Skillmine
Technology ▪ Consulting ▪ Services

Skillmine Auth

Partner Pre-Sales Technical Enablement

Unified Identity, Access & Governance Platform



Enablement Deck Purpose

This deck enables partner pre-sales teams to understand, position, and operationalize Skillmine Auth as an enterprise IAM execution platform.

IAM Capabilities Covered

- Single Sign-On (SSO) across web, SaaS, and thick clients
- Multi-Factor Authentication including Windows MFA and advanced methods
- User Lifecycle Management (ULM) using SCIM-based connectors
- Deployment, integration prerequisites, and partner readiness

What Partners Will Be Able to Do

- Position Skillmine Auth confidently in IAM discussions
- Explain SSO, MFA, and ULM working models to customers
- Scope integrations realistically and avoid over-commitment
- Prepare for demos and initial implementations

Scope Clarity

- Focused on authentication, MFA, and user lifecycle execution
- Governance-heavy features and deep authorization are intentionally out of scope
- ACLM discussed as an extension, not a starting point

Product Overview: Skillmine Auth

An IAM execution platform designed for real enterprise environments

What Skillmine Auth Is

- Enterprise Identity & Access Management (IAM) execution platform
- Focused on authentication, MFA, and user lifecycle operations
- Built for real-world enterprise deployment scenarios
- Designed for fast rollout and predictable integrations

What Skillmine Auth Does Best

- Enables rapid Single Sign-On across web, SaaS, and thick-client applications
- Provides comprehensive MFA including Windows MFA and advanced methods
- Delivers practical User Lifecycle Management using SCIM-based connectors
- Enforces centralized access and authentication policies consistently

Deployment & Operational Flexibility

- Docker-based deployment model for infrastructure flexibility
- Supports on-prem, private cloud, and hybrid environments
- Allows organizations to retain control over identity infrastructure
- Enables data residency, network isolation, and operational governance

Execution Advantage Over Cloud-Only IAM

- Does not mandate SaaS-only identity control
- Integrates into existing enterprise infrastructure without disruption
- Fits environments where cloud-only IAM tools are restrictive
- Balances security, control, and deployment flexibility

Why Skillmine Auth: Key Differentiators

Built for enterprises where cloud-only IAM falls short

Adaptive & Region-Relevant MFA

- Pattern-based (PIP) MFA resistant to shoulder-surfing
- Offline OTP / Backup Codes for restricted or OT environments
- WhatsApp OTP for India & APAC user adoption
- Designed for environments with limited phone/email access

Partner angle: MFA that aligns with real user and regulatory constraints

Core IAM Capabilities, Executed Well

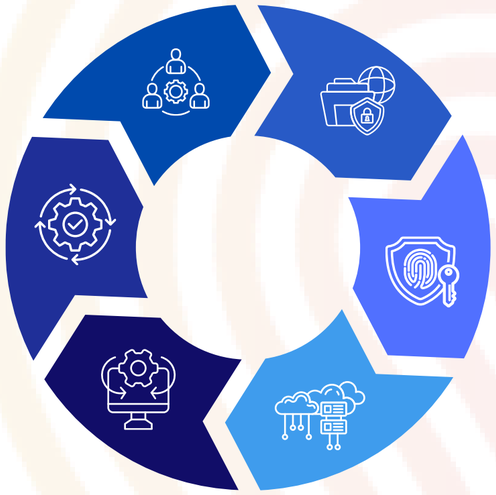
- Enterprise SSO across web, SaaS, thick & legacy clients
- Wide MFA coverage: standard + advanced methods
- SCIM-based connectors enabling ULM and ACLM
- Proven execution, not just feature availability

Partner angle: Strong IAM fundamentals with predictable delivery

Legacy & In-House Application Modernization

- Native Oracle IDP EBS integration (no heavy middleware dependency)
- Secures legacy enterprise applications directly
- REST APIs & SDKs for in-house or custom applications
- No protocol dependency if APIs are available

Partner angle: Simplifies IAM for legacy and custom-built environments



Windows & RDP-Level MFA Protection

- Secures local Windows logins
- Protects RDP, Citrix, and VMware sessions
- Covers shared desktops and server access
- Extends IAM controls beyond browser-based apps

Partner angle: IAM at the OS and infrastructure layer

Zero-Trust, Context-Aware Authentication

- “Never trust, always verify” enforced in real time
- Evaluates device context, IP reputation, user behavior
- Supports alerts, step-up MFA, or access blocking
- Policies enforced centrally via Skillmine Auth

Partner angle: Practical Zero Trust without complexity

True Hybrid & Air-Gapped Deployment

- SaaS, On-Prem, Private Cloud, or Air-Gapped
- No forced dependency on public cloud IAM
- Supports data residency and network isolation
- Suitable for government, defense, and regulated sectors

Partner angle: IAM that adapts to customer infrastructure, not vice-versa

Core Modules Summary

Single Sign-On (SSO)

- SAML 2.0
- OAuth 2.0 / OIDC
- Kerberos / RADIUS
- WS-Federation
- Legacy app support via APIs
- Seamless login
- Reduced passwords

Outcome: Unified authentication across diverse application types

Multi-Factor Authentication (MFA)

- Adaptive MFA
- Windows MFA
- Advanced factors
- Policy-driven

Outcome: Strong authentication beyond passwords

User Lifecycle Management (ULM)

- User provisioning
- De-provisioning
- Attribute sync
- Lifecycle control

Outcome: Automated onboarding and exits across applications

Provisioning & Connectors

- SCIM-based
- API-driven
- App integrations
- Scalable framework

Outcome: Consistent user propagation across systems

Directory Services

- Central identity
- LDAP compatible
- Attribute store
- User repository

Outcome: Single source of truth for identities

SSO Overview: Protocols & Application Support

Supported Protocols

- SAML 2.0 for enterprise web applications
- OpenID Connect (OIDC) & OAuth for modern cloud apps
- WS-Federation for Microsoft-based environments
- Kerberos & RADIUS for Server integrated authentication

Application Types

- Web-based applications (browser SSO)
- SaaS platforms (cloud applications)
- Thick client applications (desktop software)
- Legacy systems via REST API

Multi-Factor Authentication Options in Skillmine Auth

Standard MFA Methods

- **SMS OTP** — Telecom-based OTP
- **Push Notification** — App-based approval
- **TOTP** — Time-based OTP
- **Email OTP** — Email-delivered OTP
- **Pattern MFA** — User-defined pattern
- **WhatsApp OTP** — Messaging-based OTP

Advanced MFA Methods

- **Windows MFA** — OS-level authentication
- **FIDO** — Hardware-backed authentication
- **PIP MFA** — Pattern-based grid authentication
- **Offline OTP (Windows MFA)** — No network dependency
- **Biometrics** — Device-based authentication
- **HOTP** — Counter-based OTP
- **QR Code** — Scan QR to validate

Skillmine Authenticator App

Available on **Google Play Store** and **Apple App Store**

Mandatory for

- Push Notification
- Pattern MFA
- Offline OTP

Optional for

- TOTP

Not required for:

- SMS OTP
- Email OTP
- WhatsApp OTP

Purpose: Enables advanced and offline authentication scenarios.

MFA availability depends on user environment, device access, and configured security policy.

Security & Policy Enforcement

Location-Based Access Enforcement



- Country rules
- Region controls
- Geo allow/deny

Use case: Block or allow access based on user location

Network-Based Access Enforcement



- IP whitelisting
- VPN restriction
- Network trust

Use case: Limit access to trusted networks only

Time-Based Access Enforcement



- Business hours
- Shift windows
- Time policies

Use case: Enforce access only during approved time windows

Anomaly-Driven Risk Response



- Behavior anomalies
- Impossible travel
- Risk scoring

Action: Alert, step-up MFA, or block access

Context-Aware Authentication



- Device context
- Network context
- User behavior

Use case: Dynamic authentication based on real-time risk

All security and access policies are enforced centrally through Skillmine Auth without requiring application-side changes.

Windows MFA Agent — Technical Specifications

Where Windows MFA Is Applied

- Shared desktops
- RDP sessions
- Citrix environments
- VMware Horizon
- Server logins

Use case: Secure access in shared, remote, and virtualized Windows environments

Supported Platforms

- Windows 8.1+ (endpoints)
- Windows Server 2016+
- Domain & workgroup machines
- 64-bit systems

Coverage: Endpoints, servers, and VDI environments

Deployment Model

- Agent-based MFA
- Client-side install
- Server-side policy
- Central control

Control point: Authentication enforced by Skillmine Auth

Installation & Connectivity

- MSI / GPO deployment
- Admin privileges
- HTTPS (443)
- Auth server connectivity

Requirement: Network reachability to Skillmine Auth

Authentication Capabilities

- Primary login MFA
- Step-up MFA
- Offline OTP support
- PIP-based MFA

Outcome: Strong authentication even in low-connectivity or shared-device scenarios

Enterprise Connectors: Capability Model

Basic Connector

- SCIM-based
- REST APIs
- Unidirectional sync
- Auth → Application
- Lifecycle-focused

Capabilities Enabled

User Lifecycle Management via Auth (ULM)

- User create
- User update
- User disable
- User delete

Operational Scope

- Central control
- Managed login access mapping
- No app-side roles

Advanced Connector

- SCIM + APIs
- Bi-directional sync
- Auth ↔ Application
- Lifecycle + access
- App-aware

Capabilities Enabled

User Lifecycle Management (ULM)

- Full sync
- Two-way updates

Access Control Lifecycle Management (ACLM)

- Role assignment
- Group mapping
- Entitlement control
- Dashboard access

Operational Scope

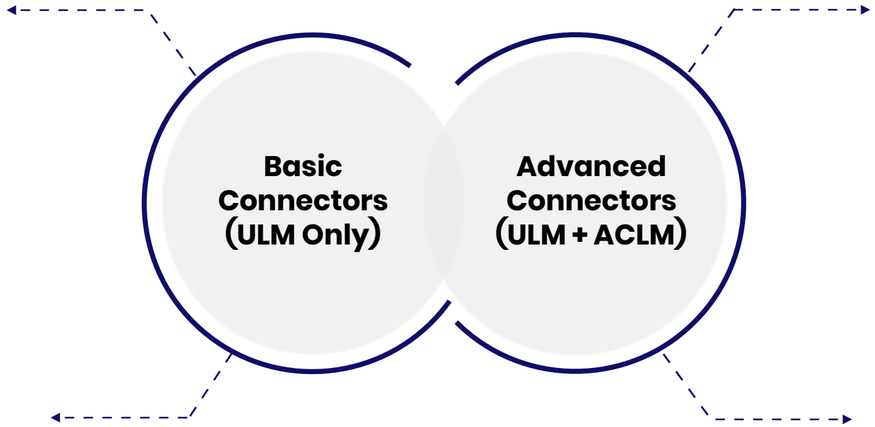
- Central governance
- App-level control
- Policy-driven access

Connector capability depends on application SCIM support and exposed APIs.

Enterprise Connectors: Representative Coverage Model

Supported Applications

salesforce · workday · Microsoft Azure · aws · SAP · ORACLE · ATLASSIAN · servicenow · slack · GitLab



Supported Applications

Google Workspace · Microsoft 365 · adrenalin® Transformative Digital HR

Capability Scope

- User create
- User update
- User disable
- User delete

Lifecycle Direction

- Auth → Application

Capability Scope

- User lifecycle sync
- Role assignment
- Group mapping
- Access control

Lifecycle Direction

- Auth → Application

Note: Connector capability depends on SCIM protocol support and exposed APIs of the target application. Additional connectors can be developed only when required SCIM support and APIs are available.

Provisioning Capabilities

Provisioning Spectrum in Skillmine Auth

- Centralized provisioning platform
- SCIM-driven automation
- Application-aware lifecycle control

User Lifecycle Management (ULM)

What ULM Enables

- User create
- User update
- User disable
- User delete

Sync Model

- One-way provisioning (default)
- Bi-directional sync (select platforms)

Supported Bi-directional Platforms

- Microsoft 365
- Google Workspace
- HrOne
- Adrenalin

Value Delivered

- Faster onboarding
- Clean offboarding
- Reduced access drift

Access Control Lifecycle Management (ACLM)

What ACLM Enables

- Role assignment
- Group membership
- Entitlement control
- Application-level access

Control Model

- Central assignment via Skillmine Auth
- Policy-driven access propagation

Value Delivered

- Consistent access enforcement
- Reduced manual role management

Windows MFA Agent — Technical Specifications

What Provisioning Does NOT Do

- Does not auto-discover application role models
- Does not replace application authorization logic
- Does not infer dashboards or permissions
- Does not bypass application API limitations

When to Lead with ULM (Recommended)

- HRMS-driven onboarding/offboarding
- Multiple applications with manual user management
- Compliance or audit-driven identity cleanup
- Quick-win IAM initiatives

Partner guidance

- Easy to scope
- Fast to demonstrate
- Low dependency on application teams

When to Position ACLM Carefully

- Application role matrix is clearly defined
- APIs expose role/group management
- Application owners are aligned
- Governance ownership is identified

Partner guidance

- Position as Phase 2
- Validate before committing
- Scope jointly with customer teams

Real-World Provisioning Example

- HRMS user create/update/exit
- Skillmine Auth detects lifecycle change
- Central sync completed in Auth
- Changes propagated to Microsoft 365, GitLab, Salesforce, and other integrated applications

Provisioning depth depends on SCIM support, exposed APIs, and application role model maturity.
ULM is broadly supported; ACLM is application-dependent.

Deployment Architecture

Docker containerized microservices architecture

Horizontal scaling with load balancer support



High availability with multi-node clustering

Automated failover and health monitoring

Infrastructure Specifications

Minimum Requirements

- 2 vCPU cores
- 4 GB RAM
- 200 GB SSD storage
- 1 Gbps network interface

Supports up to 1,000 registered users with 40% concurrency

Recommended Production

- 8 vCPU cores
- 32 GB RAM
- 500 GB SSD storage
- 10 Gbps network interface

Supports up to 10,000 registered users with 40% concurrency

Enterprise Scale

- 16+ vCPU cores
- 64+ GB RAM
- 1+ TB SSD storage
- 10+ Gbps network interface

Clustered deployment for 20,000+ registered users with 40% concurrency

All deployments require HTTPS/443 inbound, SMTP for notifications, and network connectivity to integrated applications. Firewall rules must permit container-to-container communication within the deployment subnet.

Important: These specs apply only to single-node deployments of Auth. The HA & DR setup will have a different and separate requirements.

Partner Capability Checklist

Infrastructure Readiness

- Provision Docker infrastructure
- Configure networking
- Establish database connectivity
- Verify SSL certificate installation

SSO Configuration

- Configure SAML 2.0 or OIDC integration with target applications
- Establish metadata exchange
- Validate authentication flows

MFA Setup in Admin UI

- Enable MFA methods per application
- Configure policy enforcement rules
- Assign MFA requirements to user groups or roles

SCIM Connector Configuration

- Generate API keys for SCIM endpoints
- Map attribute schemas
- Configure provisioning workflows

Policy Restriction Setup

- Define geographic, IP, and time-based access policies
- Configure anomaly detection thresholds
- Establish exception workflows

Windows MFA Agent Deployment

- Deploy agent via Group Policy or SCCM
- Configure server communication endpoints
- Test RDP, Citrix, and VMware integration
- Validate credential provider registration