Chapter 15: BIZUIT Authentication

Welcome to this chapter dedicated to one of the essential pillars of digital security: authentication. We'll discover how this process ensures that only authorized individuals access the right resources within an organization.

We'll start by defining what authentication is and why it's indispensable in today's business environment, where protecting data and processes is a strategic priority. We will also discuss its intrinsic link to security and access management, thus laying the groundwork for the rest of the session.

Below, we will explore in detail the authentication methods offered by BIZUIT, reviewing their features, configuration, and application examples. With this, we will be able to identify the most appropriate alternative for each scenario.

Upon completion, we will have the necessary knowledge to design and implement strong and reliable authentication strategies, capable of responding to the highest standards of security and usability.

Ideal Audience

The class is aimed at professionals involved in BPM projects, with a focus on the configuration and management of user authentication and authorization in BIZUIT. Basic knowledge of systems administration, user management, and security and authentication in enterprise applications is recommended.

Objectives

1. **Understand the basics of authentication in BIZUIT:** Learn how different authentication methods protect access to the platform.
2. **Configure authentication methods in BIZUIT:** Implement and customize options such as Active Directory, Microsoft Entra ID, OAuth, Google OAuth, Facebook OAuth, and the BIZUIT Native System.

3. **Maximize authentication security and flexibility:** Combine authentication methods according to the specific needs of the organization.
4. **Synchronize users from external systems:** Configure authentication flows that allow users from external applications and services to be integrated.

Unit 1: Key Authentication Concepts

In today's digital world, where security is a strategic pillar, authentication becomes the first barrier of defense against unauthorized access. It is the mechanism that ensures that only the right people, at the right time, enter the resources that correspond to them. Without this initial step, any system would be exposed to risks that could compromise critical data, processes, and assets.

What is Authentication?

Authentication is the process by which a system verifies a user's identity. In layman's terms, it answers the question, "Is that really you?" This process is made up of three fundamental elements:

- **Credentials:** The information that the user submits to prove their identity. It can be something you know (a password), something you have (a token or security key), or something you are (a fingerprint or facial scanner).
- **Verification:** The validation of those credentials against an authority source, such as an on-premises database or a third-party identity provider.
- **Result:** The system grants or denies access based on the validity of the credentials.

Why is it Important?

A strong authentication strategy not only protects information, but also has a direct impact on operational efficiency and regulatory compliance.

- **Resource protection:** Prevents unauthorized users from accessing sensitive data or features. In BIZUIT, for example, successful authentication can allow a user to access financial reports, while their **Authorization role** will determine whether they have permission to edit them.
- **Risk reduction:** Implementing robust methods, such as **multi-factor authentication (MFA),** hinders common attacks such as credential theft. This is not a minor detail: **more than 80% of security breaches are caused by compromised credentials**.
- **Regulatory compliance:** Sectors such as healthcare or finance are subject to strict regulations (GDPR, HIPAA), and proper authentication is an essential requirement to comply with them and avoid penalties.

Authentication, Security and Access Management

Authentication is not an isolated process. It is part of an ecosystem that also includes **authorisation** and **supervision**.

- **Authentication: Verify who you are**. It is the gateway.
- **Authorization: Define what you can do once inside**. Once a user is authenticated in BIZUIT, their role (e.g., Administrator, Operator, or Auditor) determines the modules, forms, and processes they have access to.
- **Monitoring: Logs and analyzes activity** to detect suspicious behavior or failed login attempts.

Conclusion

Authentication is much more than just a login – it's the first step in protecting data, preventing incidents, and ensuring precise control over who can do what within an organization. A robust strategy ensures that the right users access the right resource at the right time, reducing risk and improving operational efficiency.

In the next unit, we'll explore how to implement different authentication methods in BIZUIT, from on-premises options like **Active Directory** to integrations with third-party providers like **Google OAuth**.

Unit 2: BIZUIT Authentication Methods

In this unit we will delve into the authentication options offered by BIZUIT, a platform designed to respond to the highest security and integration requirements. We will analyze in detail each available mechanism and its configurations.

1. Active Directory

Active Directory (AD) is Microsoft's most widely used solution in corporate environments to manage users, resources, and security policies from a single point. Thanks to its centralized structure, it is ideal for local networks and hybrid scenarios where unified management is key.

- **Advantages of integrating AD into BIZUIT:**
    - **Centralization:** Credentials are managed in a single repository.
    - **Security:** Use encrypted connections using LDAP.
    - **Compatibility:** Works seamlessly in on-premises and hybrid environments.
- **Configuration options in BIZUIT:**
    - **AD Type:** Allows you to select between connection to a **Domain Controller**, a local AD (Machine) or an application directory (Application Directory).
    - **Active Directory Domain Path:** Defines the LDAP path for the domain (optional).
    - **Role and User Synchronization:** Allows you to import roles from AD, although it is recommended to disable if more granular management is required.

2. Microsoft Entra ID (Azure AD)

Microsoft Entra ID, formerly known as Azure Active Directory, is Microsoft's cloud solution for identity management and access control. Designed for hybrid or fully remote environments, it enables organizations to authenticate users from anywhere and with high security standards.

- **Advantages of integrating Entra ID into BIZUIT:**
    - **Global access:** Users can authenticate from any location.

- **Multi-factor authentication (MFA):** Adds a second layer of verification, such as a code sent to the mobile.
- **Advanced Security:** Includes features such as *Conditional Access*, which restricts access based on location, device type, or risk level.

- **Configuration options in BIZUIT:**

  - **Customer ID and Directory:** Credentials obtained in the Azure portal, required for connection.
  - **Role Sync:** Allows you to import the roles defined in Entra ID.

3. Generic OAuth

OAuth (Open Authorization) is a widely used standard for securely delegating authorization. Thanks to this protocol, BIZUIT can connect to external systems – such as business applications or identity providers – without directly storing user passwords.

- **Benefits of integrating OAuth into BIZUIT:**

  - **Enhanced Security:** Prevents password exposure.
  - **Scalability:** Enables integration with multiple vendors, from in-house solutions to cloud services.
  - **Customization:** It is possible to configure parameters to map supplier information (such as roles and permissions) to internal BIZUIT fields.

- **Configuration options in BIZUIT:**

  - **Authorization and User URLs:** Addresses for authentication and obtaining user data, respectively.
  - **Client ID and Client Secret:** Credentials that validate the application to the vendor.
  - **Custom Parameters:** Fields to map the information obtained from the supplier (e.g., user.name, user.roles).

4. Google OAuth

Google OAuth is a mechanism that allows users to access BIZUIT using their Google credentials. This method centralizes access management and optimizes the user experience.

- **Advantages of integrating Google OAuth into BIZUIT:**
    - **Quick integration:** Setup via the Google Cloud Console is simple.
    - **Secure authentication:** Delegate identity verification to Google.
    - **Optimized user experience:** Users use the same credentials they already handle in other services.
- **Configuration options in BIZUIT:**
    - **Client ID and Secret:** Credentials generated in the Google Cloud console.

5. Facebook OAuth

Facebook OAuth is an ideal authentication system for consumer-facing applications and external portals. It eliminates the need to create new credentials, leveraging the user's Facebook account for quick and familiar access.

- **Advantages of integrating Facebook OAuth into BIZUIT:**
    - **Optimized user experience:** Quick and familiar access.
    - **Greater reach to consumers:** Ideal for portals looking to integrate with social networks.
    - **Secure authentication:** Facebook takes care of the verification process.
- **Configuration options in BIZUIT:**
    - **App ID and App Secret:** Credentials obtained in the Facebook Developer Portal.

6. BIZUIT Native System

The **BIZUIT Native System** is an integrated authentication mechanism that uses **ASP.NET Membership**. Always available as a backup, it's especially useful for quick setups, temporary users, or scenarios where you don't have a third-party identity provider.

- **Main features:**

    - **Always-on availability:** Works even if external methods fail.
    - **Centralized user management:** Allows you to create and manage accounts directly from BIZUIT.
    - **Flexibility:** Ideal for granting temporary access or specific permissions.

Practical example: A company creates a temporary account for an external consultant, assigning them limited permissions to access specific reports without relying on an external directory.

Conclusion

In this unit we systematize the authentication options available in BIZUIT and their configuration parameters.

We reviewed Active Directory as a centralized corporate solution, with LDAP encrypted connections and full compatibility in local and hybrid environments; at BIZUIT we configured the type of AD (Domain Controller, Machine or Application Directory), the **Active Directory Domain Path** (optional) and the synchronization of roles and users, which should be disabled when we need more granular management.

We looked at Microsoft Entra ID as a cloud service with global access, multi-factor authentication (MFA), and **Conditional Access**; in its integration, we defined the **Customer ID** and **Directory ID** obtained in Azure and, if necessary, enabled role synchronization. We study **generic OAuth** to delegate authorization without storing passwords, with scalability to multiple providers and configurable mapping of information (roles and permissions); in BIZUIT we establish the **Authorization and User URLs**, the **Client ID/Secret** and the **custom parameters** (e.g., user.name, user.roles).

We reviewed **Google OAuth** as an access mechanism with delegated verification to Google and agile configuration from Google Cloud Console (with **Client ID** and **Secret**), and **Facebook OAuth** for consumer-facing portals, supported by **App ID** and **App Secret**.
Finally, we confirm the validity **of the BIZUIT Native System** – based on ASP.NET Membership – as an alternative always available for quick configurations, temporary users or the absence of an external provider, with centralized management and flexibility; we illustrate its use with the creation of a temporary account for an external consultant with limited permissions.

With this journey, we have a clear framework to choose and implement, in each project, the appropriate authentication mechanism and its specific settings within BIZUIT.

Chapter Summary

We've explored the basics of authentication and, specifically, the various **authentication options offered by BIZUIT**. The platform is distinguished by its flexibility, allowing organizations to choose the method that best suits their security policies and technology infrastructure.

We analyze the strengths of each approach:

- **Active Directory (AD):** The ideal choice for corporate environments with on-premises or hybrid networks, as it enables **centralized credential management** and leverages existing security infrastructure. It is a proven and reliable solution for access control at the network perimeter.
- **Microsoft Entra ID (Azure AD):** A modern, cloud-oriented alternative. Its main advantage is native support for **Multi-Factor Authentication (MFA)** and **Conditional Access** policies, allowing for more granular and adaptable security to the challenges of remote work and global access.
- **Generic OAuth:** An open standard protocol that gives BIZUIT a unique ability to integrate with **custom or third-party identity systems**. This is critical for environments where full flexibility is required without compromising security.
- **Google and Facebook OAuth:** These integrations not only simplify access by allowing users to use their existing social or corporate credentials, but also **improve the user experience** and **reduce administrative burden** by delegating password management to a trusted third-party provider.
- **BIZUIT Native System:** This built-in authentication mechanism acts as an **essential backup** and agile solution for specific scenarios. It is perfect for managing temporary access, service accounts or environments where the complexity of an external provider is not required, always guaranteeing the **operational continuity** of the system.

BIZUIT's ability to combine and adapt to these different authentication methods demonstrates its robustness. Understanding these options is critical to designing a security strategy that not only protects the organization's assets, but also optimizes usability and aligns with business needs. The right choice in this security layer is the first step to efficient and reliable business process management.