KuppingerCole Report

EXECUTIVE VIEW

by Martin Kuppinger | November 2019

Atos DirX Access

Atos DirX Access is a mature solution for Access Management, covering the full range of targets from legacy web applications to modern SaaS services. It comes with comprehensive support for modern standards, including FIDO 2.0. A specific strength is the support for specific capabilities such as session state sharing across servers, Dynamic Authorization Management, or integrated User Behavior Analytics. Atos DirX Access counts amongst the most feature-rich solutions on the market.

by **Martin Kuppinger**
mk@kuppingercole.com
October 2019

Content

Related Research

Leadership Compass: Access Management and Federation – 71147
Executive View: Evidian Identity & Access Management – 70872
Leadership Compass: Access Governance & Intelligence – 71145
Leadership Compass: Identity Governance & Administration - 71135

1 Introduction

Identity and Access Management (IAM) is a foundational element of cybersecurity today. In the early days of computing, identity was established with user accounts, and access was managed by group membership. In the decades since, the concepts, principles, and technologies of IAM have evolved and become increasingly specialized. User accounts and group memberships are still important constructs, but the tools for authenticating, authorizing, auditing, and protecting identities have proliferated.

As a set of technologies, IAM encompasses user and entitlement provisioning, identity repositories, authentication mechanisms, authorization systems, web access management (WAM), federation and Single Sign-On (SSO), identity governance, access reconciliation, risk management, and many interfaces to other security systems.

Many of the components of IAM have become standardized and even commoditized. To interoperate with other solutions and be successful in the marketplace, IAM products generally support the following standards:

- Provisioning: SCIM
- User identity storage: LDAP, sometimes NoSQL databases for CIAM implementations.
- Authentication: Kerberos, RADIUS, PKI/x.509 including SmartCards, FIDO U2F/UAF/2.0, and more
- Federation: OAuth, OpenID, OpenID Connect (OIDC), and SAML
- Authorization: JSON, JWT, UMA, and XACML

Commonly, IAM is split into three major parts:

- Identity Management: The management of identity lifecycles and their governance. This is commonly referred to as Identity Provisioning (Lifecycle Management) and Access Governance, or as IGA (Identity Governance and Administration),
- Access Management: Enabling access of users, i.e. supporting authentication, identity federation, and authorization.
- Privileged Access Management (PAM): These technologies focus on highly privileged users and the specific requirememts around these users, plus shared accounts. Capabilities include management of passwords for shared accounts and of privileged user sessions.

Access Management, also referred to as Web Access Management & Identity Federation, as one of the major disciplines is focused on providing access for users to services. They can deliver a SSO (Single Sign-On) experience to users, by authenticating the users on behalf of the target applications.

Integration can work either via standards for identity federatin or – for legacy web applications that do not support modern identity federation standards – with methods such as password injection and providing authentication information as part of modified https headers. Authentication should integrate with the authentication standards listed above.

Access Management should support a range of applications from modern SaaS services to legacy web applications. While deployment models are shifting towards cloud-based delivery of Access Management, there is still a need and place for on premises solutions, specifically for B2E and B2B use cases, or B2C use cases that work against backend systems within the enterprise.

A specific requirement for all types of Access Management is scalability and high availability. Access of users to services depends on the availability of these services, and specifically in B2C scenarios, massive workloads and peaks can arise.

Atos is one of the vendors of Access Management solutions, with their DirX Access offering. DirX Access is a proven, mature solution that has been consequently enhanced by new features, supporting all major use cases. While being an on premises solution, Atos as one of the leading IT service providers also can provide MSP-style deployments.

2 Product Description

DirX Access is a feature-rich solution for Access Management, supporting Adaptive Authentication including risk- and context-aware authentication, Web Access Management, and Identity Federation, with broad support for standards. Additional capabilities include UBA (User Behavior Analytics) in the context of Adaptive Authentication, and support for Dynamic Authorization Management for applications, based on XACML standard support. As mentioned, it operates as an on premises solution, but with flexible deployment options provided by Atos.

In authentication, DirX Access comes with broad support for authentication factors and standards. Factors range from username/password and X.509 to various types of OTP (One Time Password), an own authenticator app, W3C support e.g. for Microsoft Windows Hello. The list of supported standards is comprehensive as well, also including the most modern standards such as W3C WebAuthn, and FIDO2. Authentication methods can be combined flexibly, based on policies and risks.

For risk- and context-based authentication, DirX Access supports a range of factors, including geolocation, IP address ranges, and user context from earlier sessions. Other factors can be added by call-outs to 3rd party solutions that deliver additional information. This example might include providers of whitelist/blacklist services for authentication.

A security session is created for each user. DirX Access can provide session context to applications and, based on the sessions, handles SSO to multiple parallel sessions based on what the defined access policies allow. Other supported features include e.g. session correlation between browsers if a user uses more than one browser. Overall, DirX Access comes with a high degree of flexibility.

Additionally, DirX Access tracks every user session if configured. This includes login failures, client addresses used, locations, and other information. Based on that information, DirX Access can identify anomalies in user behavior. Based on the policies, DirX Access than e.g. can request additional authentication factors or revoke access to a session. Session state sharing across multiple DirX Access servers is supported as well.

In Identity Federation, all relevant standards are supported, i.e. SAML v2.0, OAuth 2.0, and OpenID Connect. DirX Access supports a broad range of specific profiles for these standards, but also specific use cases such as SAML proxying for authentication flows across multiple IdPs. A specific capability is Dynamic Provisioning of users to target systems in combination with federation protocols. Thus, user accounts can be created and removed on the fly, for single session or during the first access of a user.

Both push models (initiated by DirX Access) and pull models (initiated by the Service Provider) are supported. For several of the most commonly used SaaS services such as Microsoft Office 365, SAML is already preconfigured. However, DirX Access does not provide an exhaustive list of preconfigured targets as some of the IDaaS Access Management solutions do. Notably, DirX Access also delivers STS (Secure Token Transformation) capabilities, e.g. inter-protocol proxying.

Aside from Identity Federation, DirX Access comes with mature and feature-rich support for traditional Web Access Management requirements. Given that many applications, both legacy applications and cloud services, still lack support for standards-based Identity Federation, such capabilities are essential in support the full range of target applications in hybrid IT environments. DirX Access again comes with various integration options, including PEPs (Policy Enforcement Points) that run close to application servers, web servers, and web applications. This allows for flexible deployments, where e.g. certain elements are placed in different network zones.

Furthermore, these capabilities allow for a vast range of different integration types, ranging from basic web SSO to very tight integration with applications based on web services. Additionally, DirX Access comes with XACML support and thus for Dynamic Authorization Management. Applications can query DirX Access, which returns decisions based on the configured access policies. That type of in-depth integration support is rarely found in Access Management solutions.

The internal security model of DirX Access is very granular and based on roles. It allows for a fine-grain assignment of permissions to users for various tasks. This also allows for implementing delegated administration in more complex environments. Additionally, multiple tenants can be set up to allow for a clear segregation between use cases such as B2C and B2E, and supporting specific regulatory requirements.

Additional capabilities include auditing and reporting as well as performance monitoring capabilities. The product also comes with advanced support for high availability and failover. Factually, DirX Access counts amongst the most feature-rich solutions in the market.

Even while the architecture and deployment follow a traditional approach of Access Management, this solution sufficiently covers the common use cases of organizations, specifically when also including MSP options provided by Atos. Unfortunately, the UI also follows a traditional approach and clearly would benefit from modernization. Graphical configuration of authentication flows and other modern capabilities are lacking. Some customizations and call-outs also require coding.

3 Strengths and Challenges

DirX Access is a mature and proven Access Management solution. From a feature perspective, all common features are covered. Some of the features are rarely found in that combination, such as support for Dynamic Authorization Management and the integrated User Behavior Analytics capabilities.

The product is also cutting-edge when it comes to standards support, covering all relevant standards of today, with comprehensive support for specific profiles of such standards and additional capabilities such as SAML proxying.

Integration capabilities of DirX Access are very flexible. However, the approach for call-outs to third-party applications commonly requires coding. Generally speaking, the flexibility of the offering is very high, as well as its maturity regarding specific requirements.

On the downside, full IDaaS deployment support is lacking. However, Atos should be flexible enough for providing a range of options for customers, based on their capabilities as MSP. The biggest challenge, from our perspective, is the outdated UI. While this is good enough for efficiently managing DirX Access, it fails to meet the expectation of today's users.

In summary, DirX Access is an Access Management solution that is very worth closer examination, specifically in complex environments. Due to its maturity and the comprehensive support for modern standards, DirX Access is able to cover very complex requirements as well as standard environments where access to SaaS services such as Microsoft Office 365 is the basic requirement.

Strengths	Challenges
• Very mature Access Management solution, delivering many specific capabilities for complex environments • Comprehensive support for modern standards, including full support for current federation standards and for FIDO2 • Supports a variety of configurations, including high availability, multi-tenancy, and failover • Flexible customization and integration of third-party solutions, however commonly requiring coding • Supports a broad range of authentication mechanisms • Proven scalability • Integrates specific capabilities for User Behavior Analytics and Dynamic Authorization Management • Good support for risk- and context-based authentication	• No full IDaaS solution, but on premises solution can be provided in MSP-style deployment models including multi-tenant support • Low visibility in the market, despite strong technical capabilities • Administrative UI would benefit from UI modernization

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com