

OpenText Core Identity Foundation

The first step to gaining control of your entitlements is recognizing that identities span across your whole environment



Benefits

- **Enhanced productivity:** 81% of organizations surveyed report that they manually review all or most of their access requests.¹
- **Compliance with privacy mandates:** Cost of compliance, \$5.47 million; cost of non-compliance, \$14.82 million.²
- **Faster ROI:** 83% say that difficulty integrating with IGA systems is the primary cause of manual IGA processes.³
- **Block attacks:** Multi-factor authentication for sensitive data and services can block more than 99% of compromise attacks.⁴

To protect your high-value assets across your entire environment, you need to manage identity and access control beyond Microsoft® Active Directory and Microsoft Entra® ID, including all your distributed identity stores and even your edge ones. Using an event model, OpenText fully integrates with all identity stores across your entire environment. This approach alleviates the need for manual true-ups that plague adopters of competing solutions.

Enhanced productivity

OpenText™ Core Identity Foundation allows organizations to boost their productivity by streamlining user access to secured services. It allows IT and security teams to deliver single sign-on while centralizing user identity management, eliminating the need for multiple logins and passwords and saving valuable employee time. Automating account provisioning and lifecycle management ensures timely access to necessary resources, reducing IT support overhead. Additionally, the service's robust security features, such as multi-factor authentication and access controls, safeguard sensitive data and prevent unauthorized access, minimizing downtime and potential data breaches.

¹ Netwrix, *Netwrix Survey: 75% of Organizations Strengthen Their Cybersecurity Posture by Conducting Regular Access Reviews*, 2022

² IBM, *Cost of a Data Breach Report 2024*

³ Zilla Security, *2025 State of IGA Survey*

⁴ Microsoft, *One simple action you can take to prevent 99.9 percent of attacks on your accounts*, 2019

Compliance with privacy mandates

While business owners understand the value of centralizing identity management across their organization, applications and services distributed throughout their organization make this difficult. Not all applications use Microsoft Active Directory as their exclusive identity store, especially legacy ones, where it's far more common for each one to retain their own local accounts. When competing offerings focus their solution on Active Directory, the organization's array of distributed identity stores makes it difficult to account for them to confidently attest compliance to government mandates. OpenText Core Identity Foundation provides an event-driven identity connector technology that can apply security and mandate policies to every change made, extending the central point of control to all important edge identity stores.

Centrally automating identity management also allows organizations to strengthen customer trust, maintain their reputation, and mitigate financial risks. Allowing the pursuit of new business opportunities enables organizations to meet their commitment to data security and privacy, while enhancing their competitive edge. It also streamlines audits and reduces the burden of compliance efforts, freeing up resources for strategic initiatives.

Lower TCO

Automating management of all your identity stores lowers your identity management costs. The event-based identity engine keeps your managed environment compliant with your security and access policies by proactively applying defined policies for all identity changes. This approach distinguishes OpenText Core Identity Foundation from any other service. The bidirectional identity engine enforces entitlement policies for your managed corporate services—those that affect your organizational risk, including those that are a part of your compliance commitment.

This comprehensive approach alleviates the need for manual or custom identity true-ups, which plague organizations as they come at a significant cost and time investment. OpenText Core Identity Foundation's distinct licensing model also lowers your total cost of ownership (TCO). Rather than a fee for each feature or service you implement, the services licensing model provides access to all services, requiring licensing only for the identities accessing its services. The light and heavy usage model licensing allows you to budget OpenText services to problem areas, even if you have an identity infrastructure in place.

While the OpenText Core Identity Foundation is a set of cloud-based microservices, its cloud bridge provides all of the security and integration of on-premises, without the dedicated headcount and hardware that are typical for a traditional identity and access management infrastructure.

Block attacks

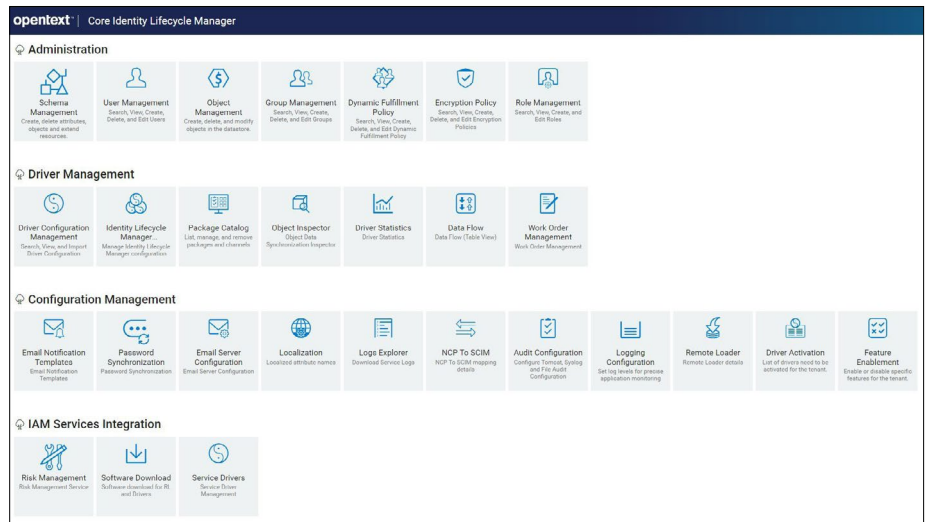
CTOs and architects have long understood the benefits of open standards. Standards are foundational to achieving interoperability between independent applications and platforms, as well as maintaining long-term architecture integrity. This is why when an organization implements an authentication solution built on proprietary protocols, it no longer has the freedom to implement devices that best fit its needs at the best price.

Among the standards that OpenText Core Identity Foundation supports, an important one for authentication is FIDO (Fast Identity Online) Alliance. FIDO U2F (Universal 2nd Factor) enables organizations to support an environment where users manage their authentication devices. FIDO2 combines the W3C's Web Authentication (WebAuthn) specification and the FIDO Client to Authenticator Protocol (CTAP) to enable passwordless authentications across websites and apps using public-key cryptography.

The OpenText Core Identity Foundation solution

From its integration of essential IAM services to its licensing model, OpenText Core Identity Foundation is designed to either be your infrastructure or a solution to an existing gap. The SaaS offering can be applied to automate your edge identity stores or consolidate your multi-factor authentication silos. Dual usage licensing options make it cost-competitive to replace custom processes that are either expensive or brittle.

Additionally, existing OpenText Identity Manager Advanced customers will benefit from the new set of integrated services, which offer a superior option for reducing your operational costs while enhancing your central point of administration and control. It helps remove much of the legwork too often needed to successfully attest to compliance mandates and makes it easier to achieve your zero trust security goals.



Identity Lifecycle Manager is part of an integrated set of services.