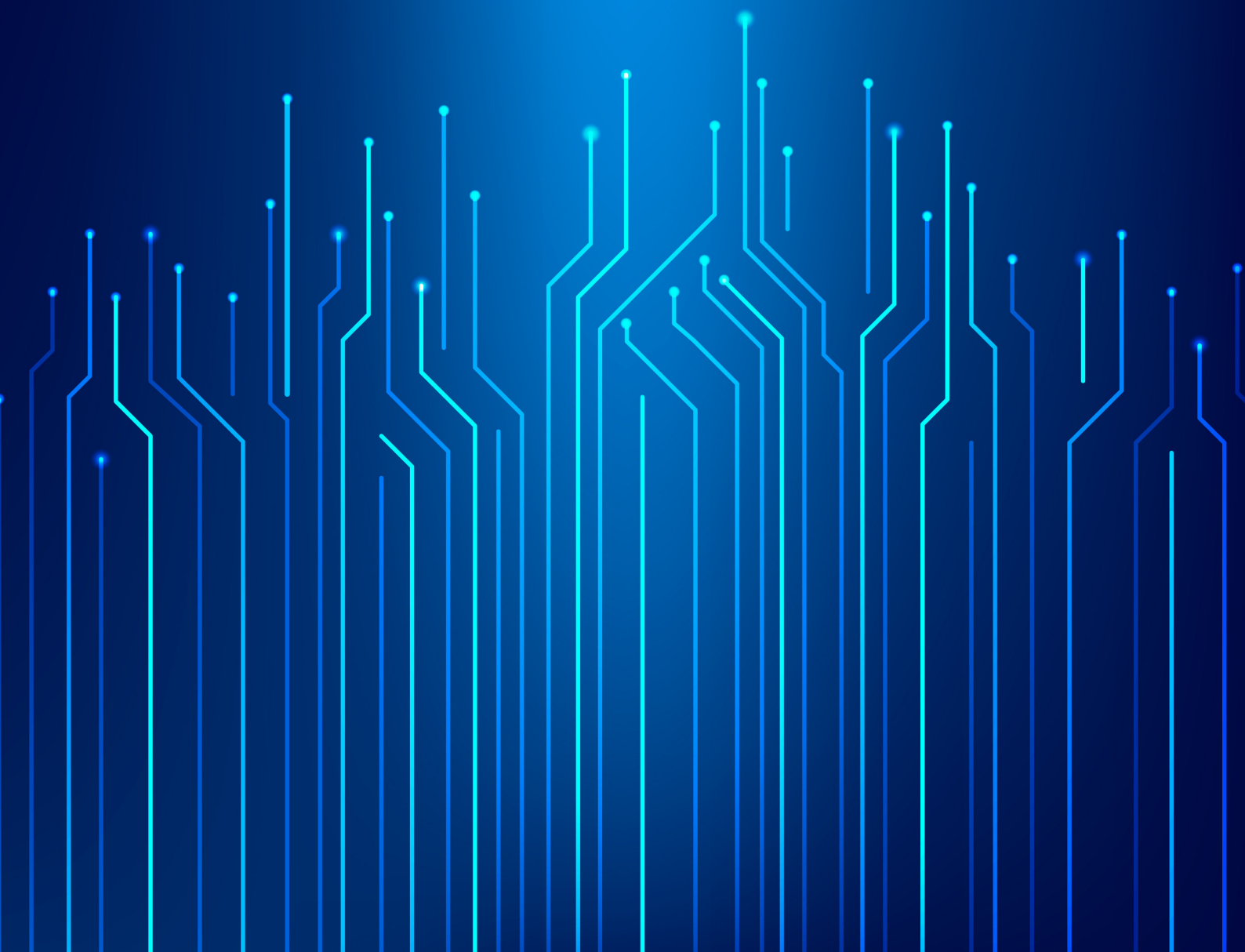


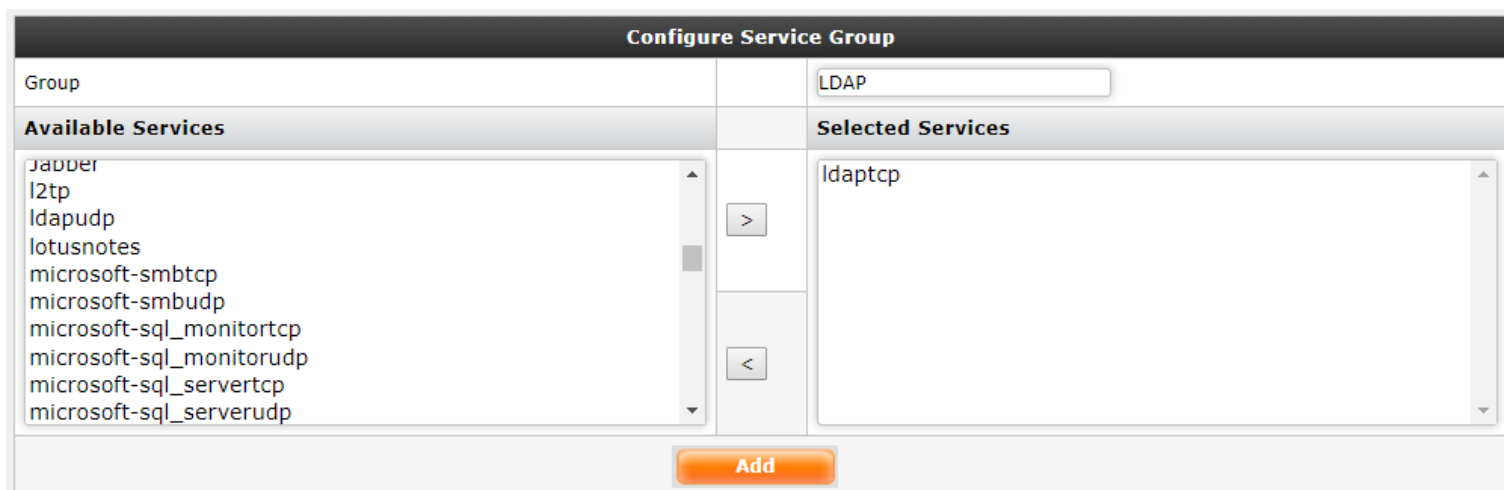
How to configure LDAP on your firewall



How to configure LDAP on your firewall

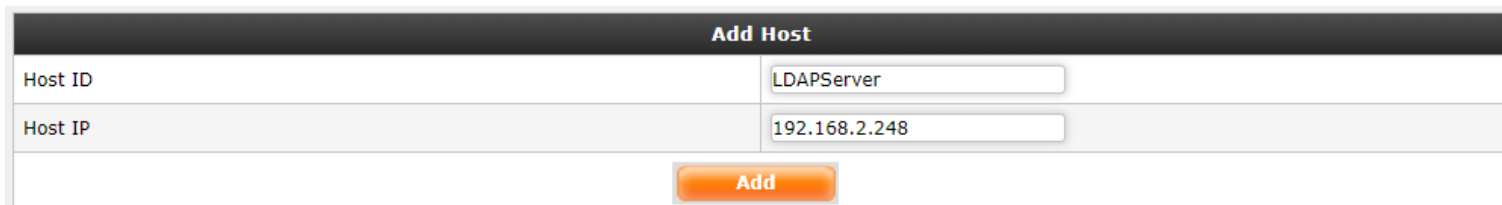
In this document, we will guide you through the configuration of LDAP on your firewall.

Step 1: Create a service group on the firewall by going to Definitions -> Protocols and Services -> Configure Service Group.



Configure Service Group	
Group	LDAP
Available Services	Selected Services
jabber l2tp ldapudp lotusnotes microsoft-smbtcp microsoft-smbudp microsoft-sql_monitortcp microsoft-sql_monitorudp microsoft-sql_servertcp microsoft-sql_serverudp	ldaptcp
Add	

Step 2: Create a host by going to Definitions-> Hosts and add **LDAPServer** as a host by specifying the appropriate IP Address.



Add Host	
Host ID	LDAPServer
Host IP	192.168.2.248
Add	

Step 3: Now create the rules for allowing LDAP service through the GajShield firewall by going to Firewall -> Policies -> Rules.

You will need to add a rule by going on Firewall > Policies > Rules & use LDAPServer in services tab to allow the firewall to access the LDAP Server as shown below

Zones			
Direction	Any	To	Any
Source	fwip-LAN	NAT	Ignore
Destination	LDAPServer	NAT	No NAT

Services and Ports			
Services	LDAP	NAT	No NAT

Step 4: Go to Configuration -> User Management -> LDAP.

Ldap Server Settings	
Server Name	gajshieldldapserver
Server IP	WebServer
Server Port	389
Distinugished Name	GAJSHIELDLDAP
Login Attribute	ldaplogin
First Name Attribute (Optional)	abc
Last Name Attribute (Optional)	xyz
Email Address Attribute (Optional)	abc@xyz.com
Bind DN (Optional)	
Password (Optional)	*****
Scope (Optional)	
<input type="button" value="Update"/> <input type="button" value="Reset"/>	
Synchronize Ldap Users/Groups	
<input type="button" value="Synchronize"/>	

Specify the following information under LDAP Server Settings:

Server name: Define a name for the LDAP configuration.

Server IP: Select the host IP Address of the remote LDAP server

Server Port: The default LDAP port is 389, if your LDAP server is using another port then you can define the custom port.

Distinguished Named: It is used to look up entries on the LDAP server and is a hierarchy of LDAP database object classes above the Common Name Identifier.

Login Attribute: Default Login Attribute is Unique Identification (UID) to identify user entries. Here you can define different login attribute as well.

First Name Attribute (Optional): Define first name attribute for LDAP configuration.

Last Name Attribute (Optional): Define last name attribute for LDAP configuration.

Email Address Attribute (Optional): Define email address attribute for LDAP configuration.

BindDN: Define distinguished name of LDAP server. Distinguished name is starting point for searching user in LDAP server.

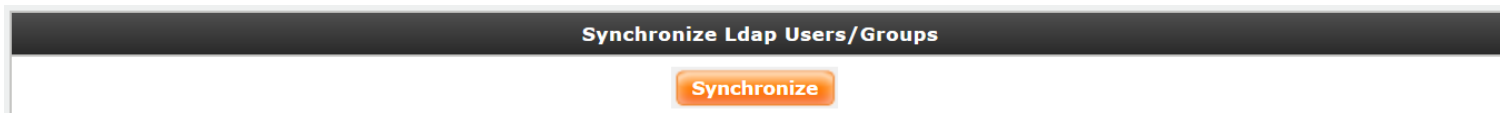
Password: Input the secret (password) to be used to connect LDAP server.

Scope: Define scope as configured on the LDAP server.

NOTE: You will also need to add a rule in the policy manager to allow the firewall access to the LDAP server.

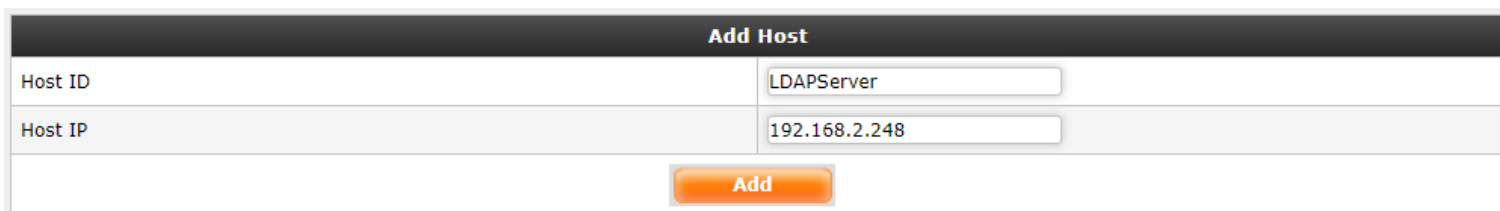
After adding the necessary information, you will have to create a firewall rule to connect to the LDAP server by going to firewall -> Policies -> Rules

Synchronize LDAP Users/Groups



The screenshot shows a dark header bar with the text "Synchronize Ldap Users/Groups". Below the header is a white rectangular area containing a single orange button with the text "Synchronize".

Synchronize LDAP Users/Groups: Click on Synchronize button to synchronize LDAP users as well as groups from LDAP users.



The screenshot shows a dark header bar with the text "Add Host". Below the header is a table with two rows. The first row has "Host ID" in the left column and "LDAPServer" in the right column. The second row has "Host IP" in the left column and "192.168.2.248" in the right column. Below the table is a white rectangular area containing a single orange button with the text "Add".

NOTE: You will have to specify LDAP option by going to Browsing -> Setup -> Browsing Options, tick on userSense and specify LDAP from the drop down menu.

Browsing Setup		
URL Blocker Instance	<input type="text" value="10"/>	
Enforce Strict Search on	<input checked="" type="checkbox"/> Google Images <input type="checkbox"/> Yahoo Images	
Enable Virus Scanning	<input checked="" type="checkbox"/>	
Large File Download Alert Limit	<input type="text" value="1024"/> KB (0 Means no alerts generated)	
App Filter Policy	Please Select ▼	
URL Filter Policy	Open ▼	
URL Filter QoS	TestPolicy ▼	

Browsing Mode Configuration		
Browsing Mode	SSL Deep Inspect	Authentication
<input checked="" type="checkbox"/> Proxy Mode Proxy Port: <input type="text" value="3128"/>	<input checked="" type="checkbox"/>	<input checked="" type="radio"/> No Authentication <input type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> TACACS+ <input type="radio"/> LDAP <input type="radio"/> Active Directory
<input checked="" type="checkbox"/> Gateway Mode	<input checked="" type="checkbox"/>	<input type="radio"/> No Authentication <input checked="" type="radio"/> GajShield userSense Choose your preference: 1. <input type="text" value="LDAP"/> ▼ 2. <input type="text" value="Local"/> ▼ 3. <input type="text" value="Please Select"/> ▼

Setup

Thus you have successfully configured LDAP on your firewall.