



[www.altman.co.uk](http://www.altman.co.uk)

# ***Password Policy Manager***

## ***for Novell Directory Services***

### **Start\_Up Guide**

**Copyright © 1999-2001 Connectotel Ltd**

Distributed by: -

**Altman & Associates**

Suite 5, 169 High Street, Boston Spa, West Yorkshire LS23 6BH, U.K.

Tel: 01937 541400

Fax: 01937 541500

From outside the UK: +44 1937 541400/541500

Email: [info@altman.co.uk](mailto:info@altman.co.uk)

Web: [www.altman.co.uk](http://www.altman.co.uk)

---

## Password Policy Manager (PPM) Start\_Up

Version 2.

Ref.4.6

For further information, or if you encounter any problems installing, please see the files "ppmadmin.doc" (MS Word format), and "Readme.txt" in the folder after unzipping. For additional information, please contact Altman & Associates ([support@altman.co.uk](mailto:support@altman.co.uk)).

Also, please see the file "a000802.pdf" (Adobe Acrobat format): a *Novell AppNote* on "Implementing Strong Passwords in an NDS Environment", written by PPM co-author, Marcus Williamson. Please read this entire document before starting the installation.

### 1. System Requirements:

PPM requires Novell's Client32 running on:

Win9.x (Client32 3.0.x or greater) or/and

WinNT (Client32 4.5x or greater) workstations.

The administration requires:

NW Admin 32 (Nwadmn32.exe, min. vn.5.0.5) or

ConsoleOne (ConsoleOne.exe, min. vn.1.2c).

### 2. Server Installation:

PPM installation is performed in four stages. When you run SETUP to install the PPM software on your server, it does not install any files on your desktop.

Firstly some schema extensions to the NDS tree are necessary. You will need to have Supervisor rights to the [Root] of the NDS tree before you can do this. Once this has been done the setup program will prompt you to install either the PPM NW Admin 32 snap-in or the PPM Client. If you select OK then another setup program will start that allows you to proceed with these installations.

Although PPM needs to be installed on a server - since it interfaces with the NDS using NW Admin 32 - the snapin is installed via a workstation. The PPM NW Admin 32 snap-in should be installed into the sys:\public\win32\snapins directory on the server from which you run NWADMN32.EXE. The install will copy two DLLs and a key, which are necessary for adding the new tabs for the Password Policy Manager.

PPM Client should be installed into a directory from where it can be distributed to the workstations that are to use PPM restrictions. The install will copy files for both Windows 95 and Windows NT Workstation. There should be two DLLs and two REG files. See below for instructions on how distribute these files to the workstations.

#### **a. Setup - PPM NDS Schema Extensions**

1. Ensure that NW Admin 32 is not currently running
2. Run **SETUP** on the Windows Workstation where you want to manage Novell NDS passwords.
3. Click the **Extend Schema** button, to install the PPM NDS schema extensions.
4. Confirm schema extensions loaded successfully.

#### **b. Setup - PPM NW Admin snap-in**

5. Click the **Install Snapin** button, to install the PPM NW Admin 32 snap-in.
6. Read the licence agreement screen, if you accept this click the **Yes** button.
7. Confirm default directory (note: this *must* be the "snapins" directory underneath the location of the "nwadmn32.exe" file), click the **Next** button.
8. Confirm successful install, click the **Finish** button.

#### **c. Setup - PPM Client**

Note: This section is only for testing, see **Client Installation**, below for live installs.

9. Click the **Install Client** button, to install the PPM client files.
10. Read the licence agreement screen, if you accept this click the **Yes** button.

#### **d. Setup - licence file**

11. The licence file (PPMSNAP.KEY) needs to be copied into the same directory into which the NWAdmin snapin was installed. This will normally be SYS:PUBLIC\WIN32\SNAPINS.
12. Click on the *Licence* button and choose this same directory. The licence file will be copied and the snapin enabled. The procedure is the same for both the demo licence and the full licence.  
Note: If you are using PPM from a downloaded PPM.ZIP and are upgrading from an evaluation version of PPM to a fully licensed version, then please place the newly-supplied PPMSNAP.KEY file in the LICENSE directory before installing the license file.
13. Confirm successful install, click the **Finish** button.

#### **e. Setup - Install completed**

14. Click the **Cancel** button, to close the Connectotel PPM setup program.

#### **Uninstall**

To uninstall PPM: run Start, Settings, Control Panel, Add/Remove Programs from a workstation where you installed PPM, ensuring you have the Sys: volume mapped to the same drive letter(s). Then scroll down to PPM & click **Remove**.

### **3. Client Installation:**

Note: the client install above only installs the client files on the Admin workstation for testing purposes.

For every workstation, you should (from the "Distribution" subdirectory of the unzip directory):

#### **[Windows 95/98]**

Copy ppmlgn95.dll to c:\windows\system.

Double click on the PPMSnap95.reg file in Windows Explorer or type:

```
regedit ppmsnap95.reg
```

#### **[Windows NT /2000]**

Copy ppmlgnnt.dll to c:\winnt\system32.

Double click on the PPMSnapnt.reg file in Windows Explorer or type:

```
regedit ppmsnapnt.reg
```

Both these stages may be automated using a ZENworks application object or other install automation software, which installs the DLL and makes the necessary registry changes.

### **4. Loading the software:**

Because the PPM administration software is a NW Admin 32 snapin, it loads automatically when the NetWare 32-bit Administrator is run. The PPM client runs automatically when workstation logins are forced to enter a new password.

## 5. Overview:

PPM has a snapin for the NetWare Administrator & ConsoleOne programs supplied with NetWare. It provides a new NDS object type (Password Policy) and a new detail view from the NDS Organisational Unit for associating a policy to a context.

### **Creating a Policy**

A number of parameters are available to create a secure yet cohesive Password Policy.

In particular, the use of a 7-length password with some punctuation & numeric - as well as the usual alphabetic - characters can create a password that would take ~2 months to crack by brute-force; whereas a password of 5-length using only alphabetic characters needs <1 minute!

Also, the "Percentage similarity with previous password" can be used to prevent users from changing a password to one that is almost identical. In this parameter, 0% similar is not similar at all; that is contains *none* of the characters in any order of the previous password.

Note: Order is not considered important, only how many characters appear from one password to the other. 100% is completely similar; that is the similarity is effectively not checked at all.

### **Demonstrating**

1. Run NW Admin 32 and create a new Password Policy object, then edit the new Password Policy object to comply with your required password policy.
2. Select an Organisational Unit containing a sample user .
3. Associate the Password Policy Object with that Organisational Unit. Select the required Organisational Unit, right-click, choose **Details**. Choose the detail view **Password Policy** and choose the required Password Policy by browsing the NDS for the one previously created.
4. Make sure the sample user has rights to see the Password Policy object and Password Policy attribute of the Organisational Unit.
5. Expire the sample user's password.
6. Login as the sample user.
7. Follow the prompts for changing the password.
8. Try with a password that does not match the password policy and one that does. Observe the differing results.

### **Year 2000 Compliance**

PPM is entirely Year 2000 compliant.

All trademarks contained in this document are the properties of their respective owners.