DeveloperNet University Publications

Implementing Strong Passwords in an NDS Environment

Marcus Williamson
Connectotel Ltd.
marcus@myrealbox.com
http://www.connectotel.com/

This AppNote describes ways in which network administrators can provide enhanced security in their network environments by making use of strong password solutions. It discusses the concepts behind strong passwords and looks at currently available options for implementing strong passwords within a Novell Directory Services (NDS) environment. In addition, it presents some available authentication solutions which do not make use of passwords, or which can be used to augment the use of password-based systems.

Contents:

Since this AppNote was written in the UK, it retains the British spelling used by the author.

Weak vs. Strong Passwords

As businesses look towards providing more customer-facing systems in the form of e-commerce and extranets, the use of solutions to provide enhanced security for both internal and external systems becomes ever more important.

The traditional username and password combination, which has for so long been part of computer security, is seen by some to be a weakness in the Internet-based world of e-commerce. Internal and external threats to an organisation's security mean that standard passwords—those that rely on the network user's own "password policy"—may not be suitable for use in some security-sensitive applications.

Without any external influence to enforce otherwise, the user's own mental "password policy" will generally prefer a shorter, more easily-remembered password to one which is more difficult to remember and therefore more difficult to "hack".

Short or easy-to-remember passwords are classified as "weak" passwords because they may be easily guessed by a human, or they can be determined programmatically by software written to generate password combinations. By contrast, a "strong" password can be defined as one which does not give itself readily to being guessed by a person, or hacked using a computer program.

Types of Password Attacks

Computer programs which are used to attempt to hack passwords are generally of two distinct types: dictionary attacks or brute force attacks. Hacking programs may incorporate both of these methods, such that they might use a brute force attack if the dictionary attack should fail.

Dictionary Attacks. This method of attack involves reading words from a "dictionary" or database of frequently-used terms. For example, these might include personal names, names of cities, and names of football teams. The rationale behind the dictionary attack is to attempt to exploit the user's weak internal mental "password policy", as described above.

According to an article published in *BusinessWeek* in June 1997, the most commonly used passwords are:

- The user's first name, last name, or child's name
- "Secret"
- Stress-related words (such as "Deadline" or "Work")
- Sports teams or terms (such as "Bulls" or "Golfer")
- "Payday"
- "Bonkers"
- The current season

- The user's ethnic group
- Repeated characters (such as "AAAAA" or "BBBBB")
- Obscenities or sexual terms

The main point to be made here is that users should avoid these types of passwords. (You can read the full text of this article on the World Wide Web at *http://www.businessweek.com/1997/06/b351314.htm*.)

Brute Force Attacks. This method of discovering passwords involves using software which can generate character combinations in sequence. Thus, to guess a three-character password where only 26 alphabetical characters (A - Z) are allowed, would involve testing all letter combinations between AAA and ZZZ—a total of 17,576 combinations.

Longer Is Stronger

The strength of a password is proportional to its length. To show how trivial it is to "hack" a three-character password, here is a simple BASIC program that will generate a file containing all 17,576 combinations of a three-character password using the letters A to Z.

```
'
' PASSGEN.BAS
' Password generator for
' three-character passwords
'
' Marcus Williamson
' 15 June 2000
'
' After this program has run, the file
' PASSGEN.DAT will contain all the
' possible three-character combinations
'
START% = ASC("A")
FINISH% = ASC("Z")
'
OPEN "O", 1, "PASSGEN.DAT"
'
FOR I% = START% TO FINISH%
      FOR J% = START% TO FINISH%
         FOR K% = START% TO FINISH%
            P$ = CHR$(I%) + CHR$(J%) + CHR$(K%)
            PRINT P$
            PRINT #1, P$
         NEXT
      NEXT
NEXT
'
CLOSE 1
'
END
```

Mathematically, as the length of the password increases, the number of possible character combinations (and therefore the password strength) increases exponentially, as shown in the table below. Password strength is increased due to the longer time required to generate all possible combinations for a given number of characters.

Number of Characters in Password	Possible Combinations (Letters A-Z Only)	Possible Combinations (All Characters)
1	26	36
2	676	1,296
3	1,7576	46,656
4	456,976	1,679,616
5	1,1881,376	60,466,176
6	308,915,776	2,176,782,336
7	8,031,810,176	78,364,164,096
8	208,827,064,576	2,821,109,907,456
9	5,429,503,678,976	101,559,956,668,416
10	141,167,095,653,376	3,656,158,440,062,980

Enabling NetWare's Intruder Detection

In a Novell network environment, the effectiveness of dictionary and brute force password attacks can be significantly decreased by the use of the Intruder Detection mechanism provided by NetWare. Intruder Detection is typically enabled to lock out a user account after three incorrect login attempts. The mechanism will temporarily disable the account and prevent further login attempts for a period defined by the administrator.

Intruder Detection is switched off by default when NetWare is installed. Those desiring the extra measure of security Intruder Detection provides should enable this mechanism immediately after installation of any NetWare-based system.

Options for Enforcing Strong Passwords

Strong passwords can be enforced to some degree by using the standard Novell facilities provided, or improved by using add-on software from Novell or third parties to provide additional functionality. This section discusses options from both categories.

Standard Novell Password Restrictions

Novell NetWare provides rudimentary facilities for ensuring the strength of passwords being used. These facilities, known as "password restrictions," are described below. The screen for setting these restrictions in the NetWare Administrator (NWAdmin) utility is shown in Figure 1.

- *Minimum password length.* Determines the shortest password which can be used.
- *Require unique passwords.* Ensures that up to ten previously used passwords cannot be used again.

Additionally, the administrator can force periodic password changes, ensuring that users are not able to use a certain password for longer than a given time. Employing this feature, as well as limiting "grace" logins, will ensure further password security.

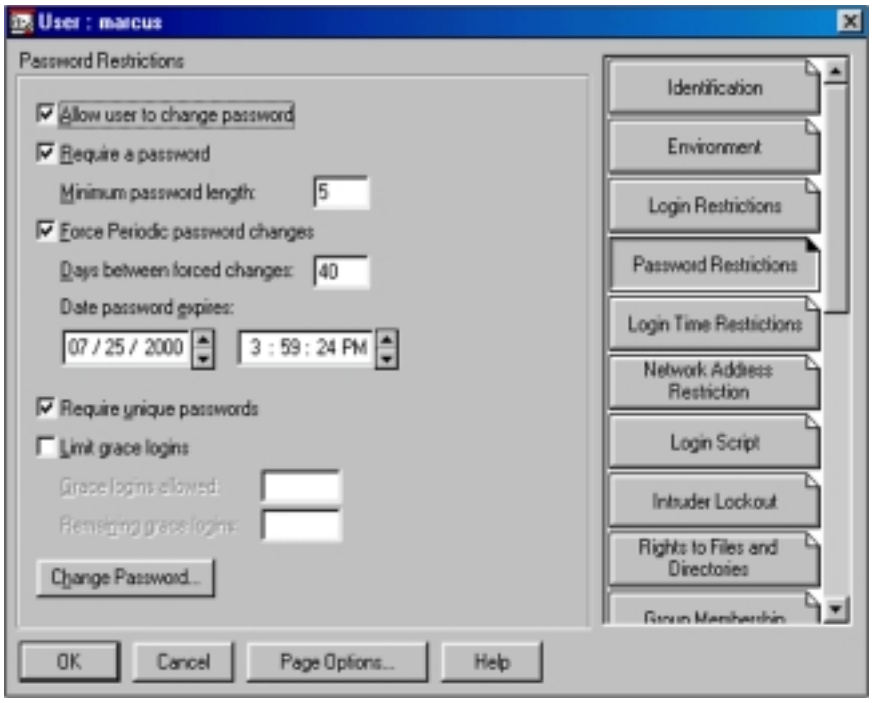


Figure 1: *NWAdmin screen for setting password restrictions for users.*

These standard Novell password restrictions allow the administrator to define only the minimum length of the password and whether passwords can be re-used.

Enhancement to Novell Password Restrictions

Since late 1999, Novell has provided an enhancement to the Novell Client software which allows enforcement of a password policy using locally stored data. In this case, the password policy is managed on each workstation and edited using a utility called LGNPWCFG (see Figure 2).

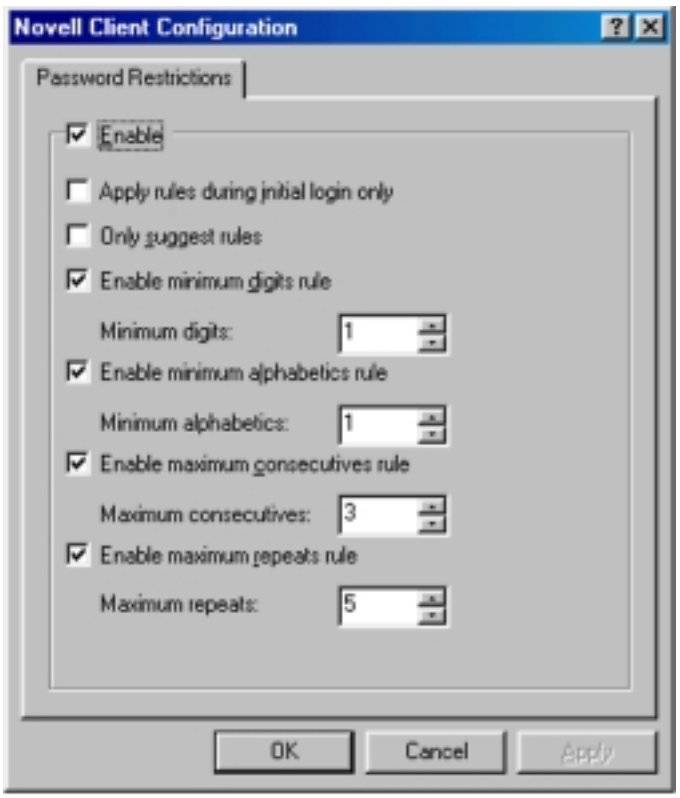


Figure 2: *Configuring additional password restrictions in LGNPWCFG.*

This utility can be downloaded from the ZENworks Cool Solutions site at *http://www.novell.com/coolsolutions/zenworks/tips/t_client_toolkit_zw.html*. The filename is LGNPW.ZIP.

LGNPWCFG writes the password policy to the local registry. The password policy registry entries and associated utility may be distributed using the Novell ZENworks for Desktops software. When the user logs in and a password change is necessary, a login snap-in module, called LGNPWW32.DLL, is invoked which checks the password against the defined password restrictions. If the password is found to be different from the policy settings, a message is displayed and the user is requested to change the password to one which matches the policy.

While this utility does have its benefits, it is not an ideal solution. Because the password policy is stored locally on each workstation, it cannot be easily seen and managed centrally using NDS. Furthermore, if a user were able to gain access to the LGNPWCFG utility, he/she would be able to change the password policy for that workstation. For administrators, this represents an unacceptable security risk.

Connectotel Password Policy Manager

Connectotel Password Policy Manager (PPM) has been available since Q4 1999. Its purpose is to provide a manageable, NDS-integrated solution to the issue of managing password policies.

The PPM software is implemented as an NWAdmin snap-in for administration of password policies, as well as a client-side login snap-in, called PPMLG95.DLL (Windows 95/98) or PPMLGNT.DLL (Windows NT/2000), which enforces the password policy. The login snap-in module may be distributed by using the Novell ZENworks for Desktops software or by using a batch file running from the login script.

Installation of PPM into NDS creates a new object type, the Password Policy object, which can be seen in Figure 3.

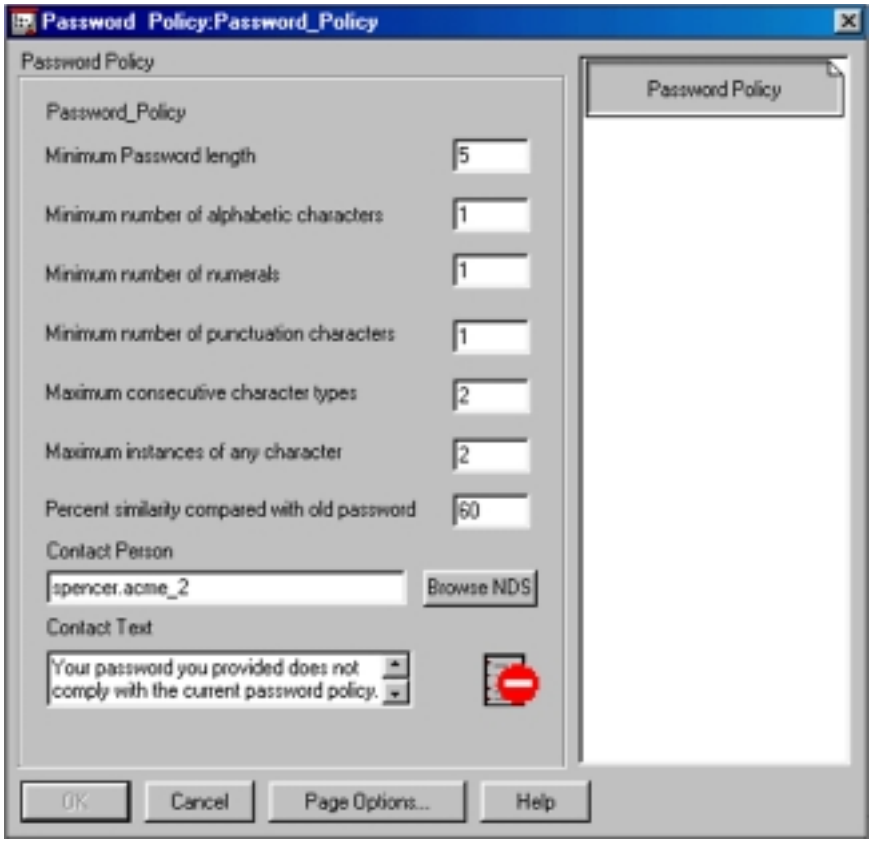


Figure 3: *The PPM Password Policy object.*

Attributes of the NDS Password Policy object include:

- *Minimum password length.* The minimum acceptable length for a valid password.
- *Minimum number of alphabetic characters.* The minimum number of alphabetic characters (A - Z) which may be present in a valid password.
- *Minimum number of numerals.* The minimum number of numeric characters (0 - 9) which may be present in a valid password.

- *Minimum number of punctuation characters.* The minimum number of "punctuation" characters (any non-numeric or non-alphabetical character) which may be present in a valid password.
- *Maximum consecutive character types.* Maximum number of alphabetic, numeric or punctuation characters which may follow each other. For example, set to a value of 2, this setting would allow "AB12" but not "ABXY". If set to 1, every character would have to be of a different type than the preceding character. Thus, "A1*B8!" would be allowed, but "AA*!34" would not be allowed.
- *Maximum instances of any character.* Maximum number of times that any character may appear in the password. For example, set to a value of 2, this setting would allow "AABCDE" but disallow "AAABCDE".
- *Percent similarity compared with old password.* A number between 0 and 100 which represents how similar the newly-chosen password is to the previous password being used.
- *Contact person.* An NDS object name for an administration user. If this field is filled in, this user's contact details will be provided in the message to the user relating to the password policy.
- *Contact text.* The message displayed to the user indicating that the password does not comply with the defined password policy.

Once the password policy has been created within a container in the NDS tree, it is associated with the container which holds the users for which the password policy should be enforced (see Figure 4).

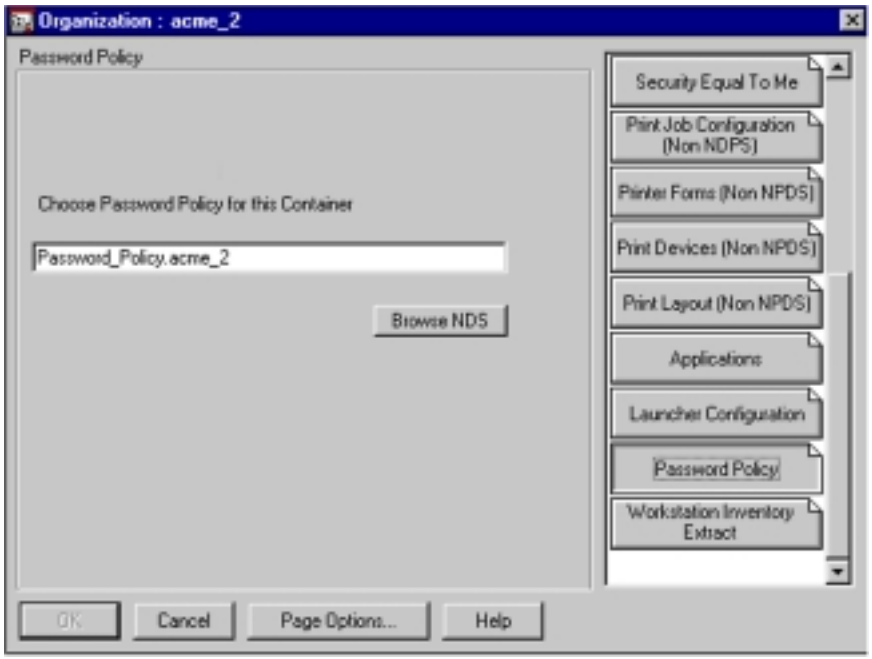


Figure 4: *Associating the Password Policy with a container.*

Using this combination of a Password Policy object and a password policy attribute at the container level, you may define multiple password policies for different parts of an organisation, if required.

When the user logs in and a password change is necessary, the user sees the prompt shown in Figure 5.

Figure 5: *PPM's password change prompt.*

Once a new password is entered, it is checked against the relevant Password Policy object in NDS. This is found by examining the Password Policy attribute of the user's parent container. If a password policy cannot be found, the next level upwards in the NDS tree will be examined, until eventually, in the absence of any other policy, the password policy of the Organisation object will be used.

Upon finding the relevant Password Policy, the PPM client software checks the user's newly-entered password against the Password Policy. If the password complies with the Password Policy, the login is allowed to continue. If it does not comply, the login attempt is halted and the message shown in Figure 6 is displayed.

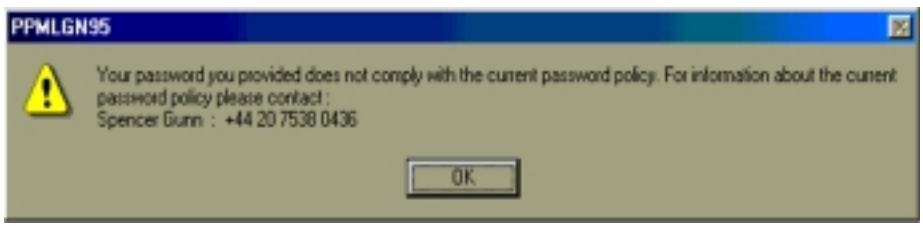


Figure 6: *Message displayed if a non-compliant password is entered.*

The user must then enter an alternative password. This cycle continues until a suitable password has been chosen.

For further information on the PPM software, see the Connectotel Web site at *http://www.connectotel.com/ppm*

Other Password Security Issues

Of course, even the strongest password policy could be easily compromised if users or administrators abuse the passwords by making them available to each other verbally, or by writing passwords on "Post It" notes attached to computer monitors.

It is therefore essential that the issue of password security be incorporated into "acceptable use" policy for the organisation's network. This acceptable use policy may be part of an employee's employment contract or may be a distinct document requiring separate signature. That same document would typically describe other aspects of acceptable use, such as permitted uses of the organisation's computer systems and regulations governing Internet access.

Examples of guidelines which could be incorporated into a written password policy include the following:

- Users shall not know the passwords of other users.
- Network administrators shall not know the passwords of users.
- Users must inform the network administrator if it becomes known that a password is no longer confidential.
- Passwords shall not be written down in any form in which they might be visible to other users.
- Passwords must have a regular expiration period, beyond which they are no longer valid. (This requirement can be enforced by using the password expiration interval within NetWare.)

Thus, the written policy and technology-enforced policy will complement each other to further ensure the security of the passwords being used.

Alternative Strong Authentication Options

In some scenarios, the use of a password alone (even if it is a strong password) is not considered sufficient for protection of the data held on especially secure systems. It may therefore be necessary to consider other options which are available for authentication to networks. These options include biometric devices and security tokens.

Biometric Devices

Biometric devices use some unique human biological characteristic to authenticate the user to a computer system. Examples include the use of a fingerprint or the pattern of the iris within the eye.

Informer Systems. Informer Systems, which incorporates Mission Data, have developed a fingerprint-based authentication solution for NDS, known as SentriNet. SentriNet allows the user to log in to the network using just a fingerprint, instead of requiring a password. This solution won the Novell Developers Contest at BrainShare in 1998.

Further information about SentriNet and Informer Systems can be found at *http://www.informer.co.uk/product/product.htm*.

Security Tokens

Security tokens are devices which are assigned to a user and which provide security by using the concept of "something owned" (the token) in addition to "something known" (the password) to ensure that users really are who they say they are.

Tokens are available in a number of formats. The most common format, implemented by both ActivCard and RSA Security (formerly known as Security Dynamics), is a device which displays an apparently random number to the user. This number is used in conjunction with a username (and often also with a password) to provide an additional piece of information for authentication of the user. The combination of the username, password, and token assignment—together with the entry of the correct token number—proves the authenticity of the user.

ActivCard. Novell provides its own "red box" version of the ActivCard One token device, shown in Figure 7. The Novell ActivCard devices can be ordered from any Novell Authorised Reseller.

Figure 7: *ActivCard token device.*

ActivCard One tokens may be used in conjunction with the following services:

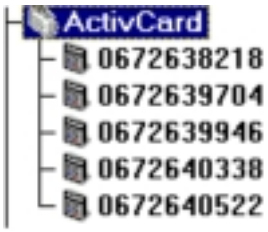
- *BorderManager VPN Client.* In this scenario, the user is prompted for a username, password, and ActivCard number when logging in to the network via a VPN connection.

- *BorderManager Proxy.* If BorderManager Proxy services has been enabled for use with ActivCard, the user must enter the ActivCard number before being granted access to the Proxy. This will allow access to the forward Proxy, for Web surfing outbound from an organisation, or to the reverse Proxy, for entry to an organisation's intranet, for example.
- *BorderManager Authentication Services.* BorderManager Authentication Services (BMAS) provides Novell's implementation of the RADIUS protocol for an NDS environment. Using BMAS, any RADIUS-compliant dial in device, or other RADIUS-compliant hardware or software, can authenticate users with an NDS account and an ActivCard device.

Note: For more information on the use of BorderManager Authentication Services with ActivCard tokens, refer to the AppNote entitled "Configuring BorderManager Authentication Services for Use with ActivCard Token" in the May 2000 issue of *Novell AppNotes*.

ActivCard devices are available in packs of 5 or 50, and are shipped with a diskette including the serial numbers of the devices contained in the pack. These device "images", as they are known, are imported into NWAdmin which results in the devices being created as NDS objects (see Figure 8).

Figure 8: *ActivCard device objects as seen in NWAdmin.*



Mobile Phone. Connectotel has developed technology (Patent Pending 9929291.4) which allows any standard mobile (cellular) phone to be used as a security token in any network environment. This solution takes advantage of the fact that the mobile phone is almost omnipresent in business in most parts of the world. It can now be used as a security device in its own right, without requiring an additional token card.

When you install the Mobile Phone Policy Manager product, the NDS schema is extended to include a Mobile Phone policy object, which can be configured for a particular user (see Figure 9).

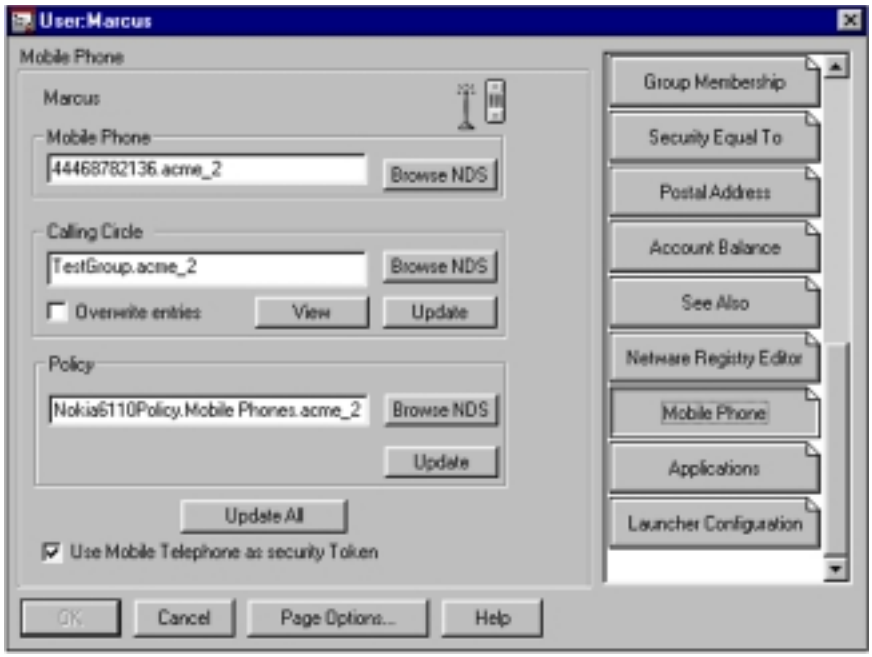


Figure 9: *Configuring the Mobile Phone policy object in NDS.*

When using this solution with NDS, the NDS user is presented with a standard Novell login prompt at which the NDS username and password are entered. A snap-in to the login process looks up the Mobile Phone object belonging to the user and, using the GSM Short Message Service (SMS), sends the user a message containing a random, unique four-character Personal Identification Number (PIN). The user then enters this PIN, as shown in Figure 10.

Figure 10: *Logging in to NDS using a mobile phone as a security token.*

The combination of username, password, the user's NDS relationship to the NDS Mobile Phone object, and successful entry of the PIN provides exceptional security for authentication, using both the concepts of "something known" and "something owned".

The same technique can be used to provide secure access to intranet and Internet Web sites, creating an inexpensive mechanism for providing token-based access to a Web site, using a security token which is already owned by many intranet and Internet users.

Novell Modular Authentication Services

Novell has recently announced a new infrastructure called Novell Modular Authentication Services (NMAS). The aim of this infrastructure is to allow third parties to develop enhanced authentication mechanisms, using a standardised interface. It is expected that, in time, all of the solutions outlined above will migrate to the NMAS environment.

For more information about NMAS, see *http://www.novell.com/products/nmas.*

Conclusion

As indicated in the introduction, weak passwords are often not a sufficiently secure solution for providing authentication to some networks. It is hoped that this AppNote has shown the options for strengthening the use of password-based security and how additional security measures can be used to supplement the login process, for networks requiring enhanced security.

If you have comments or suggestions for additional AppNotes on this subject, or related subjects, contact the author via e-mail at marcus@myrealbox.com.

Additional Resources

The following documentation may be helpful when considering solutions for providing strong authentication to NDS-based networks.

- "NetWare Security: Closing the Doors to Hackers" by Mark Foust, *Novell AppNotes*, June 2000

  http://developer.novell.com/research/appnotes/2000/a0006.htm

- "Configuring BorderManager Authentication Services for Use with ActivCard Tokens" by Marcus Williamson and Silvia Hagen, *Novell AppNotes*, May 2000

  http://developer.novell.com/research/appnotes/2000/a0005.htm

- AppNotes Special Issue on Security, *Novell AppNotes*, November/December 1997

  http://developer.novell.com/research/appnotes/1997/a9711.htm