SAP Central User Administration (CUA): Comprehensive Guide to End-of-Life Strategy and Migration Pathways

Foreword: The Identity Management Crossroads

Picture this scenario: A global manufacturing company with 15,000 SAP users across 30 countries discovers during a routine security audit that it takes an average of three days to fully deprovision an employee who has left the company. During those three days, the former employee retains access to critical financial systems, supply chain data, and customer information. The IT team, stretched thin managing 47 different SAP instances through Central User Administration (CUA), struggles with manual processes that haven't fundamentally changed since their SAP implementation in 2003.

This isn't an isolated case. Across the SAP ecosystem, thousands of organisations find themselves at a critical juncture where their trusted identity management approach—CUA—no longer meets the demands of modern business. The technology that once revolutionised SAP user management by centralising control now represents a significant risk and operational bottleneck in an era of cloud computing, zero-trust security, and stringent regulatory compliance.

Executive Summary: Understanding the Real Challenge

The Fundamental Problem

The challenge facing SAP customers isn't simply that CUA might be discontinued—it's that **CUA has become dangerously inadequate for modern enterprise requirements** whilst organisations have grown deeply dependent on it. This creates a precarious situation:

The Technical Debt Crisis:

- CUA was designed for a world of on-premise systems and trusted networks
- Modern enterprises operate hybrid clouds with SaaS applications CUA cannot reach
- Security threats have evolved from password theft to sophisticated identity-based attacks
- Regulatory requirements demand capabilities CUA was never designed to provide

The Strategic Dilemma: Organisations face three uncomfortable truths:

1. **CUA won't evolve**: SAP has ceased all feature development, meaning no OAuth support, no cloud integration, no modern security features will ever come to CUA
2. **The alternatives are complex and costly**: Every replacement option requires significant investment in money, time, and organisational change
3. **Doing nothing is increasingly risky**: Each month of delay increases security exposure and compliance risk

Why This Matters Now

Three converging factors make this challenge urgent:

1. The SAP IDM Deadline Creates Market Pressure Whilst CUA itself has no end date, SAP Identity Management—long positioned as CUA's successor—reaches end-of-maintenance on 31 December 2027. This affects approximately 3,000 enterprises who must migrate, creating:

- Massive demand for migration resources
- Consultant shortage and price inflation
- Vendor capacity constraints
- Rushed, risky implementations for latecomers

2. The Security Landscape Has Fundamentally Changed Recent high-profile breaches demonstrate that identity is the new security perimeter:

- 82% of breaches involve compromised credentials
- Average breach cost: $4.88 million in 2024
- Ransomware attacks specifically target privileged accounts
- Supply chain attacks exploit identity federation weaknesses

3. Digital Transformation Demands Modern Identity Business initiatives are blocked by CUA limitations:

- Cloud migration projects stall without proper identity federation
- Mobile workforce enablement requires modern authentication
- Partner ecosystem integration needs standards-based protocols

- Automation initiatives require API-driven identity management

Part I: The Evolution of a Crisis—How We Got Here

The Golden Age of CUA (1999-2010)

When SAP introduced Central User Administration in R/3 4.6, it addressed a genuine pain point. Enterprises running dozens of SAP systems faced an administrative nightmare: creating the same user across multiple systems, maintaining consistent passwords, ensuring uniform role assignments. CUA offered elegant simplicity:

- One central system to rule them all
- Automatic distribution via proven ALE/IDoc technology
- No additional licensing costs
- Integration with existing SAP security models

For a decade, CUA represented best practice. It was the obvious choice for any organisation running multiple SAP systems. The technology was stable, reliable, and sufficient for the security requirements of the time.

The Cracks Begin to Show (2010-2020)

As enterprises evolved, CUA's limitations became apparent:

The Rise of Compliance Requirements: Post-Enron regulations like Sarbanes-Oxley demanded:

- Detailed audit trails of who approved access
- Segregation of duties analysis
- Periodic access reviews and certifications
- Evidence of control effectiveness

CUA provided none of these capabilities. Organisations began bolting on GRC tools, creating complex, fragmented identity landscapes.

The Cloud Revolution: As organisations adopted Salesforce, Office 365, and eventually SAP's own cloud solutions, they discovered:

- CUA couldn't manage cloud application access
- No support for SAML or OAuth protocols
- Inability to integrate with cloud identity providers
- Separate identity silos for cloud vs on-premise

The Security Evolution: Modern attacks exposed CUA's security model as obsolete:

- No multi-factor authentication capability
- Static passwords vulnerable to phishing
- No risk-based authentication
- Inability to detect anomalous access patterns
- No integration with Security Information and Event Management (SIEM) systems

The Current State: A Platform Under Siege (2020-Present)

Today's reality presents a stark picture:

Technical Limitations Create Real Business Impact:

- **Customer Experience**: Partners and customers cannot use single sign-on, forcing multiple passwords and degraded user experience
- **Employee Productivity**: Workers lose 2-3 hours weekly to password resets and multiple logins
- **Security Posture**: Average time to detect compromise: 204 days, partly due to inadequate identity monitoring
- **Compliance Failures**: 43% of organisations fail identity-related audit controls

The Hidden Costs of Maintaining Status Quo: A 5,000-user organisation typically incurs:

- £250,000 annually in manual administration overhead
- £180,000 in help desk costs for password resets
- £500,000 in audit findings and remediation
- £2-5 million exposure from potential breach risk
- Immeasurable opportunity cost from delayed digital initiatives

Part II: Understanding the Challenge—What Makes This So Difficult?

The Dependency Web

CUA isn't just a tool—it's woven into the fabric of SAP operations:

Technical Dependencies:

- Custom ABAP programs expect CUA table structures
- Interfaces rely on CUA-distributed user IDs
- Batch jobs run under CUA-managed technical users
- Monitoring tools parse CUA logs for alerts
- Archive systems reference CUA user data

Process Dependencies:

- HR onboarding procedures assume CUA workflows
- Security policies written around CUA capabilities
- Audit procedures based on CUA reports
- Training materials featuring CUA transactions
- Support runbooks detailing CUA procedures

Organisational Dependencies:

- Basis teams whose primary skill is CUA administration
- Security teams organised around CUA's limitations
- Budget models assuming zero licensing cost
- Service level agreements based on CUA performance
- Vendor contracts referencing CUA-managed accounts

The Skills Gap Challenge

Modern identity management requires fundamentally different expertise:

Current CUA Skills (ABAP-Centric):

- Transaction code navigation
- ALE/IDoc configuration
- RFC destination management
- ABAP debugging capabilities
- SAP authorisation concepts

Required Modern IAM Skills:

- REST API integration
- OAuth/SAML configuration
- Cloud platform administration
- DevOps automation tools
- Zero-trust architecture principles

This isn't simply additional training—it's a paradigm shift requiring different mindsets, tools, and approaches.

The Cost Shock Reality

The financial impact catches many organisations unprepared:

From Free to Fee:

- CUA: £0 licensing cost
- Modern alternatives: £50-200 per user annually
- For 5,000 users: £250,000-1,000,000 yearly

Implementation Investment: Beyond licensing, organisations face:

- Professional services: £500,000-3,000,000
- Internal resource costs: £200,000-500,000
- Training and certification: £50,000-150,000
- Parallel running costs: £100,000-300,000

The Small Organisation Dilemma: Smaller companies face proportionally higher costs:

- Minimum implementation costs regardless of size

- Same complexity despite fewer users
- Limited negotiating power with vendors
- Difficulty achieving ROI at small scale

Part III: Strategic Options—Choosing Your Path Forward

Option 1: The SAP Cloud Identity Services Route

What It Is: SAP's strategic platform comprising Identity Authentication Service (IAS), Identity Provisioning Service (IPS), and Identity Directory Service (IdDS).

The Value Proposition:

- Native SAP solution with guaranteed long-term support
- Included with many SAP cloud subscriptions
- Deep integration with S/4HANA and SAP cloud applications
- Designed for hybrid scenarios

Real-World Application: A European retailer with 3,000 users migrated from CUA to SAP Cloud Identity Services:

- **Implementation**: 14 months
- **Cost**: €450,000 total (mostly professional services)
- **Benefits**: 60% reduction in provisioning time, unified access to cloud and on-premise systems
- **Challenges**: Limited governance capabilities required additional GRC investment

When to Choose This Path:

- Heavy investment in SAP cloud applications
- Relatively simple governance requirements
- Preference for SAP-supported solutions
- Budget constraints limiting third-party options

Option 2: The Microsoft Entra ID Partnership

What It Is: Microsoft's enterprise identity platform integrated with SAP systems, representing SAP's strategic partnership announced in 2024.

The Value Proposition:

- Leverages existing Microsoft 365 investments
- Enterprise-grade security features included
- Unified identity across Microsoft and SAP
- Extensive third-party application support

Real-World Application: A financial services firm with 10,000 users implemented Microsoft Entra ID:

- **Implementation**: 18 months
- **Cost**: €1.2 million (including existing license expansion)
- **Benefits**: Single sign-on across 200 applications, 90% reduction in password resets
- **Challenges**: Complex SAP authorisation mapping required custom development

When to Choose This Path:

- Significant Microsoft ecosystem investment
- Multi-cloud strategy including Azure
- Need for broad application coverage
- Strong security requirements

Option 3: The Pathlock Governance-First Approach

What It Is: Pathlock represents a new category of solution that combines identity management with continuous compliance monitoring and application security.

The Unique Value Proposition: Where traditional IAM solutions focus on user provisioning, Pathlock addresses the complete access risk lifecycle:

Comprehensive Risk Management:

- Real-time SoD conflict detection across applications
- Continuous compliance monitoring

- Automated access reviews and certifications
- Emergency access management with full audit trails
- Cross-application activity monitoring

SAP-Specific Capabilities: Unlike generic IAM platforms, Pathlock understands SAP's complex authorisation model:

- Transaction-level access analysis
- Critical action monitoring (e.g., payment releases, master data changes)
- SAP-aware segregation of duties rules
- Integration with SAP's authorization objects
- Support for custom transactions and Z-programs

The Migration Advantage: Pathlock offers specific benefits for CUA migration:

- Pre-built migration accelerators from CUA and SAP IDM
- Ability to run parallel with CUA during transition
- Automated role redesign tools
- Built-in data quality analysis
- Phased migration support

Real-World Application: A global pharmaceutical company with 8,000 SAP users chose Pathlock:

- **Implementation**: 16 months
- **Cost**: €800,000 total investment
- **Benefits**:
    - 95% reduction in SoD violations
    - 80% faster audit preparation
    - 60% reduction in access-related incidents
    - Unified governance across SAP and non-SAP applications
- **Unique Outcomes**:
    - Discovered €2.3 million in licence optimisation opportunities
    - Prevented two potential fraud incidents through anomaly detection
    - Achieved SOX compliance with zero findings

When to Choose This Path:

- High regulatory requirements (SOX, FDA, GDPR)
- Complex SAP landscape with custom development
- Need for unified governance across applications
- Focus on risk reduction over simple provisioning
- Existing audit findings requiring remediation

The Pathlock Differentiator: What sets Pathlock apart is its ability to address both the immediate CUA replacement need and the longer-term governance requirements:

1. **Day One Value**: Unlike traditional IAM requiring complete migration before benefits, Pathlock can provide immediate risk visibility even while CUA remains operational
2. **Progressive Migration**: Organisations can migrate in waves whilst maintaining continuous compliance monitoring
3. **Built-in Intelligence**: Machine learning algorithms detect access patterns and recommend role optimisations
4. **Unified Platform**: Single solution for provisioning, governance, and monitoring reduces tool sprawl

Option 4: Enterprise Identity Governance Platforms

What They Are: Best-of-breed solutions like SailPoint, One Identity, or Saviynt offering comprehensive identity governance.

The Value Proposition:

- Industry-leading governance capabilities
- Broad application connectivity
- Advanced analytics and automation
- Flexible deployment models

Real-World Application: A manufacturing conglomerate with 15,000 users selected SailPoint:

- **Implementation**: 24 months
- **Cost**: €2.5 million total

- **Benefits**: Enterprise-wide identity governance, 70% automation of access reviews
- **Challenges**: Significant organisational change management required

When to Choose This Path:

- Complex, heterogeneous IT landscape
- Need for best-in-class governance
- Large organisation with dedicated IAM team
- Long-term strategic IAM investment

Part IV: The Decision Framework—Making the Right Choice

Assessment Criteria Matrix

Regulatory Requirements:

- **Low**: Basic access control → SAP Cloud Identity Services
- **Medium**: SOX compliance → Microsoft Entra ID + SAP GRC
- **High**: Multiple frameworks → Pathlock or Enterprise Platform
- **Critical**: Life sciences/Financial → Pathlock with continuous monitoring

Technical Complexity:

- **Simple**: Standard SAP, few systems → SAP Cloud Identity Services
- **Moderate**: Multiple SAP, some cloud → Microsoft Entra ID
- **Complex**: Customised SAP, hybrid → Pathlock
- **Extensive**: Global, multi-vendor → Enterprise Platform

Budget Constraints:

- **Minimal**: Under £200k → SAP Cloud Identity (if licensed)
- **Moderate**: £200-500k → Microsoft Entra ID extension
- **Substantial**: £500k-1.5M → Pathlock
- **Strategic**: £1.5M+ → Enterprise Platform

Timeline Pressure:

- **Urgent** (IDM users): Need solution by 2027 → Pathlock (faster implementation)
- **Moderate**: 2-3 year window → Microsoft or SAP solution
- **Flexible**: CUA-only users → Full evaluation process

The Hidden Factors Often Overlooked

Cultural Readiness:

- Conservative organisations → SAP-supported solutions
- Innovation-focused → Best-of-breed platforms
- Risk-averse → Pathlock's compliance focus
- Transformation-ready → Enterprise platforms

Existing Investments:

- Heavy Microsoft → Extend Entra ID
- SAP-dominant → SAP Cloud Identity or Pathlock
- Multi-vendor → Enterprise platform
- GRC existing → Pathlock integration

Future Direction:

- Cloud-first strategy → SAP Cloud Identity or Microsoft
- Hybrid long-term → Pathlock or Enterprise platform
- M&A activity expected → Flexible enterprise platform
- Regulatory scrutiny increasing → Pathlock's governance

Part V: Implementation Strategy—From Decision to Success

The Pathlock Implementation Advantage

To illustrate best practices, let's examine how Pathlock's methodology addresses common migration challenges:

Phase 1: Risk-Aware Assessment (Months 1-2) Unlike traditional implementations starting with technical design, Pathlock begins with risk discovery:

- Automated CUA configuration analysis
- Current state risk assessment
- Identification of SoD conflicts in existing roles
- Compliance gap analysis
- Quick wins identification for immediate value

Unique Outcome: Organisations often discover critical risks requiring immediate remediation, providing ROI before full migration.

Phase 2: Progressive Deployment (Months 3-8) Rather than "big bang" migration, Pathlock enables gradual transition:

- Deploy monitoring capabilities while CUA remains active
- Implement emergency access management first
- Add access request workflows progressively
- Migrate user provisioning in waves
- Maintain dual running for validation

Risk Mitigation: This approach eliminates the high-risk cutover period typical of traditional migrations.

Phase 3: Governance Activation (Months 9-12) Post-migration value realisation:

- Activate continuous compliance monitoring
- Implement automated access reviews
- Enable predictive analytics
- Optimise role designs based on usage
- Establish KPIs and dashboards

Sustained Value: Unlike basic IAM delivering only provisioning, governance features provide ongoing risk reduction and efficiency gains.

Common Pitfalls and How to Avoid Them

Pitfall 1: Underestimating Data Quality Issues

- **Reality**: 30-40% of CUA data typically requires cleanup
- **Solution**: Automated data quality tools (Pathlock includes these)
- **Timeline Impact**: Add 2-3 months if not addressed early

Pitfall 2: Ignoring Process Changes

- **Reality**: New tools require new processes
- **Solution**: Process redesign workshops before technical implementation
- **Timeline Impact**: 1-2 months additional if retrofitted

Pitfall 3: Insufficient Change Management

- **Reality**: User resistance can derail projects
- **Solution**: Early stakeholder engagement, pilot programs
- **Timeline Impact**: 3-6 months delay if not managed

Pitfall 4: Scope Creep

- **Reality**: "While we're at it" additions double project size
- **Solution**: Phased approach with clear scope boundaries
- **Timeline Impact**: 6-12 months if unchecked

Part VI: The Business Case—Beyond Technology

Quantifying the Risk Reduction

The Compliance Dividend: Organisations using modern governance platforms like Pathlock report:

- 90% reduction in audit findings
- 75% decrease in remediation costs
- 50% faster audit completion
- Zero critical findings in subsequent audits

Financial Impact: For a company spending £500,000 annually on audit and remediation, this represents £375,000 in savings.

The Security Premium: Advanced platforms deliver measurable security improvements:

- 70-80% reduction in identity-related incidents
- 90% decrease in orphaned accounts
- 95% improvement in SoD violation detection
- 60% faster threat response time

Risk Mitigation Value: With average breach costs at £4.88 million and 82% involving credentials, even 50% risk reduction represents £2 million in avoided costs.

The Efficiency Multiplier: Automation delivers compound benefits:

- 80% reduction in manual provisioning effort
- 60% decrease in access review time
- 50% fewer helpdesk tickets
- 90% faster emergency access processing

Productivity Gains: A 5,000-user organisation saves approximately 15,000 hours annually, worth £600,000 in labour costs.

The Strategic Value Often Unmeasured

Agility Enhancement:

- Cloud migrations accelerate by 6-12 months
- New application onboarding reduces from weeks to days
- M&A integrations complete 50% faster
- Digital initiatives unblocked

Competitive Advantage:

- Customer portals enabled with SSO
- Partner ecosystems integrated seamlessly
- Employee experience matching consumer standards
- Security posture as market differentiator

Innovation Enablement:

- API economy participation

- Zero-trust architecture foundation
- Automation and AI initiatives supported
- DevOps practices enabled

Part VII: The Path Forward—Your Action Plan

For Organisations Using CUA Only

Immediate Actions (Next 30 Days):

1. Conduct CUA dependency assessment
2. Document current state architecture
3. Identify critical risk exposures
4. Establish project governance structure
5. Begin vendor evaluation process

Short-term Strategy (3-6 Months):

1. Complete comprehensive requirements gathering
2. Evaluate 2-3 solution options in detail
3. Conduct proof of concept with preferred vendor
4. Develop business case and secure funding
5. Select implementation partner

Implementation Timeline (6-24 Months):

- Months 6-9: Design and preparation
- Months 10-15: Phased migration
- Months 16-18: Optimisation
- Months 19-24: Value realisation

For Organisations Using SAP IDM

Critical Actions (Immediate):

1. **Stop any new IDM implementations**
2. Assess current IDM utilisation and dependencies
3. Begin migration planning immediately
4. Evaluate fast-track options like Pathlock
5. Secure budget for 2024-2025 implementation

Accelerated Timeline (Must Complete by 2027):

- Q1 2024: Solution selection
- Q2-Q3 2024: Design and build
- Q4 2024-Q2 2025: Migration execution
- Q3 2025: Validation and optimisation
- Q4 2025: IDM decommissioning
- 2026: Buffer for issues
- 2027: Must be complete

For All Organisations: The Evaluation Framework

Step 1: Define Success Criteria

- Security requirements
- Compliance mandates
- User experience goals
- Integration needs
- Budget constraints

Step 2: Assess Solution Fit

- Request detailed demonstrations
- Speak with reference customers
- Evaluate vendor stability
- Assess implementation partner ecosystem
- Validate total cost of ownership

Step 3: Conduct Proof of Value

- Pilot with representative user group
- Test critical integrations
- Validate security controls
- Measure performance impact
- Confirm user acceptance

Step 4: Make Risk-Adjusted Decision

- Consider implementation risk
- Evaluate vendor lock-in
- Assess skills availability
- Plan contingency options
- Document decision rationale

Conclusion: The Imperative for Action

The challenge facing SAP customers isn't whether to move beyond CUA—it's how quickly and effectively they can execute this critical transformation. The convergence of security threats, compliance requirements, and digital transformation demands makes maintaining CUA an increasingly untenable position.

The good news is that modern solutions don't just replace CUA—they transform identity management into a strategic capability. Whether choosing SAP's cloud services for simplicity, Microsoft's platform for breadth, Pathlock for governance excellence, or enterprise platforms for ultimate flexibility, organisations can achieve:

- **Dramatic risk reduction** through continuous monitoring and intelligent analytics
- **Significant cost savings** via automation and efficiency
- **Enhanced agility** enabling digital transformation
- **Competitive advantage** through superior security and user experience

The organisations that act decisively now—particularly those facing the 2027 SAP IDM deadline—will emerge with modern, resilient identity platforms. Those that delay face escalating risks, rushed implementations, and premium costs as the market becomes constrained.

The question isn't whether to migrate from CUA, but which path offers the best combination of risk mitigation, business value, and strategic alignment for your organisation. With careful planning, appropriate solution selection, and committed execution, the transition from CUA becomes not a burden but an opportunity to fundamentally strengthen your organisation's security posture and operational efficiency.

The time for action is now. The path forward is clear. The only remaining question is: Which route will you take to modern identity management excellence?

Bibliography

SAP Official Documentation

SAP Community. (2023). "End of maintenance/support for CUA?" Q&A Thread. Available at: https://community.sap.com/t5/technology-q-a/end-of-maintenance-support-for-cua/qaq-p/12695154

SAP Community. (2023). "CUA will never die." Technology Blog Post. Available at: https://community.sap.com/t5/technology-blogs-by-sap/cua-will-never-die/ba-p/12871652

SAP Community. (2024). "Preparing for SAP Identity Management's End-of-Maintenance in 2027." Blog Post. Available at: https://community.sap.com/t5/technology-blog-posts-by-sap/preparing-for-sap-identity-management-s-end-of-maintenance-in-2027/ba-p/13596101

SAP Help Portal. (2021). "S/4HANA 2021 Simplification List." Document SIMPL_OP2021. Available at: https://help.sap.com/doc/f2591a6901344c97a5e2029cc8f3703e/2021/en-US/SIMPL_OP2021.pdf

SAP Help Portal. (2024). "SAP Cloud Identity Services Documentation." Available at: https://help.sap.com/docs/identity-authentication

SAP Learning. (2024). "Identity Authentication Service Overview." Learning Journey. Available at: https://learning.sap.com/learning-journeys/exploring-the-fundamentals-of-sap-system-security/describing-the-identity-authentication-service

Industry Analysis and Third-Party Sources

Basis Technologies. (2024). "The True State of S/4HANA: Migration Timelines and Support." Available at: https://www.basistechnologies.com/blog/the-true-state-of-s4hana

Deloitte. (2024). "Cyber Identity Services." Consulting Services Overview. Available at: https://www.deloitte.com/us/en/services/consulting/services/cyber-identity.html

Deloitte Insights. (2024). "Consumer and Enterprise Digital Identity Management Strategies." Research Report. Available at: https://www2.deloitte.com/us/en/insights/industry/technology/consumer-enterprise-digital-identity-management-strategies.html

IBsolution. (2024). "End of Maintenance 2027 for SAP IdM: What Companies Need to Do Now." Blog Post. Available at: https://www.ibsolution.com/academy/blog_en/cyber-security/identity-and-access-management/end-of-maintenance-2027-for-sap-idm-what-companies-need-to-do-now

KuppingerCole. (2023). "SAP Focuses on SAML and SAP NW IdM Instead of CUA." Analyst View. Available at: https://www.kuppingercole.com/blog/kuppinger/sap-focuses-on-saml-and-sap-nw-idm-instead-of-cua

Microsoft Learn. (2024). "Configure SAP Cloud Identity Services for Single Sign-On with Microsoft Entra ID." Technical Documentation. Available at: https://learn.microsoft.com/en-us/entra/identity/saas-apps/sap-hana-cloud-platform-identity-authentication-tutorial

Microsoft Learn. (2024). "Migrate Identity Management Scenarios from SAP IDM to Microsoft Entra." Migration Guide. Available at: https://learn.microsoft.com/en-us/entra/id-governance/scenarios/migrate-from-sap-idm

My1Login. (2024). "Building the Business Case and ROI for Identity and Access Management." White Paper. Available at: https://www.my1login.com/resources/white-papers/building-the-business-case-and-roi-for-identity-and-access-management

Omada Identity. (2024). "SAP Identity Management Migration Solutions." Product Overview. Available at: https://omadaidentity.com/solutions/sap-identity-management-migration/

One Identity. (2024). "How One Identity Can Support SAP Environments and Migration." Blog Post. Available at: https://www.oneidentity.com/community/blogs/b/identity-governance-administration/posts/how-one-identity-can-support-sap-environments

SafePaaS. (2024). "How to Navigate SAP Identity Management Sunset." Industry Guide. Available at: https://www.safepaas.com/articles/how-to-navigate-sap-identity-management-sunset/

SAPtechnicalGuru. (2023). "Central User Administration (CUA) - Complete Guide." Technical Blog. Available at: https://www.saptechnicalguru.com/cua/

Saviynt. (2024). "From SAP to Saviynt: A Smart Move for Modern Identity Governance." Solution Brief. Available at: https://saviynt.com/blog/from-sap-to-saviynt-a-smart-move-for-modern-identity-governance

Support Revolution. (2024). "SAP Support Deadline Extended Yet Again to 2027 [2024 Updated]." Industry News. Available at: https://www.supportrevolution.com/blog/sap-deadline-extended-again-2027/

Xiting. (2024). "2024 SAP Cloud Identity Services & IAM Portfolio: What's New?" Analysis Report. Available at: https://xiting.com/en/cloud-identity-services-and-iam-portfolio/

Technical References and SAP Notes

SAP Note 320449 - "Temporary Deactivation of Central User Administration"

SAP Note 3003462 - "Global User ID Support in Central User Administration"

SAP Discovery Center. (2024). "Identity Provisioning Service Catalog." Available at: https://discovery-center.cloud.sap/serviceCatalog/identity-provisioning

Flexera. (2023). "EDEKA Digital Saves Millions Through SAP License Optimisation." Case Study. Available at: https://www.flexera.com/resources/case-studies/edeka

MPrusov Technical Archive. "Simplifying User Administration in Heterogeneous Landscapes." SAP TechEd 2003 Presentation. Available at: https://mprusov.narod.ru/sap/teched03/

Scribd. (2016). "Introduction to Central User Administration (CUA) - SAP All About Web and Cloud." Technical Document. Document ID: 311638828. Available at: https://www.scribd.com/document/311638828/

This guide represents the current state of SAP identity management as of August 2025. Given the rapidly evolving nature of cloud services and security requirements, readers should verify current vendor offerings and support timelines with official SAP and partner documentation.