Identity and Access Management Glossary

A

Access Management – The process of configuring the level of access for each user and group within a software system. Through this process, system administrators grant access to authorized users and restrict access to unauthorized users. This may be done hierarchically through the use of user groups. Access management requires periodic auditing and maintenance to keep up with evolving business needs and employee roles.

Further Resources: **An Overview of Identity and Access Management (IAM)**
IAM (Identity and Access Management): A guide to keeping the identity of your business in check

---

Active Directory Federation Services (ADFS) – A federated authentication system for Microsoft-centric networks that use Microsoft Active Directory as their directory services system. ADFS aims to provide seamless authentication and single sign-on functionality across a very large organization, while supporting autonomy for each organizational group to manage their own access control needs.

Further Resources: **Microsoft Active Directory and Active Directory Federation Services**
Single Sign-On: The Difference Between ADFS vs. LDAP

Adaptive Authentication – Adaptive authentication refers to authentication policies that are triggered based on device, user, or location context. Authentication requirements may be determined by static parameters, such as the type of user, their current location, type of device, and so on.
It may also be determined using dynamic parameters, in which the system continually

analyzes access patterns, and adjusts authentication policies accordingly. For example, a user who only ever logs in from a single location may be blocked if they attempt to log in from a different location.

Further Resources: **Okta Adaptive Multi-factor Authentication in Action**

Adaptive Multi-Factor Authentication – Adaptive authentication is all about dynamically adjusting login parameters based on unique scenarios. One of the parameters that adaptive authentication can adjust is the requirement for an additional factor of authentication, or step-up authentication. For example, if the system detects an unusual access pattern, it challenges the user for an additional authentication factor (e.g. a code sent via SMS) to establish identity assurance rather than blocking the user altogether.

Further Resources: **Learn About Adaptive Multi-factor Authentication**

API Access Management – Application programming interfaces (APIs) have unique authentication challenges because the user is typically another software system rather than a person. Okta's API Access Management system provides functionality to assist with this challenge by ensuring that API services are well-integrated with the rest of the user management system.

Further Resources: **API Access Management Demo**
API Access Management Product Page
Securing Digital Business with API Access Management

Application Network – The current trend of moving away from monolithic enterprise IT systems toward a system of of smaller applications from multiple vendors, which are integrated using open APIs and standards. This allows vendors to focus on a specialized niche, and enterprise customers to have more flexibility in choosing their functionality à la carte.

Further Resources: **Getting Started Guide: Okta Integration Network**

Attack Surface – The sum total of an enterprise's abstract "surface area" that can be targeted by attackers. Bugs, vulnerabilities, and insecure policies can all comprise part of the attack surface. The goal of strong identity access management is to limit the attack surface to reduce overall risk through security best practices such as automated user provisioning and deprovisioning, patching, and least privileged access control.

Further Resources: **Solution Brief: Protect Against Data Breaches**

Authentication – The process of determining that the party with which you are communicating is indeed who they claim to be. In other words, the process of determining a user's identity.

Further Resources: **Authentication: Achieve scale and security with innovative authentication solutions for your team**
Security Starts with Authentication
The Okta Authentication Guide

Authentication Factors – This refers to three mutually reinforcing categories of authentication schemes:
1. Something you are (e.g. your retina, thumbprint, voice characteristics)
2. Something you have (e.g. a specific device, a fob)
3. Something you know (e.g. a password, a secret code)

Further Resources: **Demo: Multi-factor Authentication**
MFA for Your Apps

Authorization – The process of determining whether a given identity is allowed to access a given resource or function.

Further Resources: **What is an Authorization Server?**

B

BeyondCorp – Refers to type of a zero trust security model that focuses on individual users and devices instead of network perimeters. BeyondCorp is guided by the principles of perimeterless design, context-awareness, and contextual access management.

Brute Force – A method of attack whereby an attacker systematically attempts all possible combinations of inputs, usually by automating the process with a script.

C

Cloud Identity Management – A service such as Okta that is hosted in the cloud, offering identity, authentication, and authorization functions for other cloud-hosted software services. A cloud identity management system is an alternative to traditional directory service systems, which typically manage identity for on-premises monolithic enterprise applications. These often leave cloud services with siloed identity services that must be managed individually, thus complicating lifecycle management.

Further Resources: **How Cloud Identity Management Helps Companies Go Digital**
The Okta Identity Cloud

Continuous Authentication – Continuous authentication is a process that continually monitors a user's session with an eye for authentication, and raises authentication challenges whenever there are signals that a user may have changed. Signals can be based on subtle usage patterns, including unique behavioral biometrics such as typing speed, language fingerprints, and mouse movement patterns.

Continuous authentication can mitigate risks such as impersonation, if someone else accesses a user's unmonitored session, and inconvenient timeouts that require users to log in again.

Customer Identity Access Management (CIAM) – Customer Identity Access Management (CIAM) is a software solution that allows an organization to control customer access to applications; determine customer identity by linking with databases, online profiles, and other available information; and securely capture and manage customer profile information.

CIAM supports organizations in conducting targeted marketing, providing seamless authentication for customer support, and gathering business intelligence analytics to better serve customers with new product features and updates.

Further Resources: **Creating a Secure, Seamless Customer Experiences with Customer Identity and Access Management**

D

Data Breach – Refers to an incident whereby data is accessed by an unauthorized individual or software system.

Further Resources: **Smart Authentication Can Stop Data Breaches**
Stop Data Breaches with Smarter Authentication
CIO eGuide: Preventing Data Breaches

Data Breach Prevention – Includes technology, people, and process considerations — all of which work together to protect an organization. From a technology perspective, this includes well-maintained user authentication and authorization configuration, systems that scan and block network activity in real time based on content filtering policies, or "circuit breakers" that detect potential exfiltration based on an abnormally high outbound data rate.

Further Resources: **Smart Authentication Can Stop Data Breaches**
Stop Data Breaches with Smarter Authentication
CIO eGuide: Preventing Data Breaches

Deprovisioning – The process of removing access for a particular user from software systems. For example, when an employee leaves the organization, their user profile must be deprovisioned.

Deprovisioning is generally more complicated than simply deleting the account, because it's often desirable to retain and accurately attribute the user's previous contributions, so the account must remain in some type of disabled state.

Further Resources: **Provisioning and Deprovisioning**
Preparing Your Organisation for the GDPR: What You Need to Know

E

Employee Identity Management – The process of cataloguing employees in a software system. Employee identity management often includes representing the organizational structure of functional groups.

Employee identity management requires ongoing maintenance, such as when employees are hired or leave the organization. It also often includes an authentication scheme, such as having the employee set their account password.

Further Resources: **Lifecycle Management**
Provisioning and Deprovisioning

F

Federated Identity – In a federated identity system, multiple software systems can share identity data from a larger centralized system. For example, an application for consumers may allow its users to log in using a Google or Facebook account.

An enterprise network may use a federated system so that branch offices can manage their own identity system, while connecting systems from each branch through a system at head office. This would allow employees traveling to a different branch office to use the computer systems, but different access policies would likely still apply.

Further Resources: **Enterprise Federation for Your Service**

I

Identity as a Service (IDaaS) – This is a variant on the concept of Software as a Service

(SaaS), indicating that identity management can be outsourced and purchased as a cloud-based service instead of either purchasing the software and operating it in-house or building the functionality from scratch in-house.

Further Resources: **What is IDaaS? Understanding Identity as a Service and Its Applications**
Modernizing the IT Infrastructure in Government with IDaaS

Identity and Access Management (IAM) – The process of codifying not only users and groups in a software system, but also what resources they are each able to access and what functions they are each able to perform. IAM addresses authentication, authorization, and access control.

Further Resources: **An Overview of Identity and Access Management (IAM)**
IAM (Identity and Access Management): A guide to keeping the identity of your business in check
Identity and Access Management Strategy

Identity Management – The process of codifying users and groups, as well as the metadata related to each of these entities, such as contact details, location, photo, etc. Includes mechanisms for authentication of these entities.

Further Resources: **Identity Management: An Evolving Landscape**

Incident Response Planning – The practice of documenting a planned reaction to a security incident. This is not necessarily a breach, rather the investigation is part of the process of determining whether there was an attack, who/what was involved, and if there was any data exfiltration. Having an incident response plan in place allows companies to react quickly and decisively if a security incident occurs. Elements of the plan may involve revoking widespread access temporarily, shutting down systems, notifying stakeholders, and establishing processes for re-establishing access, re-evaluating policy and process, remediation, backup, and recovery.

Further Resources: **Automate Security Incident Response with Okta**
Okta Incident Response Guide

J

JSON Web Token (JWT) – A token representing some number of claims, most typically the claim that the holder is authenticated and authorized to access a resource. These tokens are stored in a JSON format with standardized fields for issuer, subject, and expiry. Web applications often employ a refresh token to automatically generate new access tokens indefinitely.

JSON web tokens are standardized as **RFC 7519**.

Further Resources: **JWT Validation Guide**
Validating Access Tokens
REST Service Authorization with JWTs

L

Lightweight Directory Access Protocol (LDAP) – Lightweight Directory Access Protocol refers to a protocol for interacting with a hierarchical directory service database, particularly for authentication and authorization.

However, the term LDAP has also come to represent a wide range of directory system implementations, including OpenLDAP, Apache Directory, and FreeIPA.

Further Resources: **Single Sign-On: The Difference Between ADFS vs. LDAP**

Least Privileged Access Control – The process of codifying not only users and groups in a software system, but also what resources they are each able to access and what functions they are each able to perform. IAM addresses authentication, authorization, and access control.

Further Resources: **How Companies Need to Set Up Privileged Access Management**
The Risks of Privileged Access Management – and How to Protect Your Company

---

Lifecycle Management – This term recognizes that many entities represented in a software system will be at a certain stage in a lifecycle, and their access needs to be managed accordingly. For instance, an employee may start off as a "candidate," then become a "full employee" with one or more positions over their tenure, and ultimately cease to be an employee and be deprovisioned entirely.

Lifecycle management can also apply to other things. For instance, devices may be purchased, provisioned for a particular user, reprovisioned for a different user, and ultimately deprovisioned and sold or discarded.

Further Resources: **Okta Lifecycle Management Vision and Overview**
Identity and Lifecycle Management
Lifecycle Management: There's an API for That

M

Mobility Management – The practice of configuring security policies, monitoring usage and location, and enabling the functionality for provisioning and deprovisioning. This includes remotely wiping data from devices, whether company-owned or employee-owned.

Further Resources: **Adopting Your Mobility Management Solution**

Multi-Factor Authentication (MFA) – A combination of at least two of the three authentication factor categories. MFA is a more general form of two-factor authentication. It often refers to a system that combines two or more authentication requirements in different circumstances. MFA significantly increases system security, especially in the case of credential compromise, because each additional authentication factor requires additional effort to compromise.

For instance, phishing for passwords has a relatively high success rate and can be done at scale remotely, but stealing the corresponding physical token from a user's keychain would be quite difficult.

Further Resources: **The Ultimate Checklist for Choosing a Multi-Factor Authentication Solution**
Multi-factor Authentication: Moving Beyond Username & Password

OAuth 2.0 – OAuth is an open standard for allowing delegated access to user information in web applications. OAuth 2.0 is the second major revision to the standard, which completely overhauls the specification. As a result, it is not backwards compatible with OAuth 1.0.

Further Resources: **OAuth 2.0**
Demystifying OAuth

Okta Integration Network (OIN) – The Okta Integration Network is a directory of pre-built integrations with cloud, on-prem, and mobile applications that are linked with Okta's suite of directory and identity tools. This enables features like Single Sign-On (SSO) and Lifecycle Management across a wide number of otherwise disparate applications, improving adoption, user onboarding, and security for both vendors and customers.

Further Resources: **Okta Integration Network**
Directories and Systems of Record
Okta + F5 Networks = Greater scale, reliability for Pitney Bowes' global e-commerce platform
ServiceNow + Okta

OpenID Connect (OIDC) – OpenID Connect is a RESTful authentication system that uses OAuth 2.0 for authorization. It uses JSON web tokens (JWTs) and effectively provides single sign-on across multiple applications.

Further Resources: **Identity, Claims, & Tokens — An OpenID Connect Primer, Part 1 of 3**
OIDC in Action — An OpenID Connect Primer, Part 2 of 3
What's in a Token? — An OpenID Connect Primer, Part 3 of 3
OAuth 2.0 and OpenID Connect

P

Password Spray – A type of brute force password attack whereby a single common password (e.g.: password1) is tried in combination with many usernames, rather than the other way around. Many systems can detect a brute force attack against a single user and will lock the account after a number of failed attempts. By executing a brute force attack along a different axis, the attacker often goes unnoticed.

Further Resources: **Best Practices: Password Management for the App Explosion**
Moving Beyond User Name & Password

Passwordless Authentication – Describes a range of approaches to authenticate users by means other than a password. This could be one of the two other authentication factor categories (something you are, or something you have) or it may refer to a process by which an email or text containing a secret single-use code authenticates you with no other password required.

Some applications offers this option for users, who can request a single-use code or link by email that authenticates them to access the application.

Further Resources: **Customer Story: Passwordless Auth for TAL Customers**

Phishing – A type of socially engineered attack whereby a user is presented with a seemingly plausible and often mundane request, and is tricked into divulging their authentication credentials to a facade.

One common phishing attempt is an email that appears to be from the user's IT department, claiming their account requires verification, with a link directing them to a lookalike website. When they log in to the fake website, their credentials are sent to the attacker, which the attacker can then use to impersonate the user on the real site.

Further Resources: **Password Management**
Moving Beyond User Name & Password
Build a Strategy for Password Management

Provisioning – The process of establishing an identity and associated access configuration in a software system. An example is when a new user signs up for a service, or a new employee begins at an organization. Provisioning requires establishing a method for subsequent authentication (e.g. receiving user login credentials, choosing a password, etc.).

Further Resources: **Provisioning and Deprovisioning**
Okta Incident Response Guide

Public-Key Cryptography – An application of asymmetric cryptography, where one key is private and the other is public. Asymmetric cryptography means a message encrypted with one key can only be decrypted by the other. The public one is widely distributed, so that anyone wishing to send the owner of the private key a message can do so knowing that only the intended recipient will be able to decrypt it.

S

Security Assertion Markup Language (SAML) – This is a standardized protocol used to integrate authentication and authorization functions between multiple systems. It is most often used to gain single sign-on functionality between multiple applications from different vendors.

SAML implementations act as an "identity provider," which handle authentication and authorization on behalf of one or more applications.

Further Resources: **Beginner's Guide to SAML**
SAML

System for Cross-domain Identity Management (SCIM) – SCIM is a standard for modeling identity data through resources such as users and groups. It defines standard operations through a REST-based system for manipulating the resources as JSON objects.

Further Resources: **What is SCIM?**
SCIM: Provisioning with Okta's Lifecycle Management

Secure Web Authentication (SWA) – A compatibility layer provided by Okta's Single Sign-On product, allowing the integration of legacy applications that don't support federated authentication and would not otherwise be able to take advantage of organization-wide

single sign-on. The feature stores a unique password for each application, and securely posts the credentials directly to the application's authentication handler, resulting in a near-seamless SSO user experience.

Further Resources: **Help Center: Overview of Adding Apps and SSO**

Single Sign-On (SSO) – SSO enables a user to authenticate to multiple software systems with a single authentication session. A common business application of this is an employee enters their credentials once into a company SSO product and gains access to all their business apps without logging into each app separately. This is particularly helpful if the software systems are within the same organization and managed by the same authority.

From the end user perspective, SSO removes the fatigue of logging in to multiple systems or remembering multiple account passwords.

Okta SSO also includes additional features such as self service password resets, AD and LDAP integration, customizable end user experience, and a central access policy engine.

From the IT perspective, this enables faster, more secure deployment of business apps, while reducing help desk calls from tasks such as password resets.

Further Resources: **Single Sign-On (SSO): A secure entry portal that gives your team exactly what they need**

T

Time-Based One-Time Password (TOTP) – An algorithmically-generated code that is deterministic based on the current date and time and a secret "seed" value. The server knows the seed, and can easily verify that a given code is valid for the current time period. TOTP can significantly increase security because even if a code is intercepted, it is worthless after the time window has passed (usually less than a minute). This makes the logistics of an attack much more difficult.

TOTP can be implemented on a simple and inexpensive hardware device or on a smartphone. The seed is installed and is made difficult or impossible to recover or duplicate.

Token Authentication – A method of authenticating to an application using a signed cookie containing session state information. A more traditional authentication method is usually used to initially establish user identity, and then a token is generated for re-authentication when the user returns.

Two-Factor Authentication (2FA) – The combination of two out of the three

authentication factor categories. Two-factor authentication is a subset of multi-factor authentication, and significantly increases security, because each authentication factor requires a different style of attack to compromise.

Further Resources: **Two-Factor Authentication vs. Multi-Factor Authentication: What Are the Risks?**
Two-Factor Authentication for your Cloud & On-Prem Apps

U

Universal Directory – Universal Directory is the name of Okta's complete, cloud-based directory service. It can act as the main directory to store and authenticate all users types from internal employees to external partners and contractors to even customers. It also can act as a meta-directory, integrating with an existing on-prem directory (such as Active Directory or LDAP) or any other app (such as an HRIS), giving companies a central place to manage all their users, groups, and devices.

Other Okta products can be tied together through Universal Directory, enabling more advanced use cases. These products include Single Sign-On (SSO), Adaptive Multi-Factor Authentication (MFA), and Lifecycle Management.

Further Resources: **Tips to Better Leverage Your Active Directory**
Using Universal Directory

Universal Authentication Frameworks (UAF) – UAF is an open standard developed by the FIDO Alliance with the goal of enabling a secure passwordless experience for primary authentication, as opposed to a second factor as described in U2F. Under the spec, the user presents a local biometric or PIN and is authenticated into the service. This protocol is not yet embedded in the major browsers, which has limited its adoption.

Universal 2nd Factor (U2F) – U2F is an open standard, whereby a hardware token device can attest the holder's identity through a challenge and response protocol. The token device is connected via USB or NFC (near-field communication).

It is the standard maintained by the FIDO Alliance and is supported by Chrome, Firefox, and Opera.

Further Resources: **Should You Choose U2F or Adaptive MFA?**

W

WebAuthn – An evolution of the FIDO U2F and UAF protocols. WebAuthn continues in the FIDO tradition of allowing for using credentials for step up authentication. However, it's biggest innovation is in enabling users to authenticate to services without necessarily needing the user to identify themselves first (through the use of a username and password combination).

Further Resources: **WebAuthn: A Developer's Guide to What's on the Horizon**

Z

Zero Trust – Zero Trust is a security framework developed by Forrester Research in 2009 that throws away the idea that we should have a trusted internal network vs an untrusted external network. Rather we should consider all network traffic untrusted.

This research has evolved to discuss an Zero Trust Extended Ecosystem that includes the need to secure the workforce through strong identity and access management, along with multi-factor authentication. Forrester has coined the term "next-generation access" to describe this critical component.

Further Resources: **Zero Trust with Okta: A Modern Approach to Secure Access from Anywhere**
How Okta Delivers a Zero Trust Solution for Customers

Partners

Responsibility

Okta for Good

Diversity, Inclusion & Belonging

Starting with Okta

The Okta Advantage

Customer Identity Cloud

Workforce Identity Cloud

Free Trial

Pricing

Contact Sales

Trust

Status

Accessibility

Help & Support

Help and Support

Frequently Asked Questions

Contact Us

To connect with a product expert today, use our chat box, email us, or call +1-800-425-1267.

Contact Us