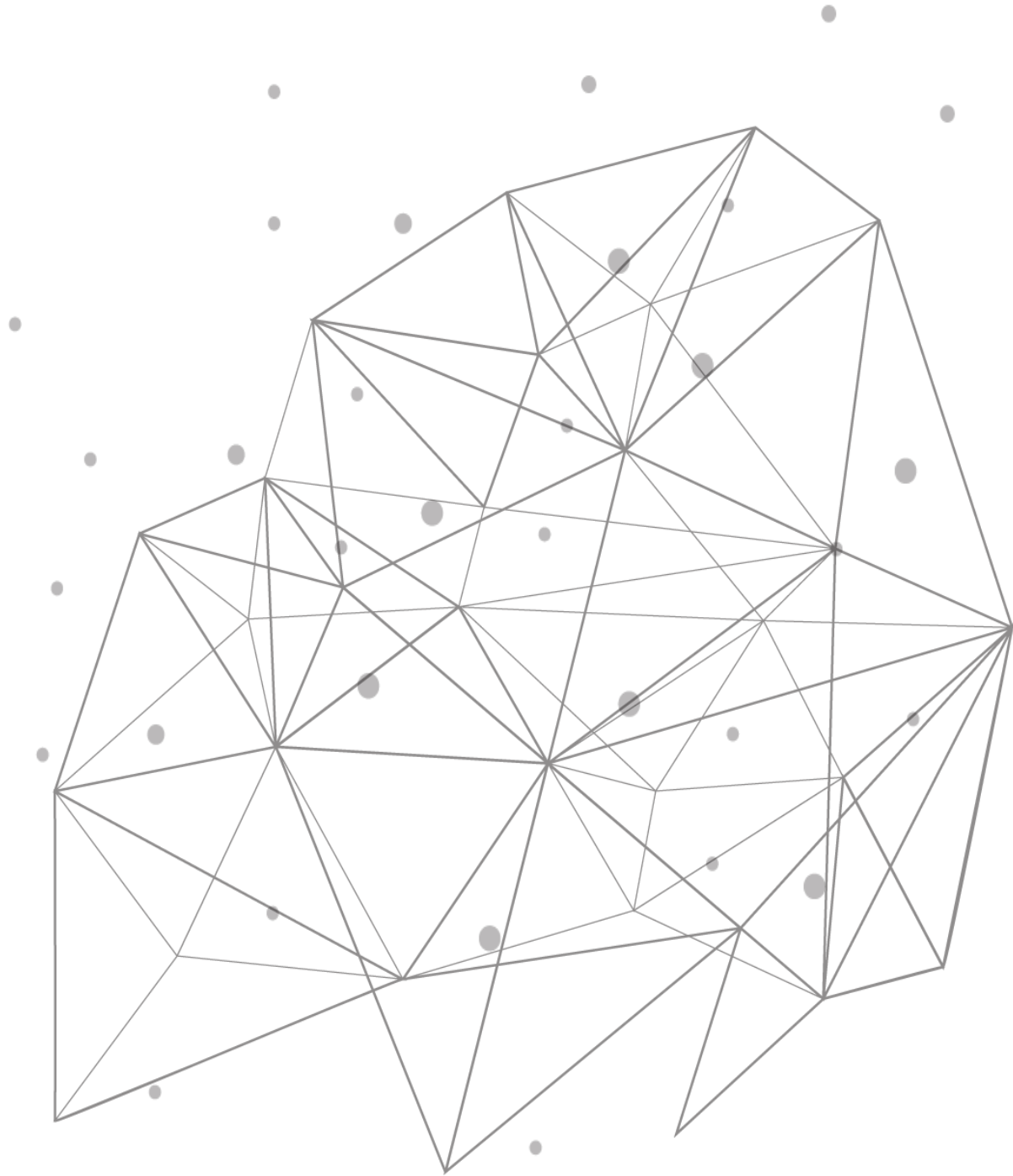

LDAP Authentication

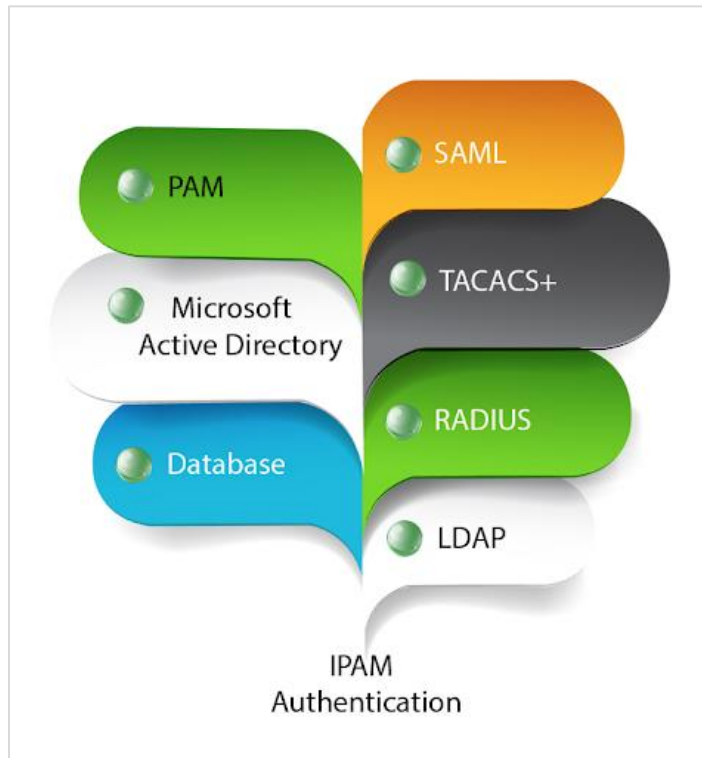


Introduction

As the years went by, user authentication and permission settings have been critical aspects of computer systems. Ever since MIT used a username and password to authenticate users, it remained part of the user interactions with the procedures and applications. After several decades later, to ensure system security, several methods have been used to authenticate users. For an organization, several types of users access the systems and applications, especially the internal ones. Several applications require logins with user accounts, sometimes the same account but with different user permissions.

TCPWave supports the following user authentication methods:

- LDAP Based Authentication
- PAM Based Authentication
- RADIUS Based Authentication
- SAML Based Authentication
- TACACS+ Based Authentication
- Internal DB Based Authentication



This whitepaper outlines the user authentication configuration in IPAM using LDAP.

Lightweight Directory Access Protocol

A Lightweight Directory Access Protocol (LDAP) server is a lightweight implementation of the Directory Access Protocol (DAP). As originally intended, X.500 Directory Low-Overhead Access provided low-overhead access to X.500 Directory. One of LDAP's main functions is to provide quick and easy access to information about organizations, people, and more. The LDAP directory stores data and authenticates

users to achieve this goal. In addition to providing applications with a means of interacting with directory services, it also provides a standard language for exchanging information.

You can find data and resources through LDAP including files and user information. It collaborates with printers, computers, and other devices connected to the internet or a company's intranet. Most vendor directory services, such as Active Directory (AD), support LDAP. It becomes easier to share information about users, services, systems, networks, and applications from a directory service to other applications and services with LDAP.

LDAP Authentication

LDAP database or directory information is a TCP protocol, that is leveraged for user authentication. LDAP databases can be replicated across multiple LDAP servers. The authentication uses port 389/tcp for normal LDAP and port 636/tcp for secure LDAP. The LDAP database contains information about users, groups, and permissions and delivers this data to connected applications. The client-server verifies Users and passwords by connecting to an LDAP directory service to validate their credentials. OpenLDAP, MS Active Directory, and OpenDJ are among the LDAP directory servers.

The following explains the authentication process:

- The client (which is an LDAP-ready system or application) requests data stored in the database of an LDAP server
- The client offers its LDAP server user credentials (username and password)
- The LDAP server checks the submitted credentials against its LDAP database's basic user identity data.
- The client can access the requested information if the submitted credentials match the recorded core user identity.
- Access to the LDAP database will be refused if the credentials are incorrect.

It's worth noting that the core user identity saved in the LDAP database includes more than just usernames and passwords, including addresses, phone numbers, and group associations.

LDAP Authentication in TCPWave IPAM

TCPWave fully supports LDAP authentication and works with different directory service providers, predominantly Microsoft Active Directory.

Prerequisites

The following are the required prerequisites to be followed by the users while setting the IPAM LDAP integration:








- Create Groups in IPAM with the same name as they exist in LDAP Servers. The names are case-sensitive.
- Configure the global policy options to auto-create the users.
- Configure the global policy options to auto clean-up of users who are no more authorized to access IPAM.








Administrator Group

Create an Administrator group for LDAP authentication. Please give it a name and assign a Role like FADM, PADM, NADM, etc. For this, please navigate to Administration -> Security Management -> Administrator Groups -> Add a new group using the '+' icon. In the below screenshot you can see such a group was

created with the name LDAP-Group.


Administrator Groups

20       


<input type="checkbox"/>	Name	Description	Created Time	Created By	Updated Time
<input type="checkbox"/>	 ldap-Group	FADM Administrator Group Created for LDAP Authentication	17:31:24 01-19-2022	twcadm	18:45:29 01-19-2022
<input type="checkbox"/>	 Default Internal FADM Group	Default Internal FADM Group	04:10:47 01-17-2022		04:10:47 01-17-2022
<input type="checkbox"/>	 Default Internal SADM Group	Default Internal SADM Group	04:10:47 01-17-2022		04:10:47 01-17-2022
<input type="checkbox"/>	 Default Internal NADM Group	Default Internal NADM Group	04:10:47 01-17-2022		04:10:47 01-17-2022
<input type="checkbox"/>	 Default Internal PADM Group	Default Internal PADM Group	04:10:47 01-17-2022		04:10:47 01-17-2022
<input type="checkbox"/>	 Default Internal RADM Group	Default Internal RADM Group	04:10:47 01-17-2022		04:10:47 01-17-2022
<input type="checkbox"/>	 Default Internal UADM Group	Default Internal UADM Group	04:10:47 01-17-2022		04:10:47 01-17-2022















Authentication Configuration

To enable the LDAP authentication, navigate to Administration >> Security Management >> Authentication Configuration, start the LDAP authentication Type, as shown in the image below.

First, select the LDAP authentication type using the check box on the left and click .

Authentication Configuration



<input type="checkbox"/>	Authentication Type	Is Active	Description
<input type="checkbox"/>	 AD		Kerberos - Active Directory authentication
<input checked="" type="checkbox"/>	 LDAP		LDAP based authentication
<input type="checkbox"/>	 PAM		PAM based authentication
<input type="checkbox"/>	 RADIUS		Radius based authentication
<input type="checkbox"/>	 SAML		SAML based authentication
<input type="checkbox"/>	 TACACSP		TACACS+ based authentication
<input type="checkbox"/>	 TIMS		Internal DB based authentication

Once this is done, you can log in to the IPAM with the LDAP user credentials successfully.

Import AD/LDAP Users

To Import users to IPAM, the global options for LDAP should be entered in Configuration -> Global Policy Management. In IPAM, if you navigate to Administration -> Security Management -> AD/LDAP Admins, you will find the top section of AD/LDAP configuration is preloaded, but it doesn't allow editing on this page.

- At the bottom section, you will find "AD/LDAP Admins Not in IPAM".
- Click Reload to pull the users from AD/LDAP server to IPAM.
- Select a user and click + to Add Admin window to the user to IPAM and save it.

However, in LDAP global policy management, if the option "LDAP Automatic IPAM User creation" is set to Yes, and if the person logs in and belongs to the group that has been authorized, then the users will get automatically created in the IPAM in case the user group already exists in TCPWave IPAM. On the other hand, if the user is previously enabled and later disabled in LDAP, if the global policy option "LDAP Automatic IPAM User Deletion" is set to yes, the user will get automatically deleted from TCPWave IPAM.

Global Policy Management					
LDAP automa					
Edit	Option	↑↓	Value	↑↓	Description
	LDAP Automatic IPAM User Creation		Yes		Controls the LDAP user creation initially in IPAM.
	LDAP Automatic IPAM User Deletion		Yes		Controls the LDAP user deletion in IPAM without associated valid admin groups.

Using LDAP Group Based Authorization

The TCPWave Global policy offers the option to use the LDAP group-based authentication to allow the users to log in to the IPAM. This can be achieved by setting “LDAP Group Based Authorization” to be set to Yes.

Global Policy Management					
LDAP Group Based Auth					
Edit	Option	↑↓	Value	↑↓	Description
	Enable LDAP Group Based Authorization		Yes		Controls use of LDAP groups for user authorization.

For LDAP Group Based Authorization to work, the following should be done.

- Create users in the AD/LDAP server and assign them to a Group in Active Directory for permission level needed in TCPWave.
- In TCPWave, create an admin group whose name exactly matches the AD Group Name.
- Create Permissions for those Admin Groups.
- Enable LDAP global policies “LDAP Automatic IPAM User creation” and “LDAP Automatic IPAM User Deletion”.

How does this option work?

- When a user logs into the TCPWave IPAM, the username/password is checked against LDAP and LDAP informs TIMs of the group membership.
- TIMS will check if there is an Admin Group that matches an LDAP GROUP of that user.
- If there is a matching group but no user exists yet, the user will be created.
- If there is not any matching group, but the user does exist from the previous entitlement, the user will be deleted.
- Revoking a users’ right in LDAP will revoke the permissions in TCPWave.

Global Policy Management

The administrator needs to define the global security settings for LDAP under global policy Management. The following needs to be determined.

- LDAP Protocol
- LDAP Security Principal DN
- LDAP Credentials
- LDAP User Group DN
- LDAP User Searchbase
- LDAP User Object Class
- LDAP Default User Admin Group

- LDAP Default User Role
- LDAP Default User Organization
- LDAP Schema
- LDAP Server
- LDAP Port
- LDAP Automatic IPAM User creation
- LDAP Automatic IPAM User Deletion
- LDAP Group Based Authorization

Note:

- Make sure that the firewall allows the IPAM to communicate with the LDAP server using 389/ 636 ports
- There should not be any typos in the user credentials.
- The users should be mapped to the appropriate LDAP user groups as configured in IPAM

Conclusion

TCPWave DDI solution assists our customers to manage and modernize their enterprise-grade solutions by ensuring they have the most innovative technology with minimal risks. For a quick demo, contact the [TCPWave Sales Team](#).