AiX Administration

v2026.3

DDX Business Solutions Limited

Customer Reference

Table of Contents

1. Administration

1.1 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.

1.2 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.

1.3 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.

1.4 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.

1.5 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

1.6 License Activation