Whitepaper | August 2024

Authentication methods

Secure user authentication with exos 9300

dormakaba

User authentication

In today's digitally connected world, where a multitude of online platforms and services hold our personal information, user authentication has become essential for protecting user data and ensuring a secure and seamless login experience.

The main objective of user authentication is to verify the identity of a user trying to access a particular application or website. By requiring users to submit unique login credentials, such as user-names and passwords, user authentication acts as an important gatekeeper that prevents unauthorised access to sensitive information.

Authentication techniques range from simple login, where users are identified by information that only the user knows (e.g. a password), to more sophisticated security mechanisms where the user is identified by something that is in their possession or that characterises them (e.g. tokens or biometrics).

exos 9300 access control software offers a range of user authentication options, including username/password, Windows authentication and user authentication through an identity provider.

exos 9300 – user authentication options

The exos 9300 access control software offers a range of user authentication options that are easy to implement and provide a secure and user-friendly login experience.

Username / Password

Logging in with a username and password is one of the most common methods of user authentication. When a user submits their username and password, the application sends these credentials to the backend server. The backend server checks the submitted credentials against a stored database of user information.

Benefits of login by username and password:

- **Simplicity:** Easy to implement and use
- **Independence from third-party services:** Does not require complex infrastructure or third-party identity providers

Windows Authentication

Windows Authentication is a security mechanism used in Microsoft Windows environments to authenticate and authorize users to access resources. It uses Windows credentials (username and password) and can integrate with Active Directory to provide centralized management of user accounts and permissions.

Benefits of Windows Authentication:

- **Integration:** Integrates seamlessly into the Windows environment
- **Centralized user management:** Centralized user account management through Windows Active Directory
- **Security:** Provides a secure way to authenticate users based on trusted Windows credentials
- **Single sign-on (SSO):** Reduces the need for multiple logins, improving user experience and productivity

Identity Provider

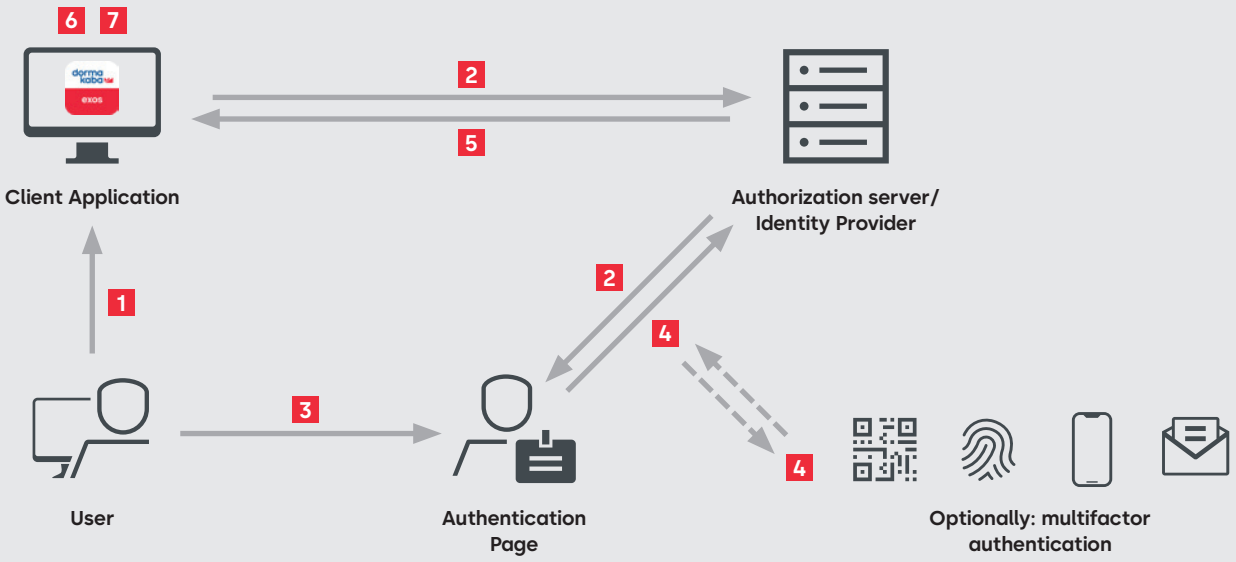
User authentication via an identity provider (IdP) is a process where a service or application delegates the responsibility of user authentication to a third-party service, known as the identity provider. Common identity providers include Microsoft Entra ID, Keycloak and Okta.

Benefits of user authentication through an identity provider:

- **Centralized user management:** User credentials and authentication processes are centrally managed by the identity provider
- **Security:** Strong protection against unauthorized access and identity theft through robust security measures, including encryption or multi-factor authentication (MFA)
- **Single sign-on (SSO):** Reduces the need for multiple logins, improving user experience and productivity
- **Federated identity:** enables users to access services and applications across different domains or organizations using the same set of credentials

User authentication through an identity provider

exos 9300 access control software supports the OpenID Connect protocol to verify the identity of users based on the authentication performed by an authorization server. OpenID Connect is an interoperable authentication protocol that is based on the OAuth 2.0 framework.



1 **User initiates authentication:** The user attempts to access a service or application that requires authentication

2 **Service redirects to IdP:** Instead of handling the authentication process itself, the service redirects the user to the identity provider's authentication page.

3 **User authentication:** The user provides their credentials (such as username and password) to the identity provider via the authentication page.

4 **IdP verifies credentials:** The identity provider verifies the user's credentials. This verification process may involve checking the username and password against its user database or using other authentication mechanisms such as multi-factor authentication (MFA).

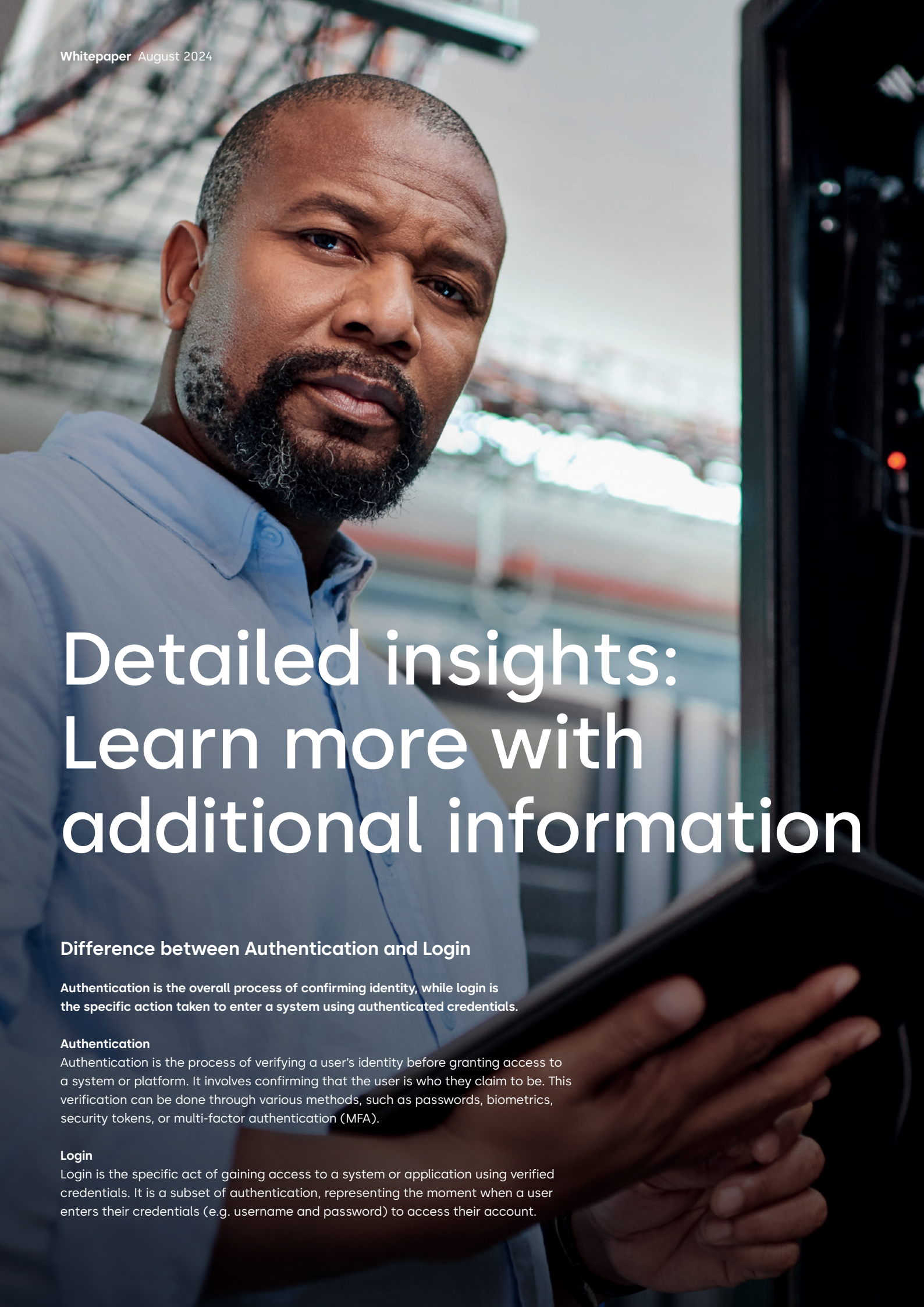
5 **User is redirected back to the service:** The identity provider sends the authentication response back to the service.

6 **Service verifies authentication response:** The service receives the authentication response from the identity provider and verifies its authenticity.

7 **User access granted:** If the authentication response is valid, the service grants access to the user, allowing them to use the application or access the requested resources.

Comparison table of user authentication methods

User authentication method	Username / password	Windows authentication	Identity provider (IdP)
Security	Medium	High	Highest
Configuration / integration efforts	Very easy	Easy	Medium (requires configuration in IdP)
3rd party application / service required	–	Microsoft Active Directory	Identity provider services such as Microsoft Entra ID, Keycloak or others
Single-sign on (SSO)	–	Yes (optionally)	Yes (optionally)
Multi-factor authentication	–	Yes (optionally)	Yes (optionally)



Detailed insights: Learn more with additional information

Difference between Authentication and Login

Authentication is the overall process of confirming identity, while login is the specific action taken to enter a system using authenticated credentials.

Authentication
Authentication is the process of verifying a user's identity before granting access to a system or platform. It involves confirming that the user is who they claim to be. This verification can be done through various methods, such as passwords, biometrics, security tokens, or multi-factor authentication (MFA).

Login
Login is the specific act of gaining access to a system or application using verified credentials. It is a subset of authentication, representing the moment when a user enters their credentials (e.g. username and password) to access their account.

7 Common Authentication Vulnerabilities

User authentication, while crucial for security, faces several threats that can compromise user accounts and sensitive data. Here are some common threats to be aware of:

1. Phishing Attacks
Phishing involves tricking users into revealing their login credentials by impersonating legitimate entities through deceptive emails or websites. Users may unknowingly provide their usernames and passwords, leading to unauthorized access.

2. Brute Force Attacks
In a brute force attack, hackers attempt to guess a user's password by systematically trying various combinations until they find the correct one. This method exploits weak or commonly used passwords.

3. Credential Stuffing
Credential stuffing occurs when attackers use previously leaked username and password combinations from one breach to gain unauthorized access to other accounts. Users who reuse passwords across multiple platforms are particularly vulnerable to this threat.

4. Man-in-the-Middle (MITM) Attacks
In MITM attacks, hackers intercept communication between a user and a website to steal login credentials. This can occur on unsecured Wi-Fi networks or compromised systems.

5. Session Hijacking
Session hijacking involves an attacker stealing a user's session token after a successful login. With this token, the attacker can impersonate the user and access their account without needing their password.

6. Insider Threats
Insider threats involve employees or trusted individuals within an organization misusing their access privileges. This could include unauthorized access to sensitive data or sharing login credentials with malicious intent.

Door
Hardware

Electronic
Access & Data

Mechanical
Key Systems

Lodging
Systems

Entrance
Systems

Service

Any questions? We will be happy to assist you.

EN, 08/2024
Subject to technical modifications without notice

dormakaba.com

dormakaba
International Holding AG
Hofwisenstrasse 24
CH-8153 Rümlang
T +41 44 818 90 11
info@dormakaba.com
dormakaba.com