



Purpose of this Document:

Windows' *Password not Required* control, which is analysed in SekChek for Windows / AD report section *Accounts not Requiring a Password* generates many questions from SekChek users. Also, the purpose of the control is often misunderstood.

The purpose of this document is to clarify the function of the control and provide a method for testing and confirming its behaviour.

Scope of the *Password not Required* Control:

The *Password not Required* control is set via the *PASSWD_NOTREQD* property flag in the *UserAccountControl* attribute for a User account.

Microsoft's documentation of the property flag is basic and unclear. However, various tests performed by SekChek confirm that the property flag *only applies to domain accounts defined in Active Directory*. I.e. it does not appear to have any affect on local accounts defined in the SAM database of workstations and member servers.

As is the case with several other security-related properties, the *Password not Required* control cannot be viewed or set via Windows' standard GUI. This means that it is necessary to use utilities such as *ADSIEdit*, or third-party software, to manipulate the control.

Security Implications:

Domain accounts with the *PASSWD_NOTREQD* property flag set have the potential to login to the domain without a password, regardless of domain-wide policies that enforce minimum password length and password complexity.

This situation can exist if: the *PASSWD_NOTREQD* property flag is enabled / set on; and an Administrator sets the User's password to Null (blank).

Note that even if the PASSWD_NOTREQD property flag is enabled, regular users cannot change their own passwords to Null, unless the Domain policy does not enforce a minimum password length. I.e. only an Administrator account can set a User's password to Null.

Test Schedule:

Microsoft provides no standard interface for displaying or modifying the *userAccountControl* attribute. You will need a tool like *ADSIEdit* (found in the Windows Support Tools) for performing these tests.

Warning: It is recommended that only advanced system administrators use this tool as incorrect changes can cause irreparable damage to the Active Directory structure.

Following is a guide on how to use the *ADSIEdit* tool to ascertain the value of the *userAccountControl* attribute on a Domain Controller running Windows 2003:

- Run the *ADSIEdit* snap-in (*Start -> Run -> adsiedit.msc*).
- Navigate within the domain tree to the container housing user accounts.
- Right-click on an account and select *Properties*.
- On the *Attributes* tab, view *Optional* properties.
- Now select the *userAccountControl* property, and note the decimal value listed. Refer to figure 1 for an example.
- You can change this value by entering the desired decimal value in the *Edit Attribute* field and clicking *Set -> OK*.

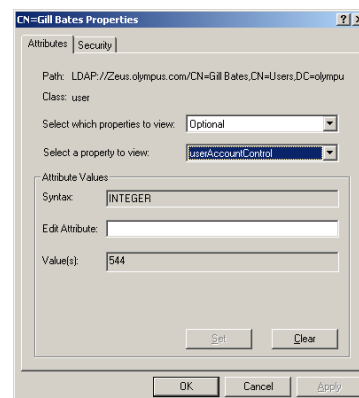


Figure 1 – View of the *userAccountControl* attribute via *ADSIEdit*



Figure 1 shows that the UserAccountControl attribute for account Gill Bates is set to a decimal value of 544 (hex 220). This value is the sum of the individual property flags for the UserAccountControl attribute of the User account.

A value of 544 (x220) indicates that the account has the following property flags set / enabled:

- NORMAL_ACCOUNT: decimal 512 (x200)
- PASSWD_NOTREQD: decimal 32 (x20)

Note that the PASSWD_NOTREQD property is represented by hex value x20, so any UserAccountControl attribute containing a value of x20 has the PASSWD_NOTREQD flag set. Some examples of values for the UserAccountControl attribute, where the PASSWD_NOTREQD flag is set are: x10220, x222, x22A and x800220.

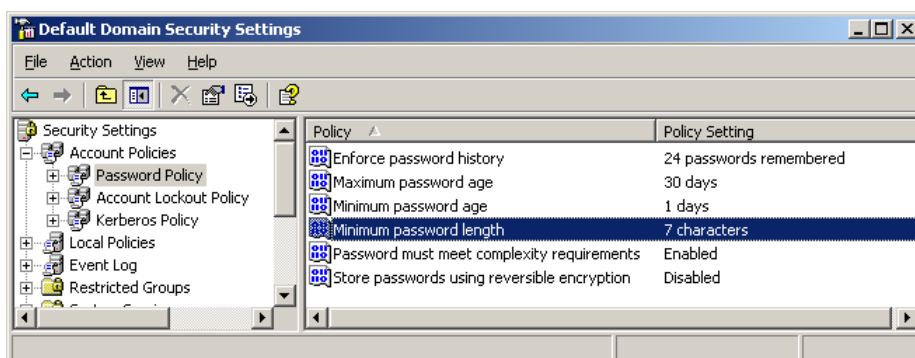


Figure 2 – The domain-level policy specifies a minimum password length of 7 characters

An account with the *PASSWD_NOTREQD* property flag set can have its password set to null. To do this, use the *Reset Password* function via the standard *Active Directory Users and Computers* interface.

Despite the domain-level policy, the account's password will be set to null. You can then logon to the domain using this account.



Figure 3 – The account has a null password set, despite the domain-level policy

Associated Risk:

Allowing the use of null passwords is a very high security risk. This is because any person in possession of the account name can easily gain access to your system and associated resources.

Additional Resources:

You can refer to Microsoft's Knowledge-Base article *KB305144 (How to use the UserAccountControl flags to manipulate user account properties)*, which defines a list of the component property flags with associated values that make up the *userAccountControl* attribute.

This paper was written by Sanjay Pather, an Operations Manager at SekChek Information Protection Services. Sanjay is responsible for the quality of SekChek reports and research and testing of security controls on the various platforms supported by SekChek.