



Integrating Novell eDirectory 8.7 With Check Point VPN-1/FireWall-1 NG

Author: **Oren Green**
Check Point Software Ltd.
Last updated: **June 1, 2003**

Trademarks	2
Document Focus	2
Known issues and limitations	2
Overview.....	3
VPN-1/FireWall-1 NG SmartDashboard.....	3
Check Point – LDAP Components	3
Verifying Correct Software Components	4
Options for LDAP integration	4
Extending the eDirectory schema to support FireWall-1 schema	5
Managing Users	6
Typical Configuration Depiction	6
Novell eDirectory 8.7 Installation/Configuration.....	7
SmartDashboard Installation/Configuration.....	7
Configuring FireWall-1 for use with LDAP.....	7
Creating Templates	12
Creating Users.....	13
Creating an OrganizationalUnit	13
Creating a Group.....	13
Defining security policy rules for LDAP authentication	14
Technical Support	14

Trademarks

Novell®, or eDirectory™ are trademarks or registered trademarks of Novell Inc. Check Point™, OPSEC™, and VPN-1/FireWall-1 NG® are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Document Focus

This document provides the information needed to configure Check Point VPN-1/FireWall-1 to work with Novell eDirectory 8.7. This document is intended to enhance the information provided by both Check Point and Novell not in any way replaces it. Basic knowledge of the Check Point and Novell architecture is a prerequisite.

Please refer to Check Point's documentation, *Administration Guide, Check Point SmartDashboard Client; Check Point SmartDashboard Client, How to install and Configure SecureClient and SecureServer*, for installation and configuration information for using VPN-1/FireWall-1 with LDAP.

Please refer to Novell's documentation that can be found at

<http://www.novell.com/documentation/lg/edir87/index.html?page=/documentation/lg/edir87/edir87/data/a4wyf4a.html>

Known issues and limitations

1. Limiting access to the eDirectory server by IP Address is not supported.
2. Enumeration of the LDAP tree structure (fetch branches from the LDAP Account Unit in SmartDashboard) doesn't work. Please add the branches manually.
3. SSL Authentication works with the following settings only: Using SmartDashboard, under the Encryption tab of the LDAP Server Properties check "Strong" for Min. and "Strong" for Max.
4. eDirectory enforces the use of SSL by default. If you want to change, turn off SSL and use port 389, open ConsoleOne and edit the LDAP Group. Under the General tab uncheck "Require TLS for simple binds with password". In case you decide to work with SSL you will need to check this option again.
5. If you decided to create a DC as your root you will need to edit the file \$FWDIR/conf/objects_5_0.C in the following way:
 1. Issue 'cpstop' and close all GUI clients.

2. Backup the objects_5_0.C file !
3. Edit the objects_5_0.C file under the Novell_DS 'read' section add :Domain right beneath :BranchObjectClass.

Example (after editing):

```
:Read (
    :AdminInfo (
        :chkpf_uid (" {97AEB649-9AEA-11D5-BD16-0090272CCB30} ")
        :ClassName (LDAP_policy_read)
    )
    :BranchObjectClass (
        : (Organization)
        : (OrganizationalUnit)
        : (Domain)
```

4. Issue 'cpstart' and install the policy.

This way you'll be able to add and change objects under the DC root using Smart Dashboard.

Overview

VPN-1/FireWall-1 NG SmartDashboard

The VPN-1/FireWall-1 SmartDashboard enables the Security Manager to integrate VPN-1/FireWall-1 with LDAP Servers, allowing user data to be shared between VPN-1/FireWall-1 and other applications. The LDAP Server and VPN-1/FireWall-1 module can reside on different hosts and be maintained by different people. Separating the functionality of the two systems provides the following benefits:

The system administrator can use existing LDAP-compliant databases without the need to import user data into VPN-1/FireWall-1. Several departments or customers, each of who can manage its own users independently using a separate management client, can use a single VPN-1/FireWall-1 system. Users can maintain and change their own passwords.

There is no limit to the number of users that can be defined. An additional feature is the live template. In the VPN-1/FireWall-1 user management model, changes made to a user template do not affect users previously defined using that template. In contrast, in the VPN-1/FireWall-1 SmartDashboard, changes made to a live template immediately apply to all users linked to the template. Users wishing to continue using the proprietary VPN-1/FireWall-1 user database may do so. Groups defined in both systems can be freely mixed in the firewall rule base.

Check Point – LDAP Components

The Check Point - eDirectory system consists of four components:

1. VPN-1/FireWall-1 Management Module
2. VPN-1/FireWall-1 Module
3. Check Point SmartDashboard GUI Client
4. LDAP Server (version 2.0 or higher compliant server)

The LDAP server must be accessible to both the SmartDashboard Client and to the VPN-1/FireWall-1 Module, that is, both when users are defined and when it is enforced.

Verifying Correct Software Components

Novell's eDirectory supports standard mechanisms for managing schema. Earlier versions of Novell eDirectory have different configurations for LDAP. Integration of versions of eDirectory prior to 8.7 are outside the scope of this document.

To verify that your eDirectory supports LDAP schema management, use the ldapsearch tool to verify where it stores the schema. Ldapsearch can be found in the directory \$FWDIR/bin in NG. In FireWall-1, ldapsearch can be done via the command "\$FWDIR/bin/fw ldapsearch". To verify the schema, use the following command:

```
ldapsearch -h <eDirectory Hostname or IP> -b "cn=schema" -s base "objectclass=*" 
```

If this command succeeds, you should see a long list of the directory server's attributes and object classes. If you get an error, such as "ldapsearch: No such object", you may need to upgrade your directory server to the latest eDirectory version.

Check Point's VPN-1/FireWall-1 versions 4.0 SP4 and greater have supported LDAP based user management. To take advantage of all user management features and performance enhancements, it is recommended that you use the latest version of VPN-1/FireWall-1.

Options for LDAP integration

Most directory servers control the types of attributes that can be defined for users. In order to define Check Point attributes, such as encryption types, authentication methods, and expiration dates, the process for extending the directory server's schema must be extended to incorporate the Check Point specific attributes used by VPN-1/FireWall-1. If users need to be assigned Check Point attributes, the schema needs to be modified if all users groups have identical configurations.

Default Templates:

In many organizations, the configuration for large groups of users is identical. The users all have the same type of authentication, encryption types, time limits, etc. In this case, it is not necessary to define those attributes for each user. By defining a default template in the account unit configuration, FireWall-1/VPN-1 will take the configuration values from the template if they are not defined in the user record. This is also very useful in situations where there is an existing group of users that do not have Check Point

attributes already defined. The template can allow use of these users without the need for modifying all the existing records.

Extending the eDirectory schema to support FireWall-1 schema

An LDAP schema is a description of the structure of the data in an LDAP directory. Each of the Check Point proprietary object classes and attributes (all of which begin with “fw1”) have a proprietary Object Identifier (OID). The two Check Point objectclass OIDs are:

fw1template 1.3.114.7.3.2.0.1

fw1person 1.3.114.7.3.2.0.2

The OIDs for the proprietary attributes begin with the same prefix (“1.3.114.7.4.2.0.X”). In order to properly define Check Point attributes on eDirectory users, the definition for the fw1person must be modified slightly.

In the standard schema.ldif file, the fw1person objectclass is defined like this:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.114.7.3.2.0.2 NAME 'fw1person' SUP 'top' MUST ( cn $ sn ) MAY ( description $
userpassword
```

To work with eDirectory, add “AUXILIARY” to the objectclass definition, as seen below:

```
dn: cn=schema
changetype: modify
add: objectclasses
objectclasses: ( 1.3.114.7.3.2.0.2 NAME 'fw1person' SUP 'top' AUXILIARY MUST ( cn $ sn ) MAY (
description
```

The attributes that Check Point products use are defined in a standard LDIF format file. This file can be found at \$FWDIR/lib/ldap/schema.ldif. This file can be used as with the ldapmodify utility to configure a directory server to allow Check Point user data. Ldapmodify is included with most directory servers, and can be found in the \$FWDIR/bin/ directory in NG. Once the schema extensions are done, the eDirectory schema can be extended. The syntax for extending the schema is:

```
ldapmodify -c -h <eDirectory IP Address> -D “<Admin bind DN>” -w <password> -f schema.ldif
```

The “Admin bind DN” is the distinguished name of the eDirectory Administrator. For example: “cn=admin, o=checkpoint, c=US”. This administrator must have permissions which allow modification of the directory schema.

If successful, you should see a line saying “modifying entry cn=schema” for each attribute or objectclass that is added. If ldapmodify immediately returns with no message, or gives an error message, verify that the Administrator DN and password are correct.

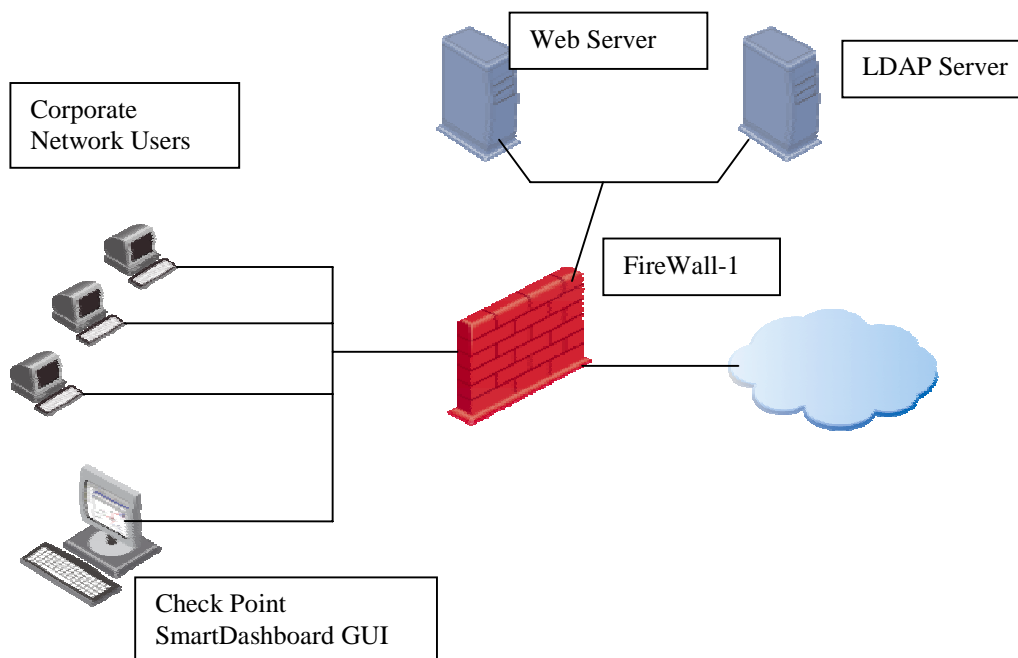
Managing Users

Once the schema is modified, you will be able to create new users from within the Smart Dashboard. These users can be configured with all Check Point settings. Users that were created prior to the schema extension, or are created with other tools, such as ConsoleOne, need to be modified to accept Check Point attributes.

To convert individual users, right click on the user object in ConsoleOne, and select “extensions of this object”. Select the “fw1person” objectclass from the menu list to allow the user to be configured with Check Point attributes.

For converting users in bulk, an automated mechanism is more efficient. One way to do this is to export the user database to an LDIF file, modify the user entries in the LDIF file to include the “fw1person” objectclass, and import the changes via the ldapmodify application.

Typical Configuration Depiction



User information can be maintained in an LDAP-Compliant directory to enforce the enterprise wide security policy.

Novell eDirectory 8.7 Installation/Configuration

Please refer to Novell's *Installing and Upgrading Novell eDirectory* guide at <http://www.novell.com/documentation/lg/edir87/index.html?page=/documentation/lg/edir87/edir87/data/a4wyf4a.html>

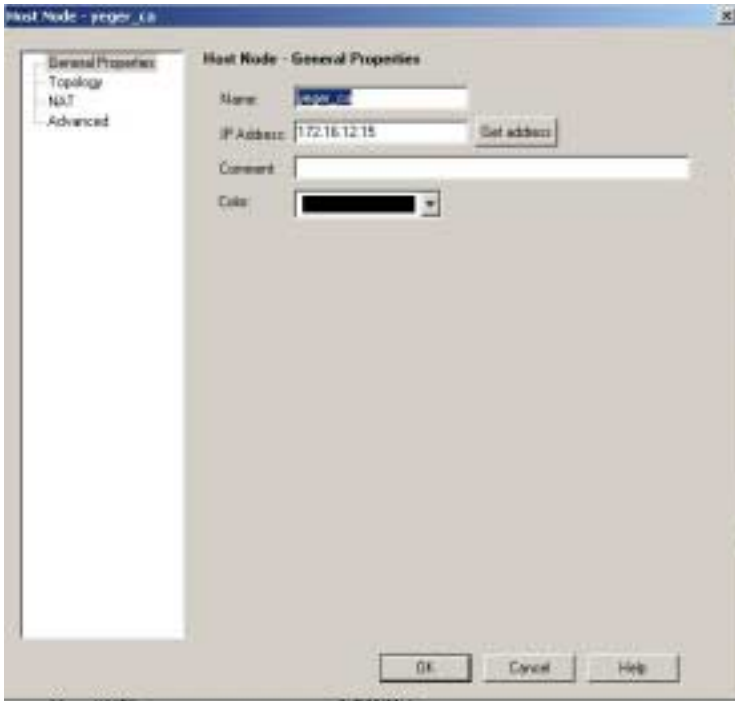
SmartDashboard Installation/Configuration

Configuring FireWall-1 for use with LDAP

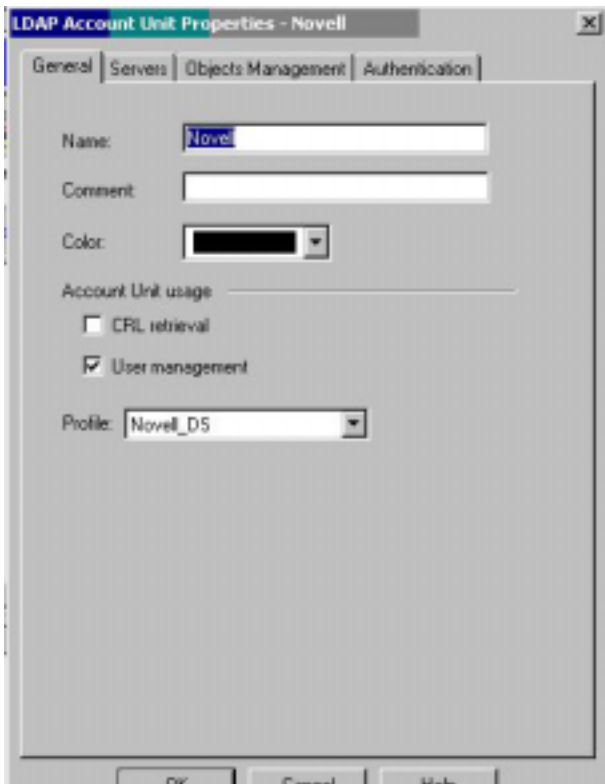
1. From the security policy editor, modify the *Policy->Global Properties* go to the *LDAP Account Management* tab and check the “*Use LDAP Account Management*” checkbox.



2. Create a network object for the LDAP server. *Manage->Network Objects... New->Node>Host* and fill out accordingly.



3. Create a server, *Manage->Servers...* and click on *New->LDAP Account Units*.



Server Object Properties

Name - Enter the Account Unit's name.

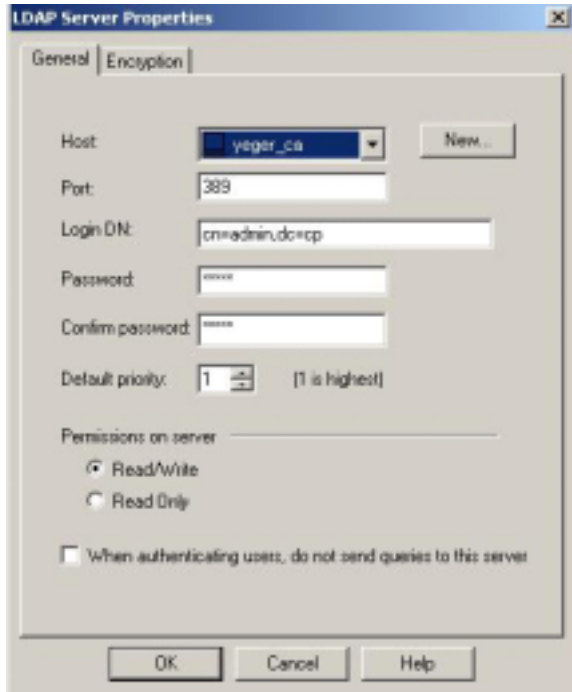
Comment - Descriptive text.

CRL Retrieval – This is used for CRL retrieval, that is, it is the CRL depository for OPSEC PKI enabled Certificate Authorities

User Management — Check this box. User Management is enabled only if Use LDAP Account Management is checked in the LDAP tab of the Properties window (Step 1)

LDAP Profile – Choose Novell_DS

Under the server tab click “Add”



The screenshot shows the 'LDAP Server Properties' dialog box with the 'General' tab selected. The 'Host' field is a dropdown menu showing 'yeager_ca' with a 'New...' button to its right. The 'Port' field contains '389'. The 'Login DN' field contains 'cn=admin,dc=cp'. The 'Password' and 'Confirm password' fields are masked with asterisks. The 'Default priority' is set to '1' with a note that '1 is highest'. Under 'Permissions on server', the 'Read/Write' radio button is selected, and the 'Read Only' radio button is unselected. There is also an unchecked checkbox for 'When authenticating users, do not send queries to this server'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.



Host - Select a server from the list, which was populated when defining network object.
(Step 2)

Port - default should be 389 for unencrypted sessions.

Login DN — The DN (**cn=Admin** is default unless) that will be used to bind (login) to the Account Unit LDAP server.

Password - The bind DN entry user password.

(Note: The Login DN and Password was obtained when installing Novell eDirectory)

Default priority — Leave as the default, further explanation can be found out of the *VPN-1/ FireWall-1 Administration Guide*.

Permissions on server — Check R and W to allow the firewall access privileges on the LDAP Server.

In case you want to use SLL go to the encryption tab and check “Use encryption (SSL)”

Encryption port – 636 (default)

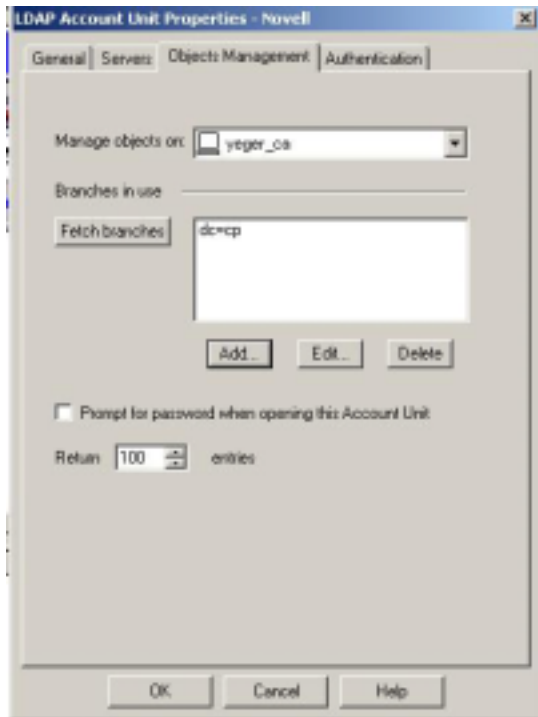
Click “Fetch” to retrieve the fingerprint form the LDAP server.

Min encryption strength – Strong

Max encryption strength - Strong



Go to the Object's Management tab



Manage objects on – select the LDAP host object

Branches — Manually enter the branches available on the LDAP (Fetch is currently not supported). For SSL, select the encryption tab and simply click on **Fetch** to retrieve the existing key. In this example, the User Preferences Tab keeps the default settings. Please

contact Check Point for more information regarding these settings. Please refer to the *VPN-1/FireWall-1 Administrator Guide*.

Note that by default the Smart Dashboard shows only 100 users per request. If you wish to see more or less than 100 LDAP user entries. Set the “Return X entries” To the number of entries you wish to view (X = number of entries)

4. Next, go to *Manage->Users and administrators...New->LDAP Group*.

The Account Unit list was obtained from Step 3. Check the appropriate radial button for Group’s Scope.



Creating Templates

1. Once logged into the LDAP Account Unit right click on the Account unit object and select *New > New template*

A template is an LDAP entry with the objectclass *fw1template*. All templates are live links, so if you modify templates, all users linked to the template will be affected.

2. Go to the **Authentication** tab and select Default Method. Other **Authentication schemes** are available, however for this example we will select Default Method. The Default Method is determined by the setting selected in User Preference tab in the Account Unit Properties.

3. Select the **Encryption** tab and the **IKE**, then modify the settings.

- a) **Enable IKE** (in this **example**)
- b) Set Authentication to **Use Password**
- c) Transform: **ESP**
- d) Data Encryption: **3DES**
- e) Data Integrity: **SHA1**
- f) Enable **Successful Authentication Track to log**
- g) Click **Save**

The Template should now show up in the LDAP branch you selected in step 1.

Creating Users

1. Right click on the Account unit object and select *New > New user* and link this entry to the new template you created.
2. Because most of the attributes for this entry have already been defined, click on the *Encryption* tab, *IKE* tab, and *Enter Password*.
3. Enter and confirm the new *Password* information, also enter the *Key* information.

Note Key for Encrypting Password: Enter the key to be used to encrypt users' IKE pre-shared secrets on the LDAP server. This field corresponds to the *IKE Key field in the Encryption tab* of the LDAP Account Unit Properties window in the FireWall-1 Windows GUI. It is the same for all users on an Account Unit (even though it is defined in a User Properties window). You define this only once. Once it is defined, it appears as the default value for all other users when you open their IKE Password windows.

Creating an OrganizationalUnit

1. To create an organizational unit, select the point in the tree under which the organizational unit should be created, and then right-click on it or select *File-> New OrganizationalUnit*. Enter the name of the new organizational unit, the default Branch is the selected tree object (if it exists on the LDAP Server), but you can select another one and click on *Add*. When you create an organizational unit in this way, the following objectclass organizationalUnit is added to the corresponding LDAP entry. Warning – “ou=” is implied. Do *not* type it. If you type it (for example, “ou=Accounting”), then the organizational unit’s name will include “ou=” (for example, “ou=ou=Accounting”).

Creating a Group

1. To create a Group, right click on the Account unit object and select *New>New Group*. Enter a name and the Branch.
 2. The group is now created, but you need to populate it with users, templates, and/or other groups.
- In this example, a template was added, which affects all users who are dynamically linked to that particular template.

Defining security policy rules for LDAP authentication

The screenshot displays the Check Point SmartDashboard interface. On the left, a tree view shows the 'Novell' domain structure, including 'Users and Administrators', 'Groups', 'LDAP Groups', and 'Novell_Test'. The main pane shows three security policy rules:

NO.	SOURCE	DESTINATION	F. VIA	SERVICE	ACTION	Log
1	yeager_ca sasha	sasha yeager_ca	* Any	* Any	accept	Log
2	novell_test@An	* Any	* Any	Authenticated	User Auth	Log
3	* Any	* Any	* Any	* Any	drop	Log

Below the rules, a table lists the Novell users:

Full Name	Login Name	DN (Distinguished Name)
as asaa	as	cn=as asaa,dc=
Adrian	Adrian	cn=Adrian,dc=
Auth_test		cn=Auth_test,dc=
Oran Green	ogreen	cn=Oran Green,dc=
shai	shai	cn=shai,dc=
Template		cn=Template,dc=
u2090	u2090	cn=u2090,dc=
u2091	u2091	cn=u2091,dc=
u2092	u2092	cn=u2092,dc=
u2093	u2093	cn=u2093,dc=
u2094	u2094	cn=u2094,dc=
u2095	u2095	cn=u2095,dc=
u2383	u2383	cn=u2383,dc=
u2384	u2384	cn=u2384,dc=
u2385	u2385	cn=u2385,dc=
u2386	u2386	cn=u2386,dc=

Technical Support

Novell 1-888-202-5799 or support@novell.com

Check Point 1-817-606-6600 or support@ts.checkpoint.com,