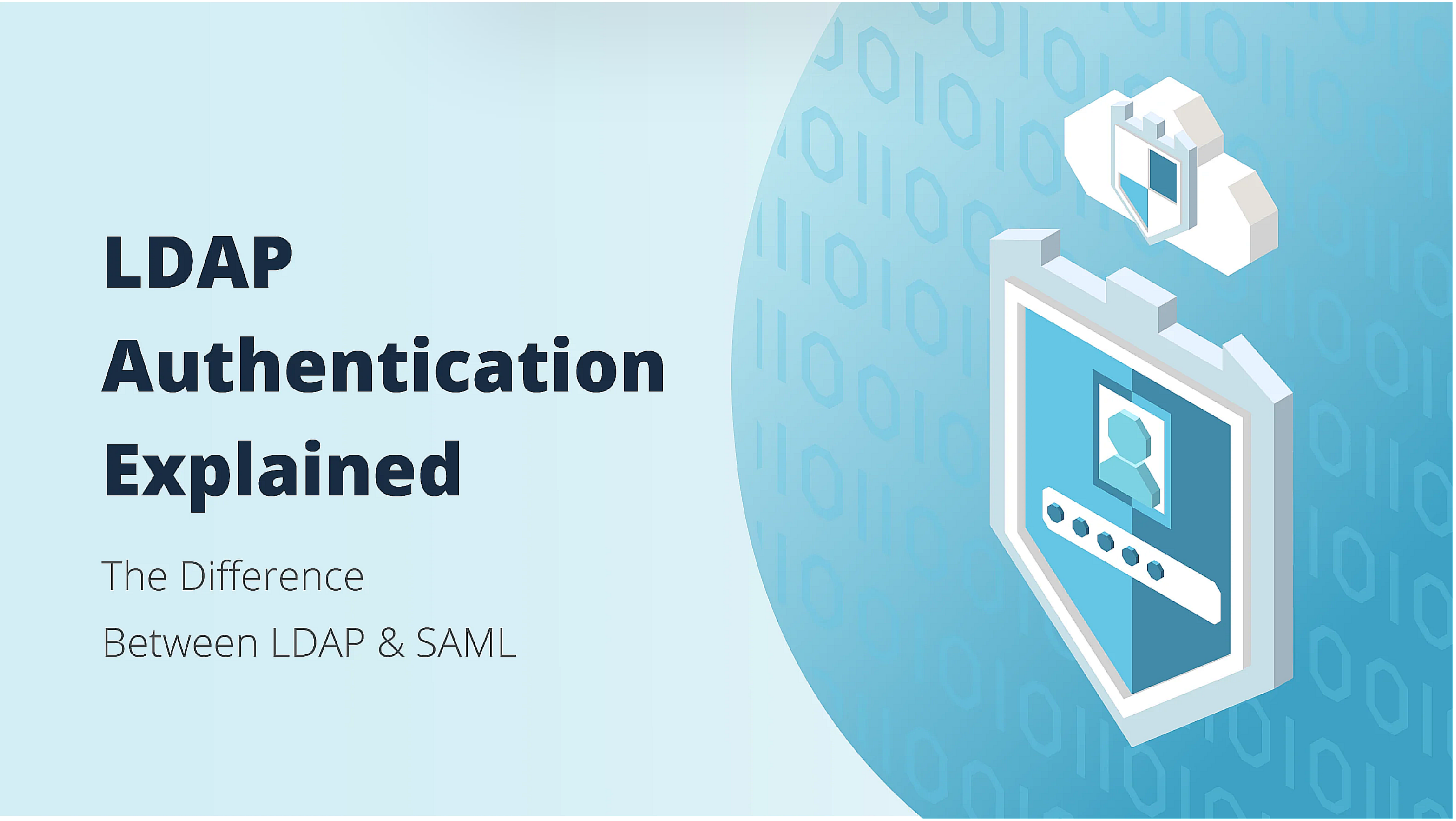
What is LDAP authentication? LDAP vs SAML

August 15, 2022

Take control of Your Online Security! ×



Both the Lightweight Directory Access Protocol and the Security Assertion Markup Language (LDAP and SAML) are widely used access and authentication protocols, often used for applications, and in a variety of organizations, yet they are employed for quite distinct use cases. Despite this, organizations should not be forced to pick either LDAP or SAML. Most firms can access a wider range of IT resources when they use a combination of authentication protocols, which ultimately helps them better achieve their business goals.

Below we'll study LDAP and SAML, compare and contrast the two, and dive into the advantages and disadvantages of these protocols.

Contents

What LDAP Authentication Is

Typically, Lightweight Directory Access Protocol is used for keeping track of authentication information, like the login and password, that will later be utilized to allow access to another protocol or system service. An LDAP database or directory cannot be accessed by a user without first authenticating (proving they are who they say they are). The database typically holds information about users, groups, and permission data and sends requested data to connected applications.

LDAP authentication entails validating the provided usernames and passwords by establishing a connection with a directory service that makes use of the LDAP protocol. OpenLDAP, MS Active Directory, and OpenDJ are a few directory servers that use LDAP in this manner.

Here is a step-by-step explanation of the authentication procedure:

- The client (a system or application that is LDAP-capable) **sends a request to access data** stored within an LDAP database.
- The client provides their LDAP server **user login details** (username and password).
- The LDAP server **compares the user's credentials against the essential user identity information** kept in its LDAP database.
- The client can **access the requested information** if the provided credentials match the stored core user identity. Access to the LDAP database will be denied if the credentials are incorrect.

LDAP authentication can be said to follow the client/server model. In this case, the client is typically an LDAP-capable system or application that is requesting data from a related LDAP database, while the server is obviously the LDAP server.

The server side of LDAP is a database with a flexible schema. In other words, LDAP can hold a range of attributes, such as an address, phone number, group relationships, and more, in addition to login and password data. As a result, storing fundamental user identities is a common use case for LDAP.

By doing this, IT can link LDAP-enabled systems and apps (for instance) to a related LDAP directory database, which serves as the authoritative source for user access authentication.

What LDAP authentication does between a client and server?

How does LDAP authentication work between a client and server? In essence, a client sends a request for data kept in an LDAP database along with the user's login details to an LDAP server. The LDAP server next authenticates the user's credentials against their primary user identity, which is kept in the LDAP database. The client is given access and obtains the required information (attributes, group memberships, or other data) if the credentials provided by the user matches the credentials associated with their core user identity that is stored within the LDAP database. The client is prevented from accessing the LDAP database if the provided credentials do not match.

Is SAML an Alternative to LDAP?

We frequently get a question similar to this: We want to switch from LDAP to SAML authentication without sacrificing any functionality. Is that possible?

Unfortunately, no. LDAP cannot be directly replaced with SAML. This is because SAML was developed to interact with cloud-based servers and apps, whereas LDAP was developed for on-site authentication. They provide very different methods of securing the authentication process. To understand this better, it’s important to get an overview of what these access protocols do.

What is LDAP?

LDAP is an example of a directory access protocol. In its most basic form, LDAP (Lightweight Directory Access Protocol) is a protocol that may be used to look up items in a directory. LDAP is a back-end protocol that occurs between a server (like LiquidFiles) and an LDAP server/directory (like Active Directory).

LDAP can also be used for authentication and when someone authenticates to the server (LiquidFiles in this case), the server will attempt to authenticate to the LDAP directory and grant the user access if successful.

The primary distinction from SAML is that - the server will make an effort at authentication. Between the web browser/Outlook plugin or any other client and LiquidFiles, nothing LDAP-related occurs. LDAP takes place between the server (LiquidFiles) and the LDAP server/directory.

What is SAML?

SAML (Security Assertion Markup Language) is a front-end protocol created for web browsers to enable Single Sign-On (SSO) for web applications. SAML lacks user lookup features and is inoperable without a browser.

How Does SAML Work?

Technically, SAML works by redirecting the web browser to the SAML server, which then authenticates the user and redirects the browser back to the server (in this case, LiquidFiles) with a signed response in the URL.

The server (LiquidFiles) verifies the signature using the SAML servers certificate fingerprint and access is granted to the user if successful.

As a result, unlike LDAP above, when a user authenticates using SAML, there is no SAML exchange between the server (LiquidFiles) and the SAML server. The only thing that happens is that the web browser is redirected between the server (LiquidFiles) to the SAML server before returning to the server to complete the authentication.

SAML operates by sending user, login, and attribute information between the identity provider and service providers. Each user just needs to log in once to Single Sign On with the identity provider, and then, whenever they try to access a service, the identity provider can provide SAML characteristics to the service provider. The service provider requests authentication and authorization from the identity provider. The user just needs to log in once since both of those systems speak the same language - SAML.

The configuration for SAML must be approved by each identity provider and service provider. For the SAML authentication to function, both sides must have the exact configuration.

LDAP vs SAML

Both LDAP and SAML share the core goal of enabling safe user authentication in order to link users to the resources they require. However, they differ in the authentication process security measures they offer. Both have advantages and disadvantages. Additionally, their respective management requirements will change over time and be very distinct.

LDAP vs SAML: Similarities

Although there are some noticeable differences, LDAP and SAML SSO are fundamentally similar. They both serve the same purpose, which is to facilitate user access to IT resources. As a result, they are frequently used in conjunction by IT firms and have established themselves as staples in the identity management sector. Organizations have used SAML-based web application single sign-on solutions in addition to their primary directory service as the use of web applications has grown significantly.

LDAP vs SAML: Differences

LDAP and SAML SSO are as dissimilar as they come in terms of their spheres of influence. Naturally, LDAP is primarily concerned with making on-prem authentication and other server processes. SAML expands user credentials to include the cloud and other web applications.

A significant distinction that is simple to overlook between the concepts of SAML SSO and LDAP is the fact that the majority of LDAP server implementations are motivated to serve as the authoritative identity provider or source of truth for an identity. Most times with SAML implementations, the SAML is not the source of truth but rather serves as a proxy for the directory service, transforming the identity and authentication process into a SAML-based flow.

Advantages and disadvantages of LDAP

An LDAP identity provider for SSO is supported by many service providers. This makes it possible for a company to use its current LDAP directory service to manage users for SSO.

One disadvantage of LDAP is that it was not created to be used in conjunction with web applications. LDAP, which was created in the early 1990s as the internet was only beginning to take off, is better suited for use cases like Microsoft Active Directory and on-premises deployments. With IT administrators favoring newer authentication standards more and more, some service providers are abandoning support for LDAP. These potential transitions should be taken into account when comparing LDAP vs SAML SSO options for your company.

Advantages and disadvantages of SAML

The most well-known standard for cloud and web applications, SAML 2.0 (the most recent version), is versatile, lightweight, and supported by the majority of platforms. It is also a popular choice for centralized identity management.

Despite being a generally safe protocol, XML assaults and DNS spoofing are security threats to SAML. Implementing mitigation protocols is a crucial step if you intend to use SAML.

Final Thoughts

Even though LDAP and SAML function differently, they’re not mutually exclusive and you can implement both in your environment. Additionally, it should be remembered that LDAP and SAML are only two of the major authentication protocols available.

Our company has spent the last 12 years working to find solutions to challenging problems for enterprise clients with a straightforward objective "We build reliable and convenient Identity and Access Management Solutions," Since then, we have gained favorable reviews from Centrify, CyberArch, Cyphort, ISACA, Arzinger, Saife, etc.

Hideez Authentication Service combines all existing authentication methods - Passwords, One-Time Passwords, Strong Two Factor Authentication (FIDO U2F), Passwordless Authentication (FIDO2), and Single Sign-On (SSO) into one solution that easily integrates with Enterprise environment based on

Hideez Enterprise Server suppport for LDAP and SAML. Your IT team will be able to save time, money, and be rest assured knowing that every user is securely authenticated to the network and is granted access to only what is permitted.

Schedule a personalized demo to find out more about Hideez's role in safeguarding your business environment.

Introduction to Hideez Authentication Service

LEARN MORE TRY HIDEEZ SERVICE FOR FREE

SHARE TWEET PIN IT

Related Posts

The Importance of IAM in Security
How It Can Be Effectively Implemented?

FIDO2: The new passwordless standard
How Does It Work?
Advantages & Disadvantages

Hideez Key for CyberArk | Authentication Integration

Stolen credentials are used to commit fraud on an enormous scale through Account Takeover (ATO) or credential stuffin...

Hideez Last Mile Authentication Solution Now Available on the CyberArk Marketplace

Hideez is excited to announce the availability of a Hideez Key integration with CyberArk that provides an added layer...

The Importance of IAM in Cybersecurity and How It Can Be Effectively Implemented

IAM (Identity and Access Management) is a critical aspect of cybersecurity that every organization should take seri...

What Is FIDO2 and How Does It Work? Passwordless Authentication Advantages & Disadvantages

Logging into a website or service using the traditional username and password combination isn’t the best or safest ...

← BACK TO <B>HIDEEZ BLOG & NEWS</B>

Be the first to get updates and new offers

Email address

Why Hideez

Hideez Key Benefits

Business Benefits

Our Clients

Our Partners

Terms of Service

Refund policy

Products

Hideez Authentication Service

USB Bluetooth Dongle

Hideez Key 3

Hideez Key 4

Hideez Key Features

Passwordless authentication

Password management

OTP Generator

Proximity Lock

Physical access

Company

About Hideez

Bug Bounty

For Investors

Contact Sales

Support

Contact Support

Privacy Policy

Terms of Use

Warranty

Cookies

© 2022 Hideez Group, Inc. All rights reserved.

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

India (INR ₹)

English