Defining Identity and Access Management
Identity and access management (IAM) systems automate business processes to manage identities, credentials and access rights across systems and applications. This document defines the functional and integration components of IAM systems.

Contents

1 Introduction 1

2 Multiple account repositories 2

3 Managing identities and entitlements across applications 3

4 User communities 4

5 Data that must be managed 6

6 IAM components 7

6.1 Directories ................................................................. 7
6.2 Web access management (WebAM) ...................................... 7
6.3 Federated access management .......................................... 8
6.4 Password management .................................................. 8
6.5 Credential management ................................................ 9
6.6 Enterprise single sign-on (E-SSO) ....................................... 9
6.7 Identity and access management ....................................... 9
6.8 Role-based access control (RBAC) ..................................... 11
6.9 Privileged access management ........................................ 11

7 Identity and access management defined 12
1 Introduction

Identity and access management (IAM) systems automate business processes to manage identities, credentials and access rights across systems and applications. This document defines the functional and integration components of IAM systems.

The remainder of this document is organized as follows:

- **Multiple account repositories:**
  Explains why, in practice, most organizations manage data about users — who they are, how to authenticate them what they have access to — on multiple systems.

- **Managing identities and entitlements across applications:**
  The challenges created by the intersection of multiple business change processes and multiple account repositories.

- **User communities:**
  Comparing the different initial states and IAM needs of insiders and outsiders.

- **Data that must be managed:**
  An overview of the kinds of identity attributes, security entitlements and credentials that IAM automation must manage.

- **IAM components:**
  How different kinds of IT infrastructure and automated processes help to streamline and secure IAM data and processes.

- **Identity and access management defined:**
  A simple definition for what constitutes identity and access management, given the foregoing.
2 Multiple account repositories

Modern organizations run a complex mix of IT infrastructure, including:

- Directories, such as Active Directory or other LDAP implementations.
- Network operating systems, used to share files and printers.
- Customer relationship management (CRM) and enterprise resource planning (ERP) applications.
- A range of custom and vertical market applications.
- Various databases.
- Mainframe and midrange servers, typically hosting legacy applications.
- E-mail and other collaboration software.
- Human resources, payroll and contractor management systems.

Legacy systems and applications are hosted on-site but newer applications are increasingly hosted by third parties, in the cloud, often offering software-as-a-service (SaaS).

Many systems and applications rely on internal lists of accounts – users who can sign in, along with credentials such as passwords and entitlements such as group memberships. Some systems are able to externalize this information to a directory (via LDAP or Kerberos) or to a federated access system (SAML, OAuth) but many systems and applications require that some or all of this data remain in their internal, proprietary storage.
3 Managing identities and entitlements across applications

Accounts, entitlements and credentials must be managed, when users are hired, when their jobs or contact information change, when they join or leave projects, when they relocate or take time off, when they leave the organization and if they return.

The intersection of many business processes and many systems that contain IAM data is shown in Figure 1.

Unfortunately, every system and application has its own schema, its own administration user interface, is managed by a distinct team of administrators and is subject to its own change processes. This variety creates complexity, which has business consequences:

- **Cost**: Complex processes that involve multiple systems and applications are expensive to operate, requiring teams of access administrators.

- **Security**: Users with no-longer-needed entitlements, orphan accounts, dormant accounts, inconsistent approvals and gaps in audit history weaken internal controls.

- **Service**: Users are faced with complex, hard to find and hard to populate access request forms. Access is only granted after lengthy approval and fulfillment delays.

*Identity and access management* automation is intended to address this complexity and thereby reduce access administration cost, strengthen security and improve the user experience.
4 User communities

Enterprises manage identity data about two broad kinds of users:

- **Insiders**: including employees and contractors.
  Insiders spend most of their working hours engaged with the enterprise. They often access multiple internal systems and their identity profiles are relatively complex.

- **Outsiders**: including customers, partners and vendors.
  There can be many more outsiders than insiders. Outsiders generally access only a few systems (e.g., CRM, e-Commerce, retirement benefits, etc.) and access these systems infrequently. Identity profiles about outsiders tend to be less detailed and less accurate than about insiders.

The difference between insiders and outsiders and how this impacts identity and access management, can be illustrated by an example:

Consider a bank, with 15,000 employees, 5,000 contractors and 500,000 customers. Insiders at the bank are the 20,000 employees and contractors.

Insiders log into a network operating system, corporate Intranet, line-of-business applications, corporate mainframe, e-mail systems and Internet gateway. Their identity profiles include data relating to their employment and their many login IDs to internal systems. Insiders use their access – login IDs, passwords and entitlements – many times each day.

Outsiders are primarily current and prospective bank customers. Their typically have just one identifier (a customer or account number). Their profiles include contact information such as a mailing address and other contact information. Outsiders only access their login IDs occasionally.

Enterprise IAM means IAM systems managing the identities, credentials and entitlements of insiders in medium to large organizations. Business-to-business (B2B) or business-to-consumer IAM systems manage, on behalf of an enterprise, the same data but about customers or partners. In practice, both the technical and business process requirements of enterprise and B2B/B2C IAM systems are quite different.

Enterprise IAM presents different challenges than identity and access management in Extranet (B2C or B2B) scenarios:
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Enterprise IAM (typical)</th>
<th>Extranet IAM (typical)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of users under 1 million</td>
<td>2 – 10,000</td>
<td>over 1 million</td>
</tr>
<tr>
<td>Number of systems and directories</td>
<td>1 – 2</td>
<td></td>
</tr>
<tr>
<td>Users defined before IAM system is deployed</td>
<td>Thousands</td>
<td>Frequently only new users</td>
</tr>
<tr>
<td>Login ID reconciliation</td>
<td>Existing accounts may have different IDs on different systems.</td>
<td>Single, consistent ID per user.</td>
</tr>
<tr>
<td>Data quality</td>
<td>Orphan and dormant accounts are common. Data inconsistencies between systems.</td>
<td>Single or few objects per user. Consistent data. Dormant accounts often a problem.</td>
</tr>
<tr>
<td>User diversity</td>
<td>Many users have unique requirements.</td>
<td>Users fit into just a few categories.</td>
</tr>
</tbody>
</table>

In short, Enterprise IAM has fewer but more complex users. Extranet IAM has more users and higher transaction rates, but less complexity.
5 Data that must be managed

Just as there are different user communities whose identities, credentials and entitlements must be managed, there are also different types of data to manage:

- **Identity data**
  This includes names, contact information and demographic data such as gender or date of birth.

- **Legal and contractual information**
  This includes information about the legal relationship between the enterprise and the user: social security number, compensation, contract, start date, termination date, etc.

- **Login credentials**
  On most systems, these are login IDs and passwords. Other possibilities include PKI certificates, hardware devices and security questions.

- **Entitlements**
  Entitlements are the access rights assigned to users. Gartner defines an entitlement as:

  > An entitlement is the object in a system’s security model that can be granted or associated to a user account to enable that account to perform (or in some cases prevent the performance of) some set of actions in that system. It was commonly accepted that this definition of entitlement referred to the highest-order grantable object in a system’s security model, such as an Active Directory group membership or SAP role and not lower-order objects such as single-file permission setting.


- **Historical data**
  For audit purposes, it is helpful to track changes to all of the above – when was the user first granted access? Who made access requests? Who approved them? What changes have occurred in the user’s contact information or name? etc.
6 IAM components

There are multiple kinds of automation available to help streamline the management of identity, entitlement and credential data. These are described below.

6.1 Directories

The cornerstone of any identity management and access governance infrastructures is a user directory.

Directories are network services which house information about users, and in many cases also about the organization itself and about IT assets. They perform a function similar to white pages or yellow pages phone books do for the public telephone infrastructure – enabling users of the network to find information about each-other and about network services.

Most modern network directories are accessed using the lightweight directory access protocol (LDAP), which is based on the older, more powerful, but more complicated and less popular X.500 protocol.

A directory is just the starting point for identity management and access governance and provides no value in and of itself. To get value from a directory, organizations must:

- Directory-enable their business applications, to eliminate silos of identity and access information.
- Implement effective technology and business processes to manage the contents of the directory.

6.2 Web access management (WebAM)

A Web access management (WebAM or WebSSO) system is middleware used to move the authentication and authorization of users out of individual web applications, to a shared platform.

A WebAM system intercepts initial contact by the user's web browser to a web application and either verifies that the user had already been authenticated (typically tracking authentication state in a cookie) or redirects the user to an authentication service, where the user may use a password, token, PKI certificate or other method to sign in.

Once a user is authenticated, the WebAM system connects the user to the application and passes identity data to the application, which need not authenticate the user itself. Some applications support direct injection of identities and require no password at all, but other applications require users to connect with a password, in which case the WebAM system must maintain a database of passwords for all users, injecting them on demand.

WebAM systems can also limit user access within applications, for example by filtering what URLs users can access or through closer integration with individual applications, which use a WebAM API to decide whether a user should be allowed to access a given function or not.

WebAM systems normally rely on an LDAP directory to identify and authenticate users.
WebAM systems are mainly designed to work with applications that cannot externalize identification, authentication or authorization using standards-based federation protocols.

### 6.3 Federated access management

Federation enables applications in different domains to share information about users.

- Federated domains must have some pre-established relationship, bilaterally or in a group.
- Information about users is exchanged:
  - Identity: *Who is this user?*
  - Authentication: *How/when did the user sign in?*
  - Authorization: *What is the user allowed to do?*
- Federation enables single sign-on between domains:
  - User attempts to access an application in domain A (the service provider).
  - The application checks the user’s browser to see if he has already been authenticated. He has not.
  - The redirects the user’s client (browser) to an identity provider (IdP) in domain B.
  - The IdP in domain B authenticates the user and redirects his browser back to domain A, along with a cryptographically signed assertion about his identity and entitlements.
  - The application in domain A reads the assertion, validates the cryptographic signature, and automatically signs the user in.
  - The user is able to perform the same action against other applications in other domains. If they all trust the IdP at domain B, he may not be required to sign in again – hence single sign-on.
- In some deployment pattern, federation eliminates some user management:
  - Domain B trusts domain A to name its own users.
  - Domain B **does not** create its own objects for domain A users.

There are multiple standards for federation, including the security assertion markup language (SAML – v1 and v2), WS*Security (mostly Microsoft) and OAuth (used by consumer web sites like Facebook and Live.com). The most common language/protocol for federated authentication between enterprise applications is SAML v2. The most common language/protocol for consumer-facing web sites is OAuth v2.

### 6.4 Password management

Password management systems are intended to help users manage their own passwords. They typically include:
1. Password policy enforcement, to ensure that users select secure passwords.
2. Password synchronization, so that a password change on one system automatically flows to others and so that users consequently have fewer passwords to manage and remember.
3. Self-service password reset, so that users can reset forgotten passwords and clear lockouts without relying on a call to the IT help desk.
4. Enrollment for data such as security questions or mobile phone numbers, that can be used to authenticate users who forgot their password.
5. Assisted password reset, to streamline help desk resolution of login problems.

6.5 Credential management

Credential management systems are modern versions of password management systems. In addition to all the capabilities of password management systems, they add:

1. Self-service problem resolution for users with one time password tokens, including PIN resets, clock synchronization and issuing emergency pass-codes to users who left their device at home.
2. Self-service unlock for users whose PC is protected with full disk encryption, but who forgot their pre-boot password.
3. Password reset available from the PC login screen, not just a web browser. This may include access even when the PC is off-site, which requires VPN integration.
4. Strong, multi-factor authentication, for example by sending a PIN to users via SMS as a first step in the authentication process.
5. Access to self-service using smart phones and voice phone calls, not just PC browsers.

6.6 Enterprise single sign-on (E-SSO)

Enterprise single sign-on (E-SSO) systems store user passwords to applications in a “password wallet.” When users launch an application that presents a login prompt, the E-SSO system looks up the user's password to that application and automatically fills in the blanks. When an application asks the user to change his password, the E-SSO system will generate a random password, store it in the application and update its wallet.

E-SSO systems reduce the nuisance of many legacy application login prompts for users, but they tend to lock users into a single client device platform, such as corporate Windows PCs.

6.7 Identity and access management

Confusingly, the part of an IAM infrastructure that is responsible for creating and deleting identities and accounts and for granting and revoking entitlements is, itself, also commonly called IAM.
Defining Identity and Access Management

Identity and access management systems, sometimes also called user provisioning, access governance or identity governance and administration systems, externalize the management of users, identity attributes and security entitlements out of individual systems and applications, into a shared infrastructure.

IAM systems make the creation, management and deactivation of login IDs, home directories, mail folders and security entitlements faster, less costly and more reliable. This is done by automating business processes for as onboarding, change requests and deactivation for each user community and by linking these processes to the systems and applications that have account repositories.

IAM systems generally implement one or more of the following processes:

- **Automation:**
  Detect adds, changes and deletions in a system of record (SoR, such as HR) and make matching changes – create accounts, grant/revoke access, etc. on integrated systems and applications.

- **Self-service requests:**
  Enable users to update their own profiles (e.g., new home phone number) and to request new entitlements (e.g., access to an application or folder).

- **Delegated administration:**
  Enable managers, application owners and other stake-holders to request changes to identities and entitlements within their scope of authority.

- **Access certification:**
  Periodically invite managers and application or data owners to review users and security entitlements within their scope of authority, flagging inappropriate entries for removal.

- **Identity synchronization:**
  Detect changes to attributes, such as phone numbers or department codes on one system and automatically copy to others.

- **Authorization workflow:**
  Validate all proposed changes, regardless of their origin and invite business stake-holders to approve them before they are committed.

IAM systems generate value by applying the identity and entitlement changes produced by the above processes to account repositories, using connectors that can:

- List existing accounts and groups.
- Create new and delete existing accounts.
- Read and write identity attributes associated with a user object.
- Read and set flags, such as “account enabled/disabled,” “account locked,” and “intruder lockout.”
- Change the login ID of an existing account (rename user).
- Read a user’s group memberships.
- Read a list of a group’s member users.
- Add an account to or remove an account from a group.
- Create, delete and set the attributes of a group.
- Move a user between directory organizational units (OUs).
6.8 Role-based access control (RBAC)

Role-based access control (RBAC) is an approach to managing entitlements, intended to reduce the cost of security administration, ensure that users have only appropriate entitlements and to terminate no-longer-needed entitlements reliably and promptly.

In the context of a single system or application, RBAC means granting privileges directly to roles and attaching users to roles. Users acquire privileges through role membership, rather than directly. Within a single system, roles are sometimes called security groups or user groups.

Single-system RBAC is a time tested and successful strategy, as it allows administrators to group users, group privileges and attach groups of privileges to groups of users, rather than attaching individual privileges to individual users.

Identity management and access governance systems extend RBAC beyond single applications. Roles in an IAM system are sets of entitlements that may span multiple systems and applications. The key element of roles is to replace many technical entitlements with fewer roles that business users can understand. Business users can then a reasonable determination of which users should have which roles. This implicitly specifies which users should have which technical entitlements.

Roles consist of entitlements – login accounts and security group memberships. Roles are often also nested – i.e., one role can contain others. Nesting roles can reduce the cost of role administration.

6.9 Privileged access management

A privileged access management system controls access to login accounts that have elevated security rights. It typically controls access to administrator IDs, service accounts and accounts used by one system to sign into another.

Privileged access management systems typically randomize the passwords of sensitive accounts, store current passwords in an encrypted vault, connect authorized people and programs to privileged accounts and audit this activity.

A privileged access management system usually does not create privileged accounts, since that is usually a side effect of installing the system on which they exist. Similarly, these IDs are normally removed when a system is uninstalled. Instead, privileged access management systems secure access to these accounts by strongly authenticating users, authorizing their access and granting access only temporarily and with strong audit records, up to and including video capture and key-logging.
7 Identity and access management defined

With the above sections in mind, we propose a simple definition to encapsulate the various capabilities of enterprise identity management technologies:

Identity management and access governance is defined as a shared platform and consistent processes for managing information about users: who they are, how they are authenticated and what they can access.