

© 1999-2011 SecPoint , SecPoint®, Denmark. All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. SecPoint® shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software included with this product is subject to written permission by SecPoint®. We reserve the right to make any alterations that arise as the result of technical development.

Trademarks: Windows®, Windows XP® and Microsoft® are registered trademarks of Microsoft, Corp.

The SecPoint® logo and the name SecPoint are registered trademarks of SecPoint® Denmark. All other names mentioned may be trademarks or registered trademarks of their respective owners.

Subject to change without notice. No liability for technical errors or omissions.



Preface

Thank you for placing your trust in this SecPoint product.

With the SecPoint® Protector you have chosen a powerful Security Appliance for total protection. With this appliance you can simply protect and comfortably connect individual PCs or whole local networks securely to the high-speed Internet.

LDAP Setup Guide

The documentation of your device consists of two parts: the user manual and the LDAP Setup Guide.

You are now reading the user manual. It contains all information you need to know to use and control your SecPoint® Protector. The reference manual can be found on the CD as an Acrobat (PDF) document. It is designed as a supplement to the user manual and goes into detail on topics that apply to a variety of devices.

These include for example:

- Systems design of the Protectors LDAP support
- LDAP Configuration
- Diagnosis

Model variants

This user manual applies to the following models of the SecPoint® Protector series:

- SecPoint® P300
- SecPoint® P700
- SecPoint® P1100
- SecPoint® P1600

This documentation was compiled...

...by several members of our staff from a variety of departments in order to ensure you the best possible support when using your SecPoint® product. In case you encounter any errors, or just want to issue critics or enhancements, please do not hesitate to send an email directly to:

info@secpoint.com

Our online services (www.secpoint.com) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In addition, support from SecPoint® is also available to you. Telephone numbers and contact information for SecPoint® support can be found on at the Support section in your Protector, or at the SecPoint® website.

1 Getting Started

1.1 Intro to LDAP

The Protector has three main features with uses LDAP to check the Active directory if a users is valid or not.. Then next step is to use the user right if the user is allowed to use this feature yes or not. If yes it could me a policy can be created to specify some rules for this user(s)

Before we can start we need to know what kind of Active directory we customer has and if it a windows server with Windows License it used. We LDAP communication is based on a LDAP

Ldap Server : This is where you stick either the IP address of FQDN of your Active Directory server.

LDAP Port: This is where you stick either the port number your Active Directory server. Default: 389

BaseDN: This looks complicated, doesn't it? Well no worries, it's pretty simple. Right now, wavelenghts' Active Directory setup has all the user and group accounts in a folder called Users (most of you will, too - check by using Active Directory Users and Computers from your server), and the wavelenghts domain in the newer DNS format is "wlj.wavelenghtsjournal.com" (it'll be yourdomain.yourcompanywebsite.com most likely, just like this). This means that this field for my site looks like "cn=users,dc=wlj,dc=wavelenghtsjournal,dc=com".

- So to recap, cn= wherever you have your users and groups located, usually a folder named users in Active Directory
- Also, instead of being one string separated by periods, your domain's sections are each in dc= bits. i.e. if your domain is conglomom.weownyou.com, it would look like "dc=conglomom,dc=weownyou,dc=com" in LDAP
- If your company stores your users and/or groups in a folder called Users and your domain is enron.sec.gov, your entry here would look like "cn=users,dc=enron,dc=sec,dc=gov".

In our example it a Microsoft Windows SBS server the string must be

CN=Protector,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=your domain name here,DC=lan

Search Filter: mail=

- LDAP User - Password - Self explanatory. Type in the username with Administrator right (or other account you decided to use) account here.
- LDAP Password - Password - Self explanatory. Type in the password of the above account

MENU > Advanced Menu > E-Mail Configuration > LDAP User Management



The screenshot shows the SecPoint Protector web interface. The top navigation bar includes 'Home', 'Setup', 'System', 'Backup', 'Update', 'E-Mail Configuration', 'User Administration', 'Tools', 'Reset', 'Shutdown', 'Quick Setup Wizard', and 'Support'. The 'E-Mail Configuration' menu is expanded, showing 'SMTP', 'POP3', 'E-Mail Notification', 'SMTP Configuration', 'Advanced Configuration', and 'LDAP User Management'. The 'LDAP User Management' option is highlighted.

LDAP User Management

You can choose to populate the [Domain User Management](#) list with valid email addresses from your local ldap server. To do so fill out the fields below. It is possible to use both features at the same time. A typical setup would have the value "mail=*" as search filter and the baseDN "ou=people,dc=your_domain,dc=com". You can use the fields LDAP mail to test, LDAP password and Show Query output to test your setup. Depending on your setup you may need to specify a LDAP user/password to run the search query as. When you have set the values click OK. An update will begin if a connection can be established to the server. Click show query output to get the email addresses fetched from the ldap server.

Enable LDAP:	<input type="button" value="Yes"/>
Update every :	<input type="button" value="1"/> hour
LDAP Server:	<input type="text" value="192.168.0.10"/>
LDAP Port:	<input type="text" value="389"/>
LDAP BaseDN:	<input type="text" value="OU=SBSUsers,OU=Use"/>
LDAP Search filter:	<input type="text" value="mail=*"/>
LDAP user to run query as:	<input type="text" value="protector"/>
LDAP user password:	<input type="text" value="secpoint"/>
Show Query output:	<input type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Clear"/>	

In this example our Server is a Small Business server with it Active Directory server and Mail server installed on one server:

Domain name is company.lan

AD & Mailserver: IP of your Ad server

LDAP Port: 389

BaseDN: OU=SBSUsers,OU=Users,OU=MyBusiness,DC=c your domain name here,DC=lan

Search Filter: mail=

LDAP User: Protector

LDAP Password: secpoint

LDAP mail to test: Protector

LDAP Password: secpoint

MENU > Anti Spam > Quarantine > LDAP Configuration



LDAP Configuration

You can choose to pull the end user antispam login information from your local LDAP server. To do so fill out the fields below. Leave the fields blank if you wish to use conventional login. It is possible to use both at the same time. The protector first looks in the LDAP server. If the user is not found the protector will look it up locally in its database. The login script will search for the user's email address by using the search filter. The CN is extracted from the search result. A typical setup would have the value "mail=" as search filter and the baseDN "ou=people,dc=your_domain,dc=com". You can use the fields LDAP mail to test, LDAP password and Show Query output to test your setup. Depending on your setup you may need to specify a LDAP user/password to run the search query as.

Enable LDAP:	<input type="button" value="Yes"/>
LDAP Server:	<input type="text" value="192.168.0.10"/>
LDAP Port:	<input type="text" value="389"/>
LDAP BaseDN:	<input type="text" value="CN=Protector,OU=SBS"/>
LDAP Search filter:	<input "="" type="text" value="mail="/>
LDAP user to run query as:	<input type="text" value="Protector"/>
LDAP user password:	<input type="text" value="secpoint"/>
LDAP mail to test:	<input type="text" value="protector@yourname..n"/>
LDAP password:	<input type="text" value="secpoint"/>
Show Query output:	<input type="checkbox"/>

CN=Protector,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=heating,DC=lan

MENU > Webfilter > Configuration > LDAP Authentication



2 LDAP Authentication

Webfilter users can be authenticated against an external LDAP database. To do so fill out the fields below. Leave the fields blank if you wish to use IP based authentication. It is possible to use both at the same time. You need to point your browser to the protector IP address (192.168.0.250) and port 8080.

In Internet Explorer this is done by clicking Tools -> Internet Options -> Connections -> LAN settings. Activate "Use a proxy server for your LAN". Type in the Address 192.168.0.250 and 8080 in the Port field. Click OK and OK.

A typical setup (openldap) would have the value "uid=" as search filter and the baseDN "dc=your_domain,dc=com". For Active directory setup use sAMAccountName= as search filter. You can use the fields LDAP mail to test, LDAP password and Show Query output to test your setup. Depending on your setup you may need to specify a LDAP user/password to run the search query as.

This feature also provides integration with the [Group policies](#) setup. Members can be fetched from the LDAP source by renaming the policy name to match the LDAP group. You can change the Name of the group by clicking the group number in column 1.

After the changes have been made, the web filter must be restarted.

Protector UTM – Ldap Guide

LDAP Authentication

Webfilter users can be authenticated against an external LDAP database. To do so fill out the fields below. Leave the fields blank if you wish to use IP based authentication. It is possible to use both at the same time. You need to point your browser to the protector IP address (192.168.0.250) and port 8080.

In Internet Explorer this is done by clicking Tools -> Internet Options -> Connections -> LAN settings. Activate "Use a proxy server for your LAN". Type in the Address 192.168.0.250 and 8080 in the Port field. Click OK and OK.

A typical setup (openldap) would have the value "uid=" as search filter and the baseDN "dc=your_domain,dc=com". For Active directory setup use sAMAccountName= as search filter. You can use the fields LDAP mail to test, LDAP password and Show Query output to test your setup. Depending on your setup you may need to specify a LDAP user/password to run the search query as.

This feature also provides integration with the [Group policies](#) setup. Members can be fetched from the LDAP source by renaming the policy name to match the LDAP group. You can change the Name of the group by clicking the group number in column 1.

After the changes have been made, the web filter must be restarted.

During this restart period, the protector will be offline for 30-90 seconds.

Enable LDAP:	<input type="button" value="No"/>
LDAP Server:	<input type="text" value="192.168.0.10"/>
LDAP Port:	<input type="text" value="389"/>
LDAP BaseDN:	<input type="text" value="CN=Protector,OU=SBS"/>
LDAP Search filter:	<input "="" type="text" value="sAMAccountName="/>
LDAP user to run query as:	<input type="text"/>
LDAP user password:	<input type="text"/>
LDAP user to test:	<input type="text"/>
LDAP password:	<input type="text"/>
Show Query output:	<input type="checkbox"/>

Questions and Answers:

I have an LDAP Server

LDAP Server: 192.168.1.83

port 389

BaseDN o=shoek

Search filter uniqueID= (Novell uid)

user to run admin or cn=admin

user to test admin

found DN: cn=admin,o=shoek

When we test user to test administrator (also in o=shoek test user not ok)

Answer: You must have cn=* in search filter, and in admin to run, and user to test.

Question:

I can only get it to work if the user admin use the web filter all other users it do not work.

Answer: The members in the groups should be in the policies.