

The **App Server** provides the core application service layer.

Its responsibilities include:

- User and business services
- Application and workflow management
- Integrations and utilities

- Application data services
- User and permission-related functions
- Shared application services required by AI Worker and AI Engine

The App Server communicates with PostgreSQL for persistent application data.

AI Worker and AI Engine may also interact with the App Server when task execution or AI processing requires application-level information or services.

PostgreSQL

PostgreSQL provides the primary relational database for the AiX platform.

It stores persistent platform information such as:

- Application data
- User and permission information
- Workflow and content metadata
- System configuration
- Other application-level metadata

PostgreSQL is accessed through the appropriate backend services and is not directly exposed to AiX Web or end users.

AI Server

The **AI Server** provides the orchestration and API layer for AI and automation-related operations.

Its responsibilities include:

- AI service APIs
- File access and processing coordination
- AI and automation business logic
- AI Worker orchestration
- AI Engine orchestration

When AiX Web requests an AI or automation operation, the AI Server coordinates the appropriate processing service.

The AI Server does **not** directly invoke local or external LLM services. Model access is handled through the AI Engine.

AI Worker

The **AI Worker** provides workflow, task, document, and background processing capabilities.

Its responsibilities include:

- Smartflow execution

- Scheduled task execution
- Background job processing
- Document processing
- OCR and other processing workloads

The **Scheduler** operates as part of the AI Worker and initiates scheduled Smartflows and background tasks according to configured schedules.

During execution, AI Worker may interact with the App Server for application services and with AI Engine where AI or model capabilities are required.

AI Engine

The **AI Engine** provides the model and AI service abstraction layer.

Its responsibilities include:

- AI model inference
- Local and external LLM integration
- Embedding generation
- Vector processing
- ChromaDB and RAG-related services

AI Engine is the primary AiX component responsible for communication with underlying AI model services.

This provides a consistent model interface to the rest of the AiX platform and prevents application and orchestration components from being directly coupled to individual model providers.

AI Model Integration

AiX supports both **external** and **locally hosted** AI model services.

External LLM Services

External model services may include:

- OpenAI
- Qwen
- DeepSeek
- Huawei ModelArts
- Other supported or customer-approved model providers

The AI Engine communicates with approved external model services using the corresponding provider APIs, normally over HTTPS.

Local LLM Services

For environments requiring private, on-premises, or offline model execution, AiX supports locally hosted model-serving technologies such as:

- Ollama
- vLLM

Local model services can operate within the same infrastructure environment as AiX or on dedicated AI infrastructure.

The logical model path is therefore:

text

```
AiX Web
    ■
    ▼
AI Server
    ■
    ▼
AI Engine
    ■
    ■■■■■■■ External LLM Services
    ■       OpenAI / Qwen / DeepSeek / ModelArts
    ■
    ■■■■■■■ Local LLM Services
            Ollama / vLLM
```

The AI Server coordinates the AI request, while the AI Engine performs the actual model-service interaction.

Scale-Out Architecture

AI Worker and AI Engine support multi-node deployment.

A basic deployment may use one AI Worker and one AI Engine:

text

```
AI Server
   ■
   ■■■ AI Worker
   ■
   ■■■ AI Engine
```

Larger deployments can introduce additional processing nodes:

text

```
AI Server
   ■
   ■■■ AI Worker
   ■      ■■■ Worker Node 1
   ■      ■■■ Worker Node 2
   ■      ■■■ Worker Node n
   ■
   ■■■ AI Engine
          ■■■ Engine Node 1
          ■■■ Engine Node 2
          ■■■ Engine Node n
```

AI Worker and AI Engine nodes can be assigned and routed according to **location** and **department**.

This supports scenarios such as:

- Additional processing capacity

- Workload distribution
- Department-specific processing
- Location-specific processing
- Dedicated AI model infrastructure
- Data locality requirements
- Controlled access to specific AI resources

AI processing capacity can therefore scale independently from the core application services.

AiX Console

The **AiX Console** provides centralized platform configuration and management information used by AiX services.

Configuration may include:

- Service registry information
- Service host names and ports
- System settings
- Model configuration
- Scheduler settings
- Monitoring and service status information
- User and system management settings

This allows service locations and infrastructure configuration to be managed centrally rather than hard-coded into individual AiX services.

Authentication

Authentication is provided as a separate platform capability.

AiX supports:

- Local authentication
- Microsoft Azure OAuth2 authentication
- Enterprise Single Sign-On through Keycloak

For enterprise SSO, Keycloak can operate as the **AiX SSO Bridge/Gateway**, providing a standardized integration layer between AiX and the customer's enterprise identity infrastructure.

Authentication establishes the user's identity, while AiX maintains application-level authorization such as user status, roles, permissions, and access to platform capabilities.

For additional information, see:

- Authentication Support
- SSO Integration Architecture

Deployment Architecture

AiX components are containerized and can be arranged according to the size and infrastructure requirements of the deployment.

The logical architecture remains consistent regardless of whether the services operate on one host or across multiple hosts.

Single-Host Deployment

For smaller deployments, multiple AiX services can operate as Docker containers on the same server or virtual machine.

For example:

text

```
■■■■■■■■■■■■■■■■■■■■■■ AiX Host / VM ■■■■■■■■■■■■■■■■■■■■■■■■■
■                                                              ■
■  Docker Network                                             ■
■                                                              ■
■  ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■■■  ■
■  ■App Server ■     ■ AI Server ■     ■ PostgreSQL  ■  ■
■  ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■■■  ■
■                                                              ■
■  ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■■■  ■
■  ■ AI Worker ■     ■ AI Engine ■     ■ AiX Console ■  ■
■  ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■     ■■■■■■■■■■■■■■■■■  ■
■                                                              ■
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

Containers on the same Docker network can communicate using **Docker service names and internal service ports**.

For example:

text

```
http://appserver:5080
http://aiserver:5085
http://aiengine:5084
http://aiworker:5087
http://console:5088
```

Internal container-to-container traffic does not need to be exposed publicly.

Where services communicate only within the same trusted Docker host and private Docker network, internal HTTP communication may be used while HTTPS/TLS is applied at externally exposed boundaries.

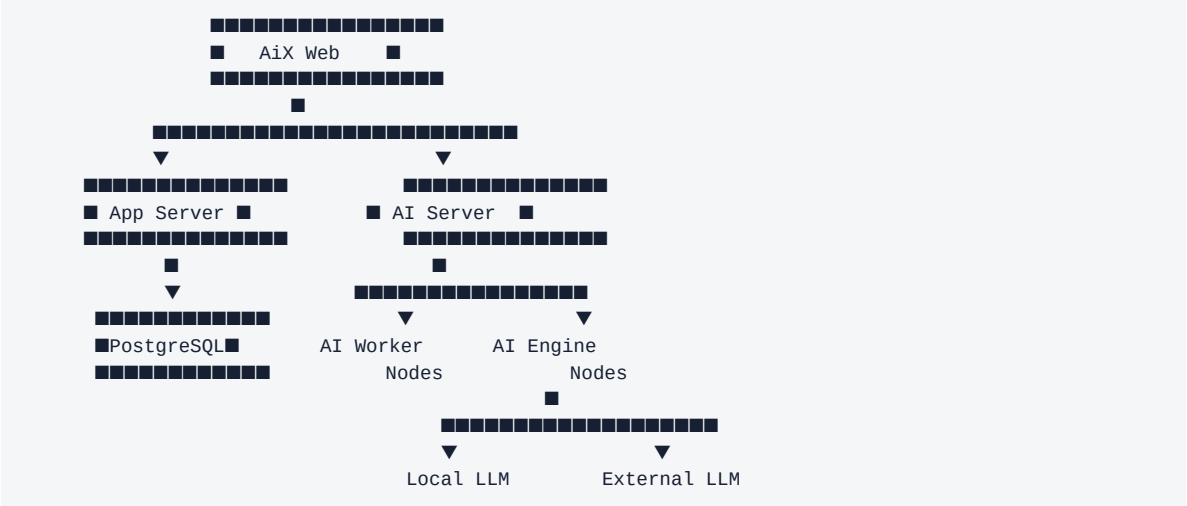
This reduces unnecessary certificate management between containers while maintaining network isolation and service-level authentication.

Multi-Host Deployment

For larger or scale-out deployments, AiX components can operate across separate servers, virtual machines, or infrastructure nodes.

For example:

text



When communication crosses host, VM, subnet, or other network boundaries, the communication should be protected according to the customer's network and security architecture.

Controls may include:

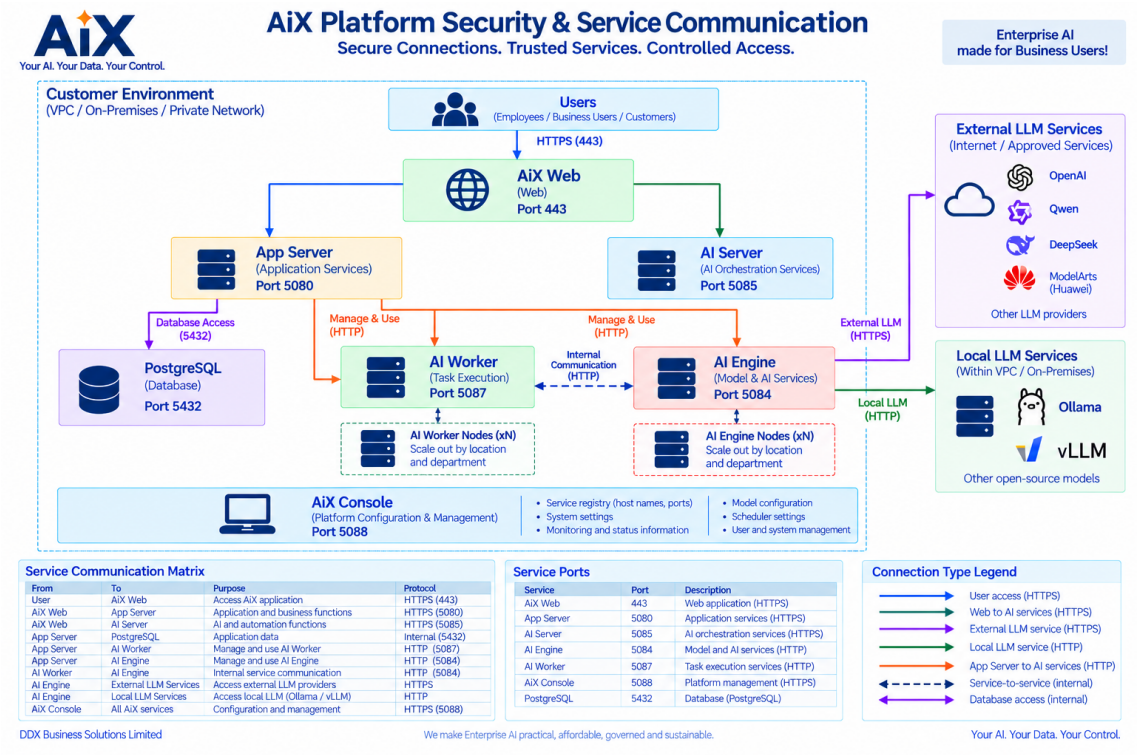
- Private VPC or internal network routing
- Network segmentation
- Firewall and security-group rules
- TLS where required across network boundaries
- Restricted service exposure
- Service-to-service authentication
- Approved outbound connectivity

The same logical AiX service architecture is therefore maintained while the physical deployment topology can evolve independently.

Security and Service Communication

The following diagram illustrates the principal service communication paths and standard service ports within the AiX platform.

<figure markdown="span">



AiX platform security and service communication

<figcaption>Figure: AiX Platform Security & Service Communication</figcaption>

</figure>

The communication architecture distinguishes between:

- User-facing HTTPS access
- Web-to-backend API communication
- Application database access
- AI orchestration
- Task and workflow execution
- Model-service communication
- Internal service-to-service communication
- External model-provider communication

Service Communication

The primary logical communication paths are:

| From | To | Purpose | | ---------- | ---------- | ---------- | | User | AiX Web | Access AiX applications | | AiX Web | App Server | Application and business functions | | AiX Web | AI Server | AI and automation functions | | App Server | PostgreSQL | Application data access | | App Server | AI Worker | Application services supporting task execution | | App Server | AI Engine | Application services supporting AI processing | | AI Server | AI Worker | Orchestrate Smartflows, scheduled tasks and background processing | | AI Server | AI Engine | Orchestrate AI and model operations | | AI Worker | AI Engine | Use AI/model capabilities during task execution | | AI Engine | External LLM Services | Access approved external model providers | | AI Engine |

Local LLM Services | Access locally hosted model services | | AiX Console | AiX Services | Platform configuration and service information |

The actual network protocol used for an internal connection depends on the deployment topology and security boundary.

Standard Service Ports

The standard AiX service ports are:

| Service | Port | Purpose | | ---------- | ---: | ---------- | | AiX Web | 443 | Web application / HTTPS | | App Server | 5080 | Application services | | AI Server | 5085 | AI orchestration services | | AI Engine | 5084 | Model and AI services | | AI Worker | 5087 | Task execution services | | AiX Console | 5088 | Platform configuration and management | | AiX SSO Bridge | 5090 | Enterprise SSO integration | | PostgreSQL | 5432 | Database service |

These ports identify the standard service endpoints. They do not imply that every port must be exposed outside the host or deployment environment.

In a containerized deployment, only services that require access from outside the internal Docker network should normally be published or exposed through the appropriate network boundary.

Service-to-Service Authentication

AiX uses a **platform credential** for trusted service-to-service authentication.

This is separate from end-user authentication:

text

```
User Authentication
        ■
        ■■■ Local
        ■■■ Azure OAuth2
        ■■■ Enterprise SSO
        ■
        ▼
      AiX User
   Roles & Permissions


Service Authentication
        ■
        ▼
Platform Credential
        ■
        ▼
Trusted AiX Service
```

The platform credential allows a receiving AiX service to verify that a request originates from an authorized platform service.

Network location alone should therefore not be treated as the only mechanism for establishing service trust.

Data Protection

AiX uses an application encryption key to protect sensitive stored information where application-level encryption is required.

Protected information may include items such as:

- Credentials
- Authentication tokens
- Sensitive configuration values
- Other protected application secrets

This is separate from encryption in transit.

HTTPS/TLS protects communication in transit where required, while the AiX encryption mechanism protects designated sensitive information handled or stored by the application.

Infrastructure-level protections such as encrypted disks, encrypted database storage, private networks, and cloud security controls may provide additional layers of protection depending on the deployment environment.

Network Exposure

AiX follows the principle that services should only be exposed to the networks that require access to them.

A typical deployment therefore separates:

text

```
External / User Access
        ■
        ■ HTTPS
        ▼
      AiX Web
        ■
        ▼
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
 Internal / Trusted Environment
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
 App Server
 AI Server
 AI Worker
 AI Engine
 AiX Console
 PostgreSQL
 Local LLM Services
```

Backend services, databases, workers, engines, and locally hosted model services should normally remain within the trusted deployment network unless there is a defined requirement to expose them through another controlled network boundary.

External LLM connectivity is initiated by **AI Engine** to approved model endpoints.

Deployment Models

AiX supports several deployment models:

- **Cloud**

- **On-Premises**
- **Hybrid**
- **Local**

The deployment model does not change the logical responsibilities of the AiX components.

A small deployment may consolidate services onto a single Docker host, while larger deployments can separate application, database, AI processing, and model infrastructure across multiple nodes.

This allows the platform to evolve from a compact deployment into a distributed architecture without changing the fundamental application design.

Architecture Principles

The AiX platform architecture follows several core principles:

Modular — Application, orchestration, processing, model, database, authentication, and management responsibilities are separated into defined services.

Scalable — AI Worker and AI Engine can scale independently through multi-node deployment and location or department-based routing.

Flexible — AiX supports cloud, on-premises, hybrid, and local deployment models together with external and locally hosted LLM services.

Secure by Design — External exposure, internal service communication, user authentication, service authentication, data protection, and network controls are treated as separate security layers.

Infrastructure Independent — The same logical architecture can operate on a single Docker host or across multiple infrastructure nodes.

Model Independent — AI Engine provides an abstraction layer that allows AiX to work with different external and local model services without directly coupling the application layer to a particular LLM provider.

Business-Oriented — The underlying service architecture supports AiX applications, Smartflows, Knowledge Bases, Assistants, scheduled automation, document processing, and other AI-enabled capabilities while abstracting the complexity of the underlying infrastructure.

Download Documentation

Prefer an offline or printable copy of this section?

Download Architecture (PDF)

The PDF contains the complete Architecture documentation for this release and is generated from the same documentation source as this website.

6.2 Authentication Support

Overview

AiX supports multiple authentication methods to accommodate different deployment environments, security requirements, and enterprise identity infrastructures.

Authentication is managed through the **AiX Auth Service**, which provides a consistent authentication and user management layer for the AiX platform.

AiX currently supports three primary authentication methods:

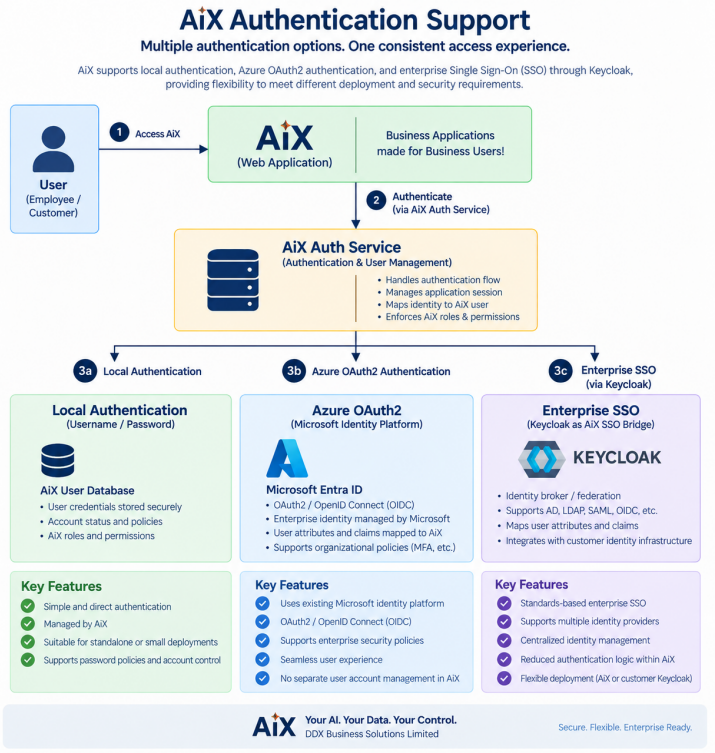
- **Local Authentication** – Username and password authentication managed directly by AiX.
- **Azure OAuth2 Authentication** – Authentication using Microsoft identity services through OAuth2 / OpenID Connect (OIDC).
- **Enterprise Single Sign-On (SSO)** – Enterprise identity integration through Keycloak, which acts as the **AiX SSO Bridge/Gateway**.

Regardless of the authentication method used, AiX maintains application-level user information, roles, permissions, and access controls.

Authentication Architecture

The following diagram illustrates the authentication methods supported by AiX and how they integrate through the AiX Auth Service.

<figure markdown="span">



AiX authentication support

<figcaption>Figure: AiX Authentication Support</figcaption> </figure>

The **AiX Auth Service** provides the common authentication layer between the AiX application and the configured authentication method.

This architecture allows the authentication mechanism to vary according to the deployment environment without requiring the AiX application itself to implement separate authentication flows for each identity platform.

Local Authentication

Local authentication provides direct username and password authentication using credentials managed by AiX.

The AiX Auth Service validates the supplied credentials against the AiX user database and establishes an application session when authentication is successful.

Local authentication can be used where an external identity provider is not available or where a deployment requires AiX-managed user authentication.

AiX remains responsible for the associated user account, account status, roles, permissions, and applicable authentication policies.

Azure OAuth2 Authentication

AiX supports authentication using the **Microsoft identity platform** through OAuth2 / OpenID Connect (OIDC).

With this authentication method, the user's identity is authenticated by Microsoft rather than through a locally managed AiX password.

The authentication result and associated identity information are returned to the AiX Auth Service, which maps the authenticated identity to the corresponding AiX user and establishes the AiX application session.

This approach allows organizations already using Microsoft identity services to use their existing enterprise identities and authentication policies when accessing AiX.

Enterprise Single Sign-On

For enterprise environments requiring integration with different or existing identity infrastructures, AiX supports Single Sign-On through **Keycloak**.

Keycloak acts as the **AiX SSO Bridge/Gateway**, providing an identity brokering and federation layer between AiX and the customer's enterprise identity infrastructure.

Depending on the customer environment, Keycloak can integrate with identity technologies such as:

- Microsoft Active Directory / LDAP
- Microsoft Entra ID
- SAML 2.0 identity providers
- OpenID Connect (OIDC) identity providers
- Existing customer-managed Keycloak environments
- Other identity providers supported through Keycloak

This architecture provides AiX with a standardized enterprise SSO integration while allowing the customer's existing identity infrastructure to remain responsible for user authentication.

For additional information about the enterprise SSO architecture, see AiX SSO Integration Architecture.

Authentication and Authorization

AiX separates **authentication** from **application authorization**.

Authentication determines and verifies the identity of the user. Depending on the configured authentication method, this may be performed by AiX, Microsoft identity services, or the customer's enterprise identity provider through Keycloak.

After authentication, the AiX Auth Service maps the authenticated identity to an AiX user.

AiX then applies application-level authorization, including:

- User account status
- Roles and permissions
- Module access
- Application access
- Other AiX-specific access controls

This separation allows organizations to retain control of their enterprise authentication policies while AiX independently manages application-level authorization.

Authentication Method Selection

The authentication method used for an AiX deployment depends on the customer's infrastructure and security requirements.

| Authentication Method | Authentication Provider | Typical Use | | ---------- | ---------- | ---------- | | **Local Authentication** | AiX | AiX-managed accounts or environments without an external identity provider | | **Azure OAuth2** | Microsoft identity platform | Organizations using Microsoft identities and OAuth2 / OIDC | | **Enterprise SSO** | Customer IdP through Keycloak | Enterprise environments requiring federation with existing identity infrastructure |

The supported authentication architecture allows AiX to operate in standalone, cloud, on-premises, and enterprise environments without coupling the AiX application directly to a specific identity technology.

Enterprise SSO Integration

Enterprise SSO is implemented as an additional integration layer rather than embedding customer-specific identity integrations directly within the AiX application.

The logical architecture is:

text

```
AiX
 ■
 ▼
AiX Auth Service
 ■
 ▼
```

```
Keycloak
(AiX SSO Bridge/Gateway)
 ■
 ▼
Customer Enterprise Identity Provider
```

This approach isolates AiX from differences between customer identity environments and provides a consistent integration point for enterprise authentication.

The detailed architecture, authentication flow, identity federation model, and Keycloak deployment options are described in AiX SSO Integration Architecture.

6.3 Authentication & SSO

Overview

AiX supports enterprise Single Sign-On (SSO) through a dedicated identity integration layer based on **Keycloak**.

Keycloak acts as the **AiX SSO bridge/gateway** between AiX and the customer's enterprise identity infrastructure. This approach provides AiX with a consistent authentication interface while allowing different customer environments to use their existing identity providers and authentication technologies.

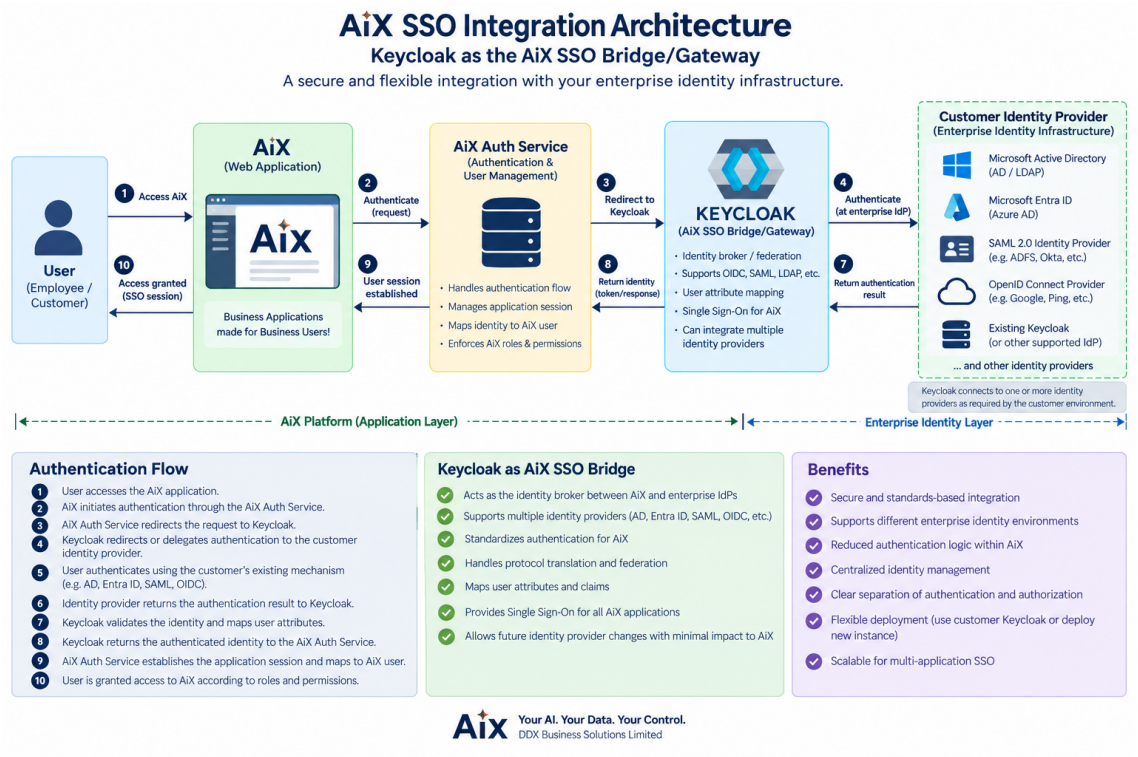
AiX integrates with Keycloak using standard authentication protocols such as **OpenID Connect (OIDC)**. Keycloak manages the connection to the customer's identity provider using the appropriate supported protocol or federation mechanism.

This architecture separates AiX application authentication from customer-specific identity infrastructure and reduces the need for AiX to implement separate authentication logic for each identity platform.

SSO Integration Architecture

The following diagram illustrates the logical integration between AiX, the AiX Auth Service, Keycloak, and the customer's enterprise identity infrastructure.

<figure markdown="span">



AiX SSO integration architecture

<figcaption>Figure: AiX SSO Integration Architecture</figcaption> </figure>

The architecture consists of four primary logical components:

- **AiX Application** – The application accessed by the user.
- **AiX Auth Service** – Manages the AiX authentication flow, application sessions, user identity mapping, and application-level authorization.
- **Keycloak (AiX SSO Bridge/Gateway)** – Provides the standardized identity integration layer between AiX and external enterprise identity providers.
- **Customer Identity Provider** – The customer's existing enterprise identity infrastructure responsible for authenticating the user.

Depending on the customer environment, the identity provider may include technologies such as:

- Microsoft Active Directory / LDAP
- Microsoft Entra ID
- SAML 2.0 identity providers
- OpenID Connect (OIDC) identity providers
- An existing customer-managed Keycloak environment
- Other identity platforms supported through Keycloak

Authentication Flow

When a user accesses AiX using enterprise SSO, the authentication process follows a standardized flow:

1. The user accesses the AiX application.

2. AiX initiates authentication through the AiX Auth Service.
3. The AiX Auth Service redirects the authentication request to Keycloak.
4. Keycloak identifies the configured customer identity provider and redirects or delegates authentication accordingly.
5. The user authenticates using the customer's existing authentication mechanism.
6. The customer identity provider returns the authentication result to Keycloak.
7. Keycloak validates the identity and maps the required user attributes and claims.
8. Keycloak returns the authenticated identity to the AiX Auth Service.
9. The AiX Auth Service maps the authenticated identity to the corresponding AiX user and establishes the application session.
10. The user is granted access to AiX according to the roles and permissions configured within AiX.

Authentication and Authorization Separation

The AiX SSO architecture separates **enterprise authentication** from **application authorization**.

The customer's identity provider is responsible for authenticating the user and establishing the user's enterprise identity.

Keycloak provides the identity brokering and federation layer between the customer's identity environment and AiX. It normalizes the authentication process so that AiX can use a consistent integration regardless of the underlying enterprise identity provider.

The AiX Auth Service remains responsible for AiX-specific application access, including:

- Mapping the authenticated identity to an AiX user
- User account status
- AiX roles and permissions
- Module and application access
- Application session management

This separation allows enterprise authentication policies to remain under the control of the customer's identity infrastructure while AiX maintains control over application-level authorization.

Keycloak as the AiX SSO Bridge/Gateway

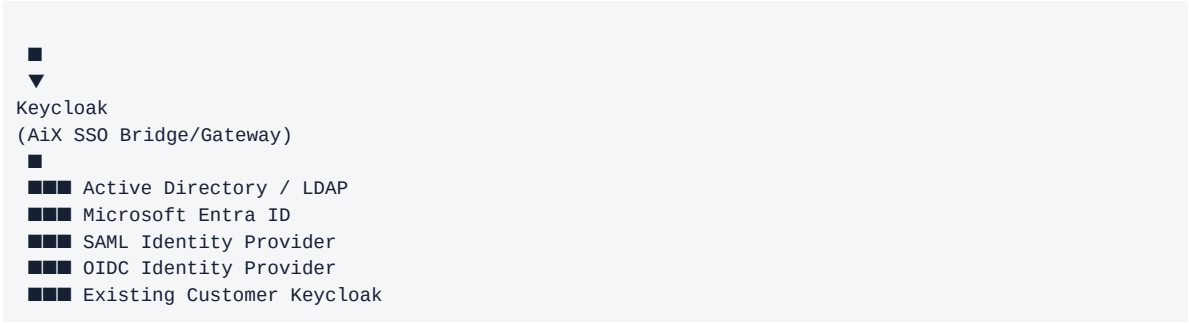
Keycloak provides an abstraction layer between AiX and the customer's identity infrastructure.

Instead of implementing separate authentication integrations within AiX for each identity technology, AiX communicates through a standardized Keycloak integration.

For example:

text

```
AiX
 ■
 ▼
AiX Auth Service
```



If the customer's identity infrastructure changes in the future, the corresponding integration can generally be handled at the Keycloak layer without requiring the AiX application authentication architecture to be redesigned.

Deployment Models

The Keycloak integration layer supports different deployment models depending on the customer's existing infrastructure.

AiX-Provided Keycloak

Where the customer does not already operate a suitable Keycloak environment, a dedicated Keycloak instance can be deployed as part of the AiX SSO integration architecture.

The deployed Keycloak instance acts as the AiX SSO bridge between AiX and the customer's identity infrastructure.

Customer-Managed Keycloak

Where the customer already operates Keycloak, AiX may integrate with the customer's existing Keycloak environment, subject to the customer's architecture, security policies, and configuration requirements.

In this deployment model, an additional AiX-specific Keycloak instance may not be required.

Architecture Benefits

The AiX SSO bridge/gateway architecture provides:

- Standards-based enterprise SSO integration
- Separation between AiX and customer-specific identity infrastructure
- Support for different enterprise identity technologies
- Centralized identity federation and protocol handling
- Reduced authentication-specific logic within AiX
- Consistent authentication integration across customer environments
- Flexibility to accommodate future identity infrastructure changes
- Clear separation between enterprise authentication and AiX authorization

The architecture therefore allows AiX to maintain a consistent authentication model while integrating with the identity infrastructure and security policies already established within the customer's enterprise environment.

7. Deployment

7.1 Overview

■# Deployment Overview

AiX supports controlled deployment through UAT and Production environments.

Mermaid diagram source

```
flowchart LR
    Build[Approved Release] --> UAT[UAT]
    UAT --> Acceptance[Validation / Acceptance]
    Acceptance --> Prod[Production]
```

Promote the same approved release artifacts from UAT to Production; do not rebuild application artifacts specifically for Production.

Download Documentation

Prefer an offline or printable copy of this section?

Download Deployment (PDF)

The PDF contains the complete Deployment documentation for this release and is generated from the same documentation source as this website.

7.2 Environment Requirements

Document supported operating systems, container runtime, compute, storage, network, database, TLS, DNS, identity, and AI service prerequisites.

7.3 UAT Deployment

- [ ] Release identified
- [ ] Environment prerequisites confirmed
- [ ] Configuration validated
- [ ] Database migration reviewed
- [ ] Services deployed
- [ ] Health checks passed
- [ ] Integrations tested
- [ ] UAT completed

7.4 UAT to Production

Mermaid diagram source

```
flowchart TD
    UAT[UAT Release] --> Pass{Accepted?}
    Pass -->|No| Fix[Correct and Retest]
    Pass -->|Yes| Approve[Production Approval]
```

```
Approve --> Backup[Production Backup]
Backup --> Rollback[Confirm Rollback Plan]
Rollback --> Deploy[Deploy Same Release Artifacts]
Deploy --> Smoke[Production Smoke Test]
Smoke --> Result{Pass?}
Result -->|Yes| Live[Release Live]
Result -->|No| Backout[Rollback]
```

7.5 Production Checklist

- [ ] UAT accepted
- [ ] Release manifest confirmed
- [ ] Image digests confirmed
- [ ] Backup completed
- [ ] Restore/rollback readiness confirmed
- [ ] Database migration approved
- [ ] Production configuration validated
- [ ] Services healthy after deployment
- [ ] Authentication tested
- [ ] Integrations tested
- [ ] Critical workflows tested

7.6 Rollback

Every production release should identify the previous release, application rollback method, database rollback/restore approach, configuration rollback, validation steps, and responsible parties.

7.7 Upgrade Procedure

Document the standard AiX upgrade lifecycle: release review, backup, UAT deployment, validation, approval, Production promotion, smoke testing, and rollback readiness.

8. Integration

8.1 Overview

■# Keycloak

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

Download Documentation

Prefer an offline or printable copy of this section?

Download Integration (PDF)

The PDF contains the complete Integration documentation for this release and is generated from the same documentation source as this website.

8.2 Overview

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.3 Keycloak

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.4 Active Directory

Document supported Active Directory/LDAP integration patterns, normally through the approved identity bridge architecture.

8.5 LDAP

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.6 SAML

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.7 Kerberos

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.8 Overview

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.9 Microsoft Entra ID

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

8.10 Microsoft 365

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

9. Security

9.1 Overview

■# Keycloak

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

Download Documentation

Prefer an offline or printable copy of this section?

Download Security (PDF)

The PDF contains the complete Security documentation for this release and is generated from the same documentation source as this website.

9.2 Security Architecture

Document standard AiX security boundaries, authentication, authorization, encryption assumptions, network controls, secrets handling, auditability, and deployment responsibilities.

9.3 Authentication & Access Control

Document standard AiX audit events, AI interaction logging, retention considerations, and administrative access.

9.4 Audit Logging

Document standard AiX audit events, AI interaction logging, retention considerations, and administrative access.

9.5 Data Protection

Document standard AiX audit events, AI interaction logging, retention considerations, and administrative access.

9.6 Provenance

Document standard AiX provenance identifiers, metadata handling, output marking, and traceability behavior.

10. Troubleshooting

10.1 Overview

■# Troubleshooting Overview

Use a consistent diagnostic sequence: identify environment and release, confirm service health, reproduce safely, inspect relevant logs/metrics, isolate the component, apply an approved corrective action, and record the outcome.

Never place credentials, tokens or sensitive customer content in troubleshooting documentation.

Download Documentation

Prefer an offline or printable copy of this section?

Download Troubleshooting (PDF)

The PDF contains the complete Troubleshooting documentation for this release and is generated from the same documentation source as this website.

10.2 Installation

Document common installation/container, configuration, dependency, port, DNS/TLS and startup issues and their supported diagnostic procedures.

10.3 Authentication

Document safe diagnostics for AiX Auth Service, Keycloak/OIDC, identity-provider connectivity, redirect/issuer configuration, claims and role mapping. Never record tokens or secrets.

10.4 Database

Document supported checks for connectivity, schema/migration status, capacity, permissions and database health.

10.5 Storage

Document checks for paths/mounts, permissions, capacity, network storage connectivity and container volume mappings.

10.6 AI Models

See AI Model Troubleshooting for the primary model diagnostic procedure. This page can contain cross-component incidents involving AiX application services and AI runtimes.

10.7 Smartflow

Document diagnostics for workflow validation, execution state, worker availability, tool/input/output errors, timeouts and execution logs.

10.8 Performance

Correlate user-observed latency with application response time, worker load, database/storage performance and local/external model latency before changing capacity or configuration.

10.9 General

Document safe diagnostic procedures, common symptoms, logs, escalation information, and approved corrective actions. Never include secrets in examples.

11. Upgrade & Migration

11.1 Overview

■# Troubleshooting Overview

Use a consistent diagnostic sequence: identify environment and release, confirm service health, reproduce safely, inspect relevant logs/metrics, isolate the component, apply an approved corrective action, and record the outcome.

Never place credentials, tokens or sensitive customer content in troubleshooting documentation.

Download Documentation

Prefer an offline or printable copy of this section?

Download Upgrade & Migration (PDF)

The PDF contains the complete Upgrade & Migration documentation for this release and is generated from the same documentation source as this website.

11.2 Upgrade Planning

Use a consistent diagnostic sequence: identify environment and release, confirm service health, reproduce safely, inspect relevant logs/metrics, isolate the component, apply an approved corrective action, and record the outcome.

Never place credentials, tokens or sensitive customer content in troubleshooting documentation.

11.3 Upgrade Procedure

Use a consistent diagnostic sequence: identify environment and release, confirm service health, reproduce safely, inspect relevant logs/metrics, isolate the component, apply an approved corrective action, and record the outcome.

Never place credentials, tokens or sensitive customer content in troubleshooting documentation.

11.4 Database Migration

Use a consistent diagnostic sequence: identify environment and release, confirm service health, reproduce safely, inspect relevant logs/metrics, isolate the component, apply an approved corrective action, and record the outcome.

Never place credentials, tokens or sensitive customer content in troubleshooting documentation.

11.5 Rollback

Use a consistent diagnostic sequence: identify environment and release, confirm service health, reproduce safely, inspect relevant logs/metrics, isolate the component, apply an approved corrective action, and record the outcome.

Never place credentials, tokens or sensitive customer content in troubleshooting documentation.

12. Release Notes

12.1 Overview

■# Keycloak

Document the standard supported AiX-to-Keycloak integration model. Customer realm names, URLs, mappings, and deployment-specific settings belong in customer documentation.

Download Documentation

Prefer an offline or printable copy of this section?

Download Release Notes (PDF)

The PDF contains the complete Release Notes documentation for this release and is generated from the same documentation source as this website.

12.2 Release Template

Release Summary

- Version:
- Release date:
- Documentation version:

Components

| Component | Version / Image | Digest | |---|---|---| | Web | | | | App Server | | | | AI Server | | | | AI Worker | | | | AI Engine | | |

Changes

Added

Changed

Fixed

Security

Upgrade Notes

Known Issues