

Education Pricing & Package Offering.

Okta Education Cloud Overview

Higher, Further and Schools are eligible to use Okta for Education products. These products utilise the aMAU unit of measure but have some additional Workforce product features. This gives Education customers the flexibility to manage their seasonality and differing user types.

Okta traditionally offers products in either the IT/Workforce – WIC or the API/CIAM – OCI Solutions . Given the complex nature of a campus ecosystem – where traditional “workforce” users, such as staff/faculty, and traditional “customer” users, such as students, are blended (e.g. a student can be a work study student, and therefore also employed by the institution; a graduate student is both a student and a professor; etc.)

Education customers have been given a unique set of SKUs that better address the needs and pricing model for education institutions. The Education SKUs also address this fluctuation of active users when considering admission applicants, alumni, donors, and others.

Pricing

At Okta, we understand that a 'Big Bang' implementation isn't always feasible. We recognise that much of the first year will focus on configuring and integrating the Identity Platform into the university's ecosystem. With Okta, license metering only beginning when users actively utilise the provisioned services.

SaaS Licencing illustration:

Pricing based on a 3 Year Agreement – £60k for 5k Users per Annum £250k for 25K users per Annum

Pricing based on Institutions who have taken the full Okta for Education Identity Solution– Okta as the IDP, JML, Governance & PAM

We look at the User People Groups- possible approach

Year .1. Assumed Staff and Students will be the initial groups set up, assumed Identities will be loaded into the system at around month 5/6 - This is represented by the 50% usage in model.

Year .2. Staff, Students and Associates to be fully ramped,

Year .3. Staff, Students and Associated to be fully ramped.

We consider the Technology Adoption - model phased approach

This allows the University to use Okta SSO and aMFA in conjunction Enterprise, LifeCycle Management, Workflows and moving to full Okta Identity Governance (OIG) In Year 2.

Year .1. UD set up, LCM and workflow automations with all Key Uni Apps + SSO and MFA

Year .2. Continue - LCM and workflow automations continue with onboarding of Apps and Start OIG program of works

Year .3. Fully onboarded through this year- Start PAM project.

Implementation - Not included in Pricing

Designed in conjunction with each individual institution - dependant on Organisations People/Skills, Organisations Timeline / Projects/ Needs and requirements based on visible ROI targets.



OKTA CUSTOMER IDENTITY

Enterprise

Build secure, seamless identity experiences for your customers

Key Benefits



Create frictionless experiences to meet modern customer expectations



Bring your apps to market quicker without compromising on security



Focus on your core business while saving precious development time

Key Features

- Enterprise-grade Authentication
- Flexible and highly scalable User Management
- API Access Management (1 Authorization server)
- Unlimited OIDC and SAML applications
- Customizable user experience
- Centralized administration and monitoring
- Basic MFA: Okta Verify OTP, Google Auth
- Developer tooling: APIs, SDKs, Widget
- FastPass (Available with OIE)



OKTA CUSTOMER IDENTITY

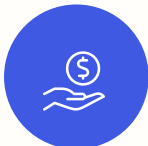
Single Sign-On Integrations

Connect to the apps of your choice

Key Benefits



Avoid vendor lock-in; choose from 6,500+ pre-built integrations with cloud and on-premises systems



Reduce operational costs while increasing customer engagement with portals.



Deploy easily with our integration wizard, while continuous monitoring and updates ensure high availability

Key Features

- Access to pre-built app integrations in the OIN
- Outbound federation (SAML, OIDC) to OIN applications
- Custom SAML assertion attributes to OIN applications

Product Requirement: Requires Enterprise

Multi-Factor Authentication

Strong Customer Authentication for every use case

Key Benefits



Use Okta's broad set of factor options to support every security use case



Enforce strong authentication using MFA at any point in the user journey



Drive developer efficiency and admin control with Okta MFA dashboards

Key Features

- Support for factors including knowledge based, possession and biometric factors (FIDO2.0)
- Fine grained MFA policy control that drives enrollment, authentication and recovery
- Integration with 3rd party factors e.g Yubikey etc.
- Support for custom MFA flows using standards
- Support for per-user multiple factors
- Stateful and stateless MFA API

Product Requirement: Requires Enterprise

OKTA CUSTOMER IDENTITY

Adaptive Multi-Factor Authentication

Contextual access management for all your critical resources

Key Benefits



Comprehensive risk analysis based on a broad range of signals



Broad set of customer authentication options for every security use-case



Threat intelligence powered by Okta's customer network

Key Features

- Risk policies engine powered by both AI/ML and heuristics
- Rich set of risk signals built around device, location, IP, Travel, Proxies etc.
- Passwordless authentication
- Wide range of out- of-box and BYO factors, including biometrics to meet every use-case
- Easy integration with APIs, Pre-built SDKs etc.
- Integration with third party security products

Product Requirement: Requires Enterprise

Device Access

Enable secure access starting from device login

Key Benefits



Secure the first vulnerable touchpoint – the device login



Integrate identity from devices to apps to simplify access



Support simplified, secure device onboarding and account mgmt

Key Features

- MFA challenge to login to a managed Windows or macOS device
 - Support for both online and offline login scenarios with a variety of factors
 - Flexible policy configurations, including the option to enable a passwordless login experience for Windows
- Device logout flow to manage risky or inactive users
- Okta password synchronization for macOS
 - Easy enrollment flow that sets up FastPass for passwordless login to apps
- Streamlined device onboarding and local account creation
- Intuitive, native OS user experience

Product Requirement: Requires SSO or MFA/AMFA





OKTA CUSTOMER IDENTITY

Lifecycle Management

Automate user journeys

Key Benefits



Free up developers by avoiding custom integration code, and launch projects faster



Automate manual tasks like provisioning and deprovisioning with more than 120 pre-built integrations



Maintain a source of truth by syncing user information between Okta and 3rd-party apps, or combine data in Okta's Universal Directory

Key Features

- Automatically provision and deprovision users to 3rd-party or custom apps.
- Assign apps based on group membership or user attribute.
- Integrate with your CRM or marketing stack by scheduling recurring imports from CSVs.
- Easily migrate customer profile data from existing user stores and enjoy fine-grained control over how profiles are mastered.
- Provision and deprovision Okta users and groups into AD / LDAP.
- Org2Org provisioning

Product Requirement: Requires Enterprise

Okta Identity Governance

Manage digital identities and access rights for all your users

Key Benefits



Converged IAM and Governance solution that provides an unparalleled comprehensive view of every user's access patterns and automates processes to meet compliance requirements.



Improve enterprises' security posture by providing visibility and control to who has access to which digital resources within their organization.



Intelligent, easy to use and efficient Identity Governance solutions that lets you orchestrate access governance to reduce management workload by automating tasks and providing process workflows.

Key Features

OCI OIG Light	OCI OIG Unlimited
50 workflows (org level)*	Unlimited workflows (org level)*
LCM for 5 apps **	LCM for unlimited apps**
Self service access requests	
Access Certification for users and apps	
Out of the box reporting	
Advanced Directory Management (ADM) included, with:	
Realms and realm assignments	
Dedicated partner admin controls	
Partner admin portal	

Product Requirement: Must match Enterprise quantity



Workflows

No code/ low code platform to automate complex identity processes, at scale

Key Benefits



Enable anyone to automate identity-based processes and drive seamless user experiences



Mitigate risks from manual/custom scripts



Accelerate time to market with operational sustainability

Key Features

- **Pre-built Connectors:** Use out-of-the-box app connectors such as Google Workspace, Office365, OneTrust, Marketo, and Jamf
- **Connect to Any API:** Call any REST API endpoint not found in our connector catalog
- **Trigger Events Instantly or on a Schedule:** Eliminate scripts by setting triggers
- **Perform Data Manipulation:** Format and clean data as it passes between apps. Compose messages by dragging and dropping fields
- **Out-of-the-Box Templates:** Leverage pre-built flows from automating on/off-boarding, securing apps, and more

Product Requirement: Must match Enterprise quantity



Directory Integration

Simplify Partner integrations for B2B applications

Key Benefits



Reduce administrative overhead of managing multiple user stores. While accelerating partner onboarding.



Integrate with an unlimited number of directories across your customers.



Developer friendly API's, SDK's and custom branding.

Key Features

- Supports Active Directory and LDAP
- Import and Update user profiles
- Delegated Authentication and Administration
- Provision users back to local directory
- High availability agent based architecture
- Just In Time User creation
- Centralized Administration of users
- Secure access
- Self Service out of the box

Product Requirement: Requires Enterprise

Inbound Federation

Add the ability for your app to accept authentication from an external SAML or OIDC identity provider (IDP).

Key Benefits



Developer friendly API's, SDK's and custom branding.



Integrate Okta with external SAML Identity Providers.



Implement real-time user creation (Just in Time provisioning) during federation.

Key Features

- Supports standards based federation (SAML, OIDC)
- Import and Update user profiles
- High availability agent based architecture
- Just In Time User creation
- Centralized Administration of users
- Secure access
- Self Service out of the box

Product Requirement: Requires Enterprise

API Access Management

Extend your security policies to your APIs

Key Benefits



Integrate with your existing API Gateway in minutes instead of days



Use OAuth 2.0 to standardize on tools, SDKs, training, and best practices to move faster and securely



Centralize your authorization policy to ensure security and compliance, while allowing developers to choose their tools

Key Features

- Standard OAuth 2.0 with Extensions
- Compatible with most tools, SDKs, and programming frameworks out of the box
- Reduces need to become OAuth 2.0 experts
- Create, maintain, and audit policies centrally regardless of the tools and technologies used
- Customize authorization policy by team, product, use case, partner, customer, or employee
- Can leverage LCM to provision/deprovision API access automatically

Product Requirement: Requires Enterprise

Okta Access Gateway

Embed modern authentication into web apps, without changing code

Key Benefits



Embed modern SSO, Adaptive MFA, and Cloud security into traditional web apps



Integrate customer apps fast without changing code to support OAuth



Reduce costs and operational burden from legacy SSO solutions

Key Features

- Secure access to traditional web apps with Okta SSO and MFA
- Secure custom web apps, pages, and web portals using traditional integration standards: Header-based, Kerberos, IWA, and Certificate-based authentication
- Implement granular authorization policies
- Support complex deployments with native support for multiple tenants and data centers
- Support On-Premise, IaaS, and Multi-Cloud environments

Product Requirement: Requires Enterprise

Requires 1 seat of Training – Implement Okta Access Gateway; Professional Services recommended



Okta Privileged Access

Privileged Access solution for cloud and hybrid infrastructure

Key Benefits



Reduced attack surface and enhanced security with just-in-time access



Streamlined compliance and auditing to meet regulatory requirements



Unified access and operational efficiency with a single control plane

Key Features

- Zero standing privileges for servers
- Store and rotate passwords for local server accounts, Okta accounts, SaaS service account, and Active Directory accounts
- Secure storage for passwords, API keys, tokens
- Integrated requests and approvals
- Time-based access controls

Product Requirement: Requires Enterprise Licence





Okta Privileged Access

Privileged Access solution for cloud and hybrid infrastructure

- Customers purchase a pool of **Resources Units** which they can use towards **any Resource type**. Resource Unit model to future proof and **provide customers with greater flexibility**
- Resources units are consumed according to a Resource Unit Conversion Factor that is set per Resource Type
- Customers are entitled to use purchased Resource Units towards future Resources types as they launch according to the Conversion Factor published in the [Product Subscription Reference Guide](#)
- Pricing model ensures the true value of the protected resource is captured as not all Resource types are valued equally while also offering customers flexibility to consume Resource Units with any Resource type mixture
- Okta will monitor Resource Unit consumption for compliance purposes but is not limited in product

		Resource Type	Resource Unit Conversion Factor
Privileged Accounts		1 User*	0.5 Resource Units
		1 Workload Identity	0.25 Resource Units
Protected Endpoints		1 Server	1 Resource Unit
		1 SaaS Applications**	35 Resource Units
		1 Active Directory Account	0.25 Resource Units

Product Requirement: Requires Enterprise Licence



DynamicScale

Ensure a seamless, reliable end-user experience for peak performance at any scale

Key Benefits



Seamless end-user experience even during surges in traffic



Okta's industry-leading reliability and scalability for optimal performance



Availability to increase rate limits from 5x to 1000x the default limits

Key Features

- Support for up to 500,000 authentications per minute
- Annual protection for seasonal or sustained high-capacity traffic in Production environments
- Temporary availability for testing purposes in a sandbox tenant
- Adjust rate limits to allow for seamless adaptation to changing requirements

Product Requirement: Requires Enterprise



OKTA WORKFORCE IDENTITY

Identity Security Posture Management



Deep Human and Non Human Identity focused posture analysis



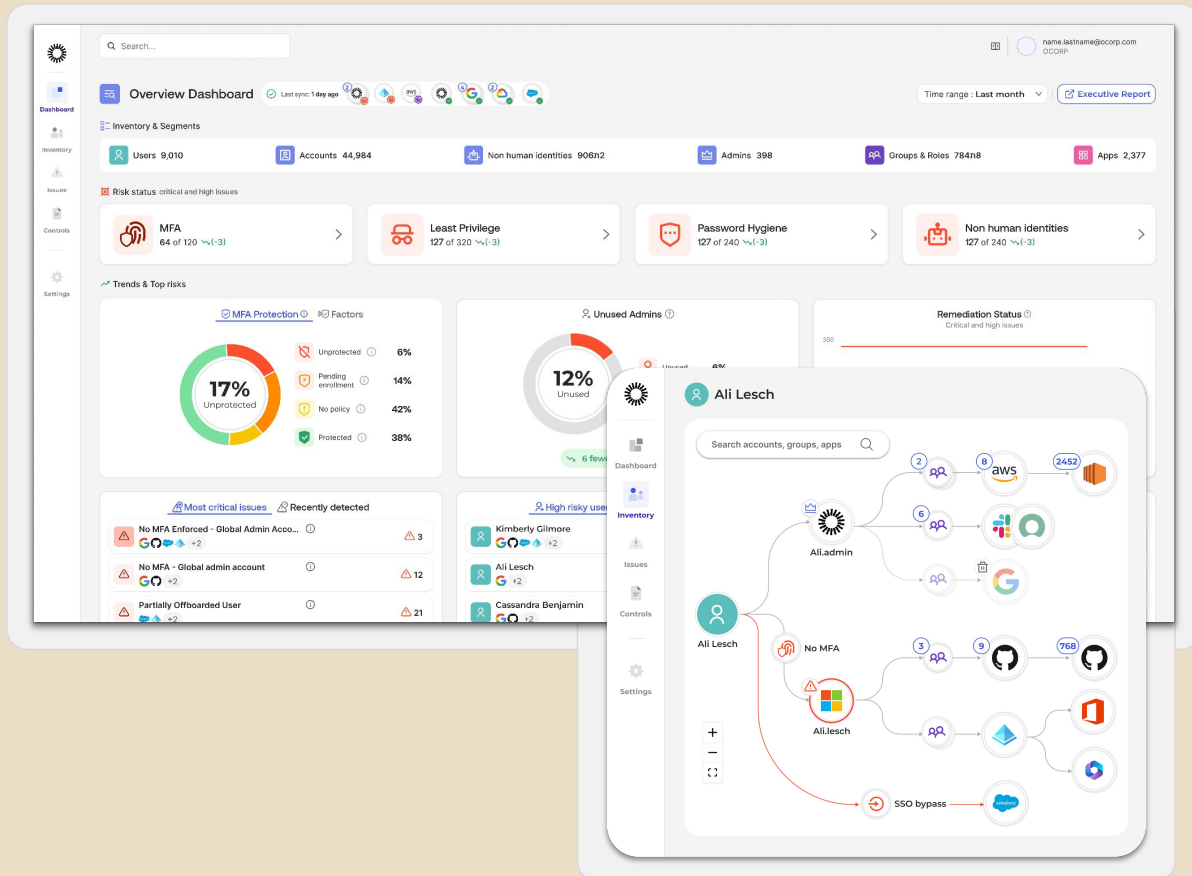
Prioritized end-to-end context with automated resolution / remediation



Continuous validation mapped to common frameworks



Delivers clear visibility to Trust but Verify



Secure Partner Access

Enable customers to securely manage business partner access to shared applications at greater scale

Key Features



Realms and Realm Assignments

Create, add, and remove partner users to/from mutually exclusive teams within a single Okta tenant.



Add Partner Users into a Realm

Configure business partners' OIDC and SAML 2.0 identity services and add to a Realm using JIT provisioning.



Delegated Partner Admin Controls

Delegate administration to partner admins with granular permissions to manage specific users, groups, and app assignments.



Partner Admin Portal

Provide an out-of-the-box portal for partner admins to manage their users and app assignments. This removes the need to grant partner admins access to the Okta Admin Console.



Realms and Realm Assignment APIs

Provides API operations to manage realms and operations to manage Realm Assignments.

Value Prop:

- Securely configure, manage, and view all partner users and policies within a single Okta tenant
- Provide secure boundaries for different users and IdPs within your user directory to safeguard user data
- Quickly onboard new partner users from external sources & automatically assign apps
- End users can use their corporate credentials to access shared apps
- Delegate day-to-day operations to partner admins
- Uphold least-privilege access with a separate app outside of the Okta Admin Console for delegated partner admins

Licensing Restrictions:

- Order form language adds terms & conditions to specify this functionality is for partner management
- Requires OIE

okta Customer First

Our solutions

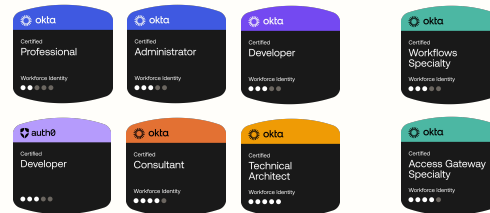


Training and Certification

Training

- Expert Learning Pass
- Private + Public Instructor-led training

Certifications



Professional Services

Value Acceleration Services

- Okta Expert Assist
- Okta Diagnostic
- Okta Experience Design
- Okta Blueprint
- Okta Transformation Design

Implementation & Migration Services

- Setup & Configuration
- Tenant Migration
- New Product Feature Rollout

Expert Services

- Tech Advisory Services
- Resident Services
- Expert Services

Customer Success, Technical Account Management, and Support

Premier Success Plans

- Basic
- Silver
- Gold

Gold Add-On Services

- Okta:
- Dedicated Customer Success Executive
- Okta and Auth0:
- Dedicated Technical Account Manager
 - Mission Critical Support Plus

(Gold add-ons available as half-time resources)

