10 Steps to a Secure FTP Server

www.windowsecurity.com/articles-tutorials/misc_network_security/Secure_FTP_Server.html

With his first article for WindowSecurity.com, we are pleased to welcome Ray Zadjmool (MCSE, CISSP, CCNA) to our team of authors. FTP [File Transfer Protocol] is one of the oldest and most popular services found on the on the internet today. Serving as an easy and effective method by which to transfer files over a network, FTP has become a standard that is both accepted and widely accessible to users across almost every network and operating system in use today. In this article we will examine 10 options available native in Windows 2000 that can be used to secure an FTP site.

FTP [File Transfer Protocol] is one of the oldest and most popular services found on the on the internet today. Serving as an easy and effective method by which to transfer files over a network, FTP has become a standard that is both accepted and widely accessible to users across almost every network and operating system in use today.

Windows 2000 comes with an FTP server as a part of IIS 5.0. Installed as a stand alone service, it is very rich in features. When combined with the other resources available inside Windows 2000 server, administrators are empowered with different options that can help make an FTP site more secure.

Having said that, we will examine 10 options available native in Windows 2000 that can be used to secure an FTP site. Some are pretty obvious but some are creative approaches that aren't readily thought of by administrators. In addition to the tips below, add-on services such as VPNs or SSH are things to consider since there is the pesky issue of sending passwords clear text over the wire.

TIP # 1: Disable Anonymous Access.

Anonymous access is enabled by default when you first install FTP services in Windows 2000. Anonymous Access is a method by which any user can gain access to your FTP site without the need of a user account.

There are some customer facing services that can be served effectively by Anonymous FTP sites, but the majority of the time allowing anonymous access will result in the eventual hijacking of your site by individuals wanting to host illegal files and copyrighted material.

By removing the capability for anonymous access, you are essentially limiting access to your FTP site to successful authentication by a predefined user account. Access controls are then configured by the use of ACLs [access control list] defined on the FTP home directory using NTFS permissions.

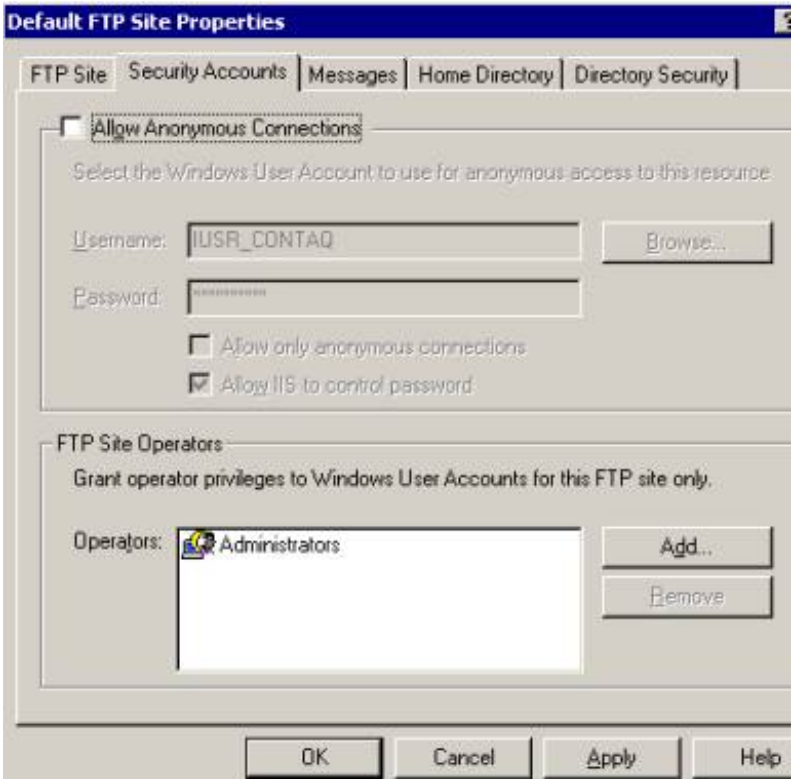
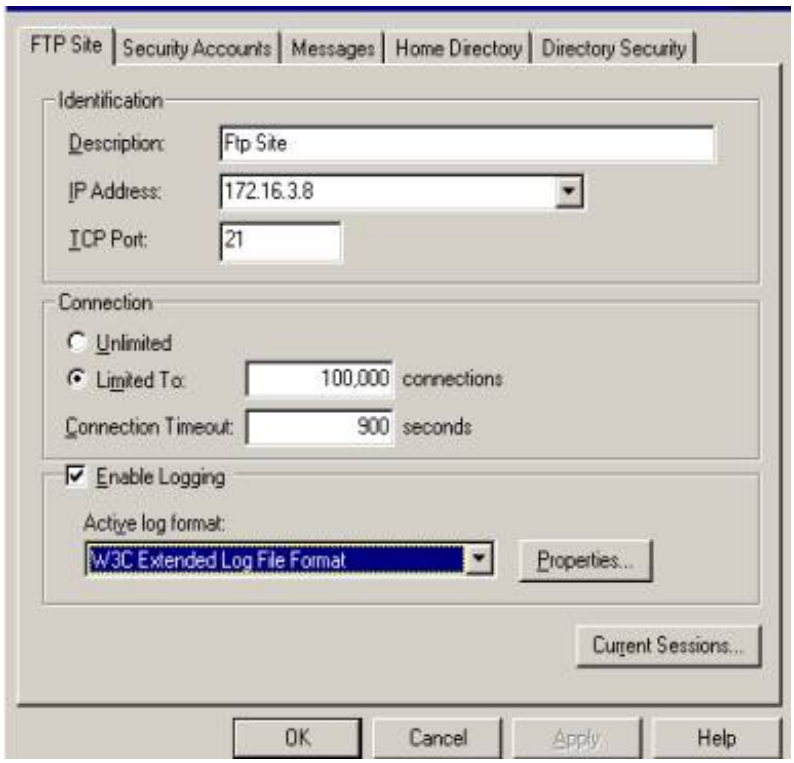


Figure 1: *To restrict the anonymous access to your FTP site, simply clear the Allow Anonymous Connections box in the security accounts tab of the ftp sites properties page*

TIP # 2: Enable Logging.

By enabling logging your FTP site, you can ensure that you will have an accurate record of which IP addresses and users accessed your site. Maintaining a practice of routine log review can enable you to assess your traffic patterns and identify any security threats and/or breaches.

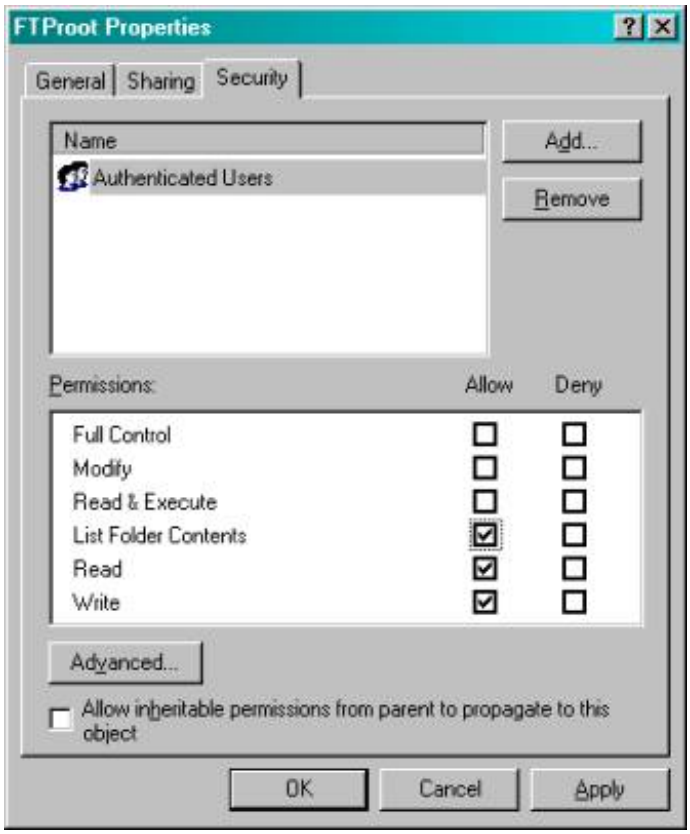


> ***Figure 2:*** *To enable logging of your FTP site, check the Enable Logging box in the FTP Site Tab found in the properties page of the FTP site. Log files are then created in a format of your choosing and can be reviewed later for analyzing traffic patterns and access controls.*

TIP # 3: Harden your ACLS.

Access to your FTP directory should be regulated utilizing ACL restrictions across NTFS permissions. This cannot be stressed enough. Your FTP directory should not have the everyone group with full rights as this will limit your ability to control the user groups that have access into your FTP site.

> ***Figure 3:*** *Typically you would want to restrict this group to Read, Write, and List only [no execute] but in the case of a blind put configuration (read below) you should also deny against Read and List and only have Write access on your directory.*



TIP # 4: Setup your FTP site as Blind Put.

If you only need your users to transfer files **to** your server and not transfer files **from** your server, consider configuring your FTP site as a “blind put”. What this means is that users are allowed to write files without the having the ability to read from your FTP directory. This will protect the contents of your ftp site in case of an unauthorized user getting access to your ftp directory.

Configuring Blind Puts should be done both at the FTP site and on the directory’s NTFS permissions.

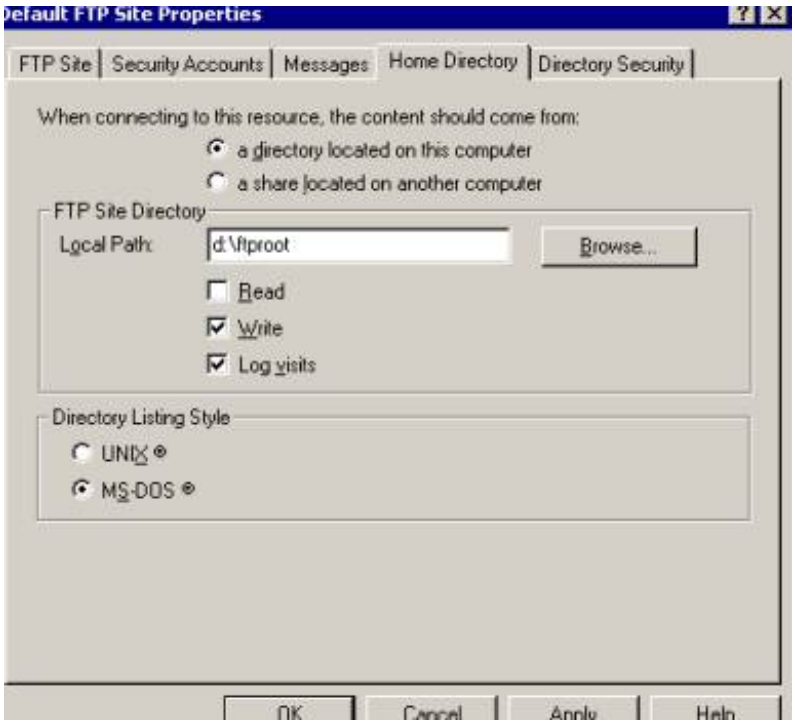


Figure 4: *shows you how to remove read access to your FTP site using the Home Directory Tab found in the properties page of the site.*

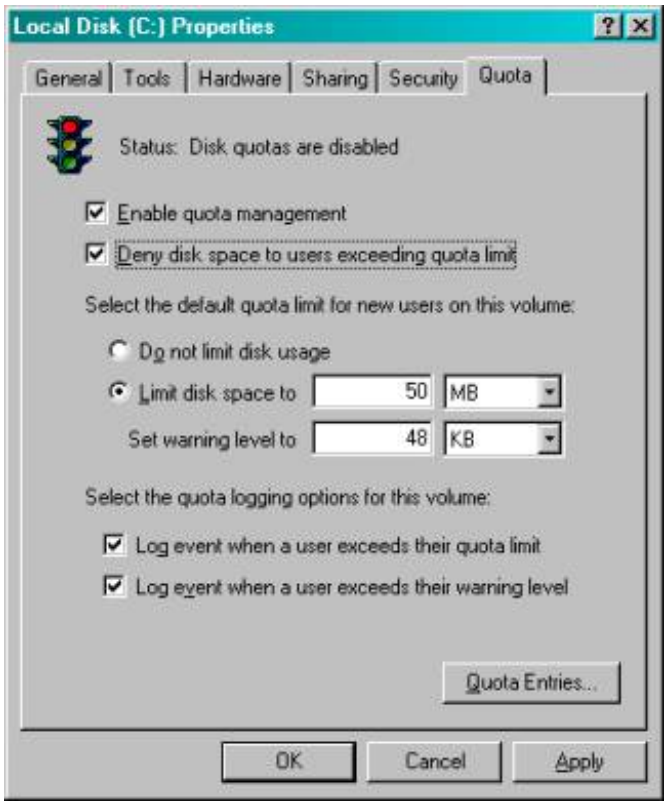
TIP # 5: Enable Disk Quotas.

Windows 2000 comes with a handy utility that allows for the enforcement of Disk Quotas. Disk Quotas can effectively limit the amount of disk space a user can have ownership of. By default, ownership is granted to whichever user wrote the file. By enabling disk quotas and checking the deny disk space to users exceeding disk quota, you can effectively limit the possible damage caused in case your FTP site gets hijacked. One worst scenario is the abuse of an FTP site to the point that the disk fills up. This of course can have disastrous consequences to other services that might share the partition with the FTP site.

Also, by limiting the amount of disk space each FTP user can have, your site becomes an unattractive target for hackers looking for someplace to share their media files.

Figure 5: *Enable Quota Management by Quota Tab found in the properties window of an NTFS disk partition.*

The use of Disk Quotas is limited to NTFS partitions. Furthermore, Quotas can only be placed on a per user basis and cannot be assigned to groups.



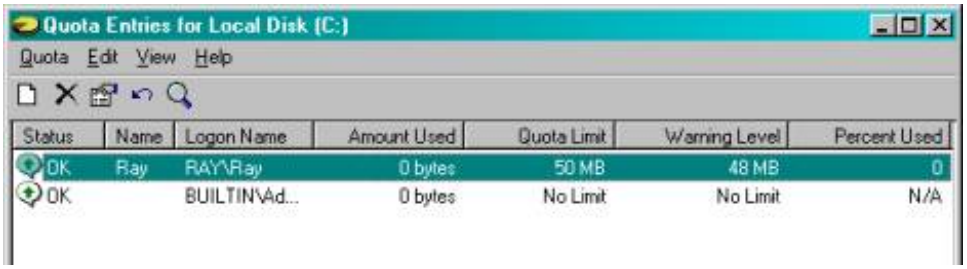


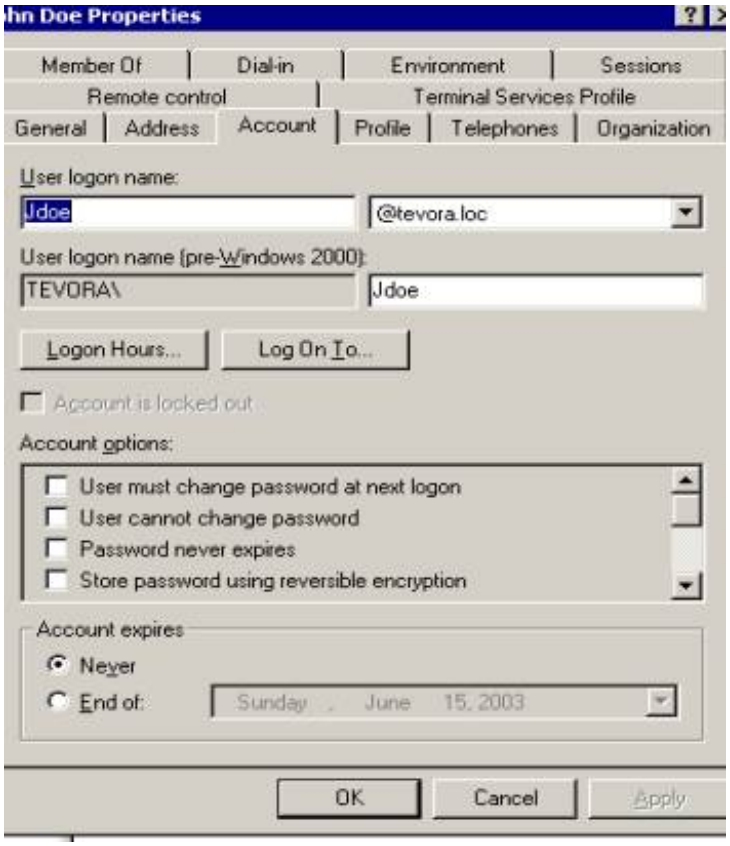
Figure 6: *Quote management can be configured on a per user basis. Limits should be set on the user accounts used for FTP access.*

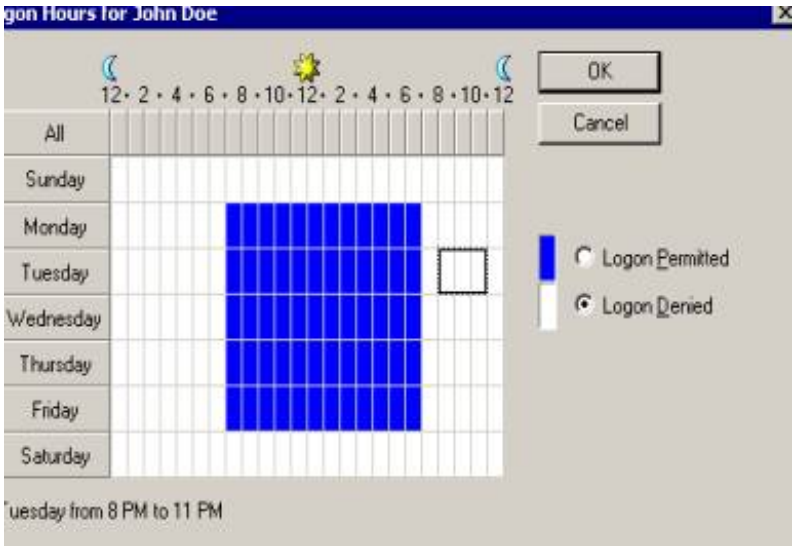
TIP # 6: Use Logon Time Restrictions.

Windows 2000 carries from NT 4.0 days the ability to logon hours of specific users. This option allows for a user to be limited to specific hours of the day in which he can logon.

This can be used creatively to limit access to your FTP site to only times that are authorized. If for instance you are using this Ftp site in an enterprise environment for business use, you could assess your availability needs to be limited to working hours. By denying logon during after hours, you would effectively shut down and secure your ftp site for most of the calendar day.

Figure 6: *The configuration of logon times in Windows 2000 can be found in Active Directory Users and Computers under the user property page.*





net user /times:

** Local User accounts cannot be configured for logon times through the Local Users and Groups console as this option is not available in the GUI.*

TIP # 7: Restrict Access by IP.

Windows 2000 FTP can be restricted to specific IP addresses. By limiting access to your FTP site to known entities, you can drastically reduce your exposure to unauthorized access.

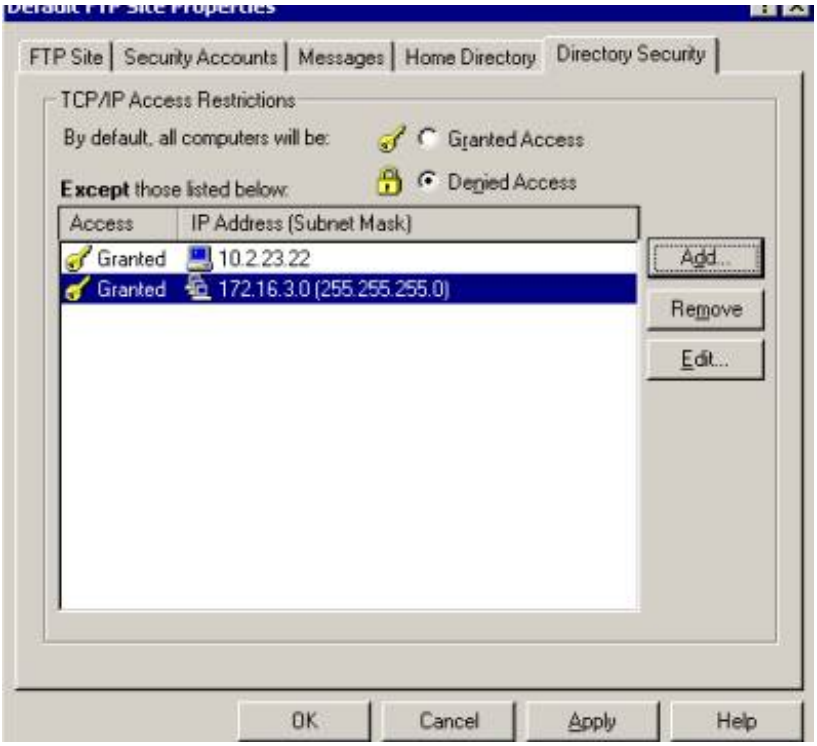


Figure 7: *To restrict FTP access via IP, use the Directory Security tab found in the properties pages of the FTP site. Make sure that the default Denied Access check box is selected and that only trusted IP Addresses are listed in the list box.*

TIP # 8: Audit Logon Events.

By enabling the Auditing of Account Logon Events, you can review success/fail attempts to your ftp site in the Security Log of the Event Viewer.

Frequent review of this log can alert you to suspicious activity that could be a malicious user trying to hack in. It can also be used as an effective method for intrusion detection by giving you a historical look into your FTP sites usage.

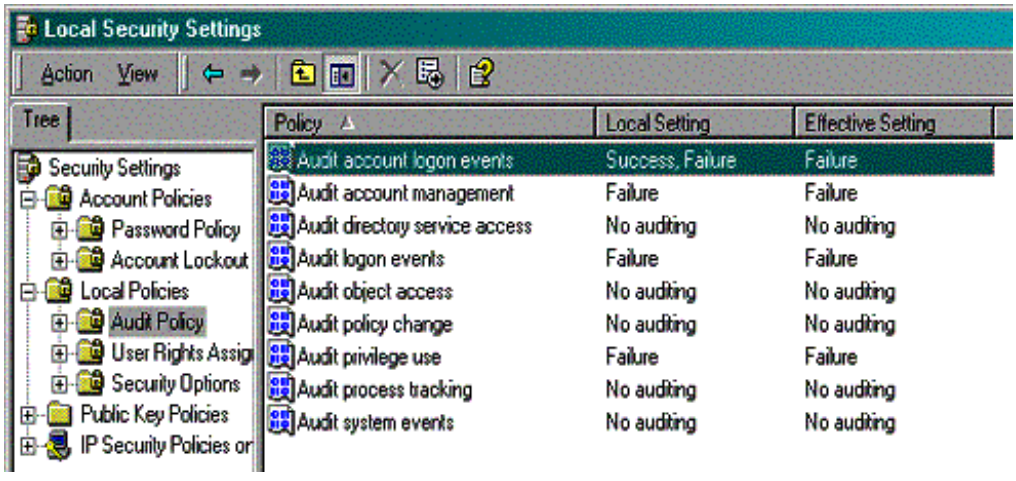


Figure 8: *Audit Account Logon Events can be turned on by using the Local Security Policy configuration tool. Navigate to the local policies/audit policy container and change the local setting to reflect Success, Failure.*

**Using Active Directory, Audit Account Logon Events can also be configured using Group Policies.*

TIP #9: Enable Strong Password Requirement.

Using complex passwords is a good security practice whenever you are dealing with end user authentication. In the case of FTP, it can be a crucial component in securing your site.

Windows 2000 allows for administrators to force users to comply with strong password requirements. By enabling the 'Passwords Must Meet Complexity Requirements' field in Local Security Policy or Group Policy, FTP user accounts will be forced to adhere to following restrictions when selecting their passwords:

- Must not contain all or part of the user's account name
- Must be at least 6 characters in length
- Contain characters from 3 of the following 4 categories:
    - English uppercase characters (A - Z)
    - English lowercase characters (a - z)
    - Base 10 digits (0 through 9)
    - Non-alphanumeric characters (e.g., !, $, #, %)

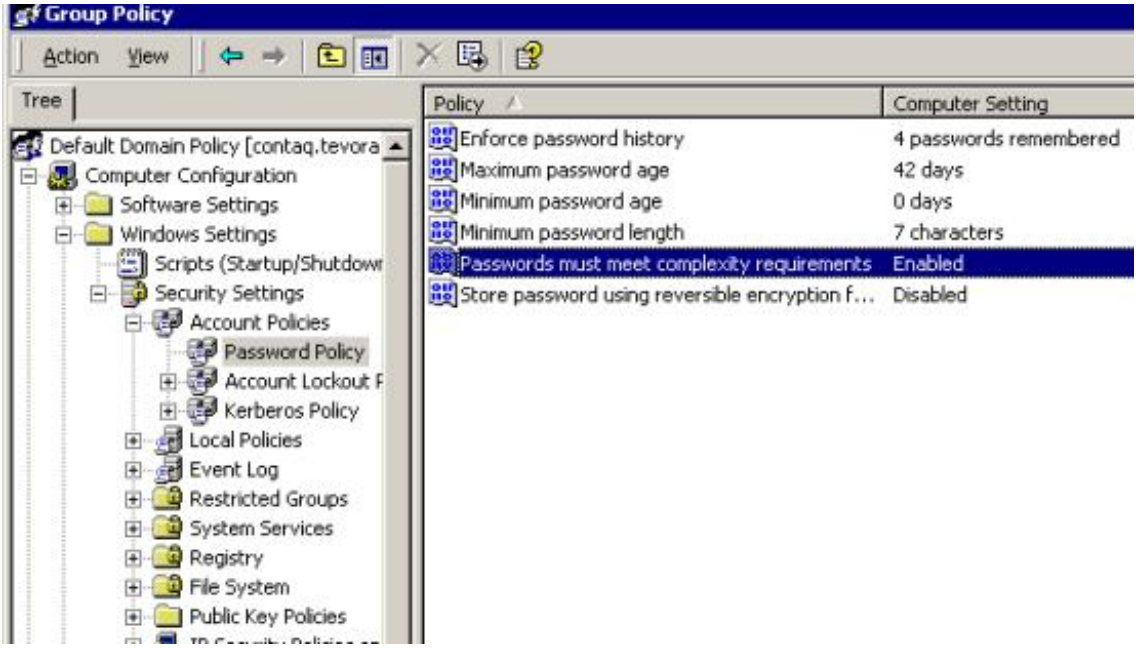


Figure 9: *Passwords must meet complexity Requirements can be enabled by using the Local Security Policy configuration tool. Navigate to the local policies/Account Policies/Password Policy container and change the setting to reflect Success, Failure.*

**Using Active Directory, 'passwords must meet complexity requirement' can also be configured using Group Policies*

TIP # 10: Enable Account Lockout and Account Lockout Threshold.

FTP accounts are pretty popular targets for password cracker programs that run through an exhaustive list of passwords in an attempt to guess, or crack account access. Windows 2000 security policies allow administrators to lock down the number of times failed logins can be attempted before an account is locked out. By enabling this option and configuring the threshold, administrators can limit their exposure to password crackers.

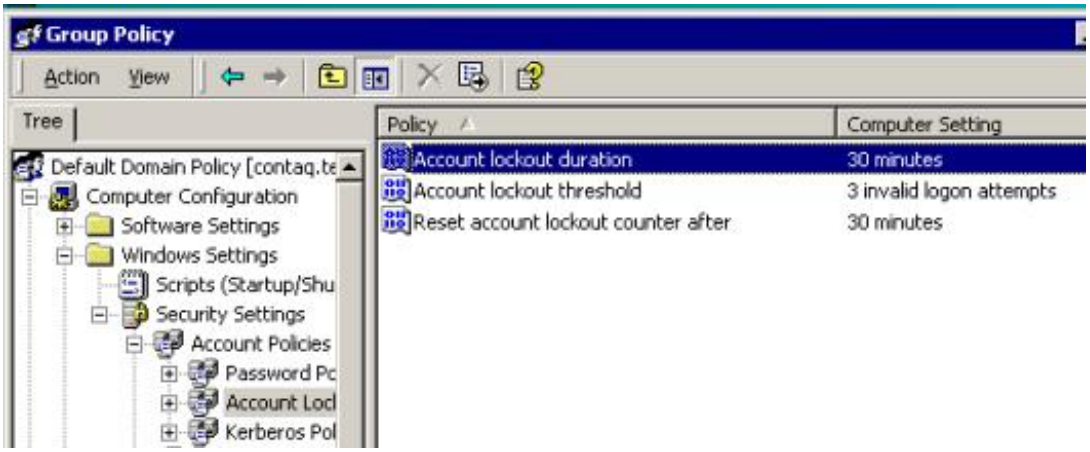


Figure 10: *Account Lockout Duration and Threshold options can be configured by using the Local Security Policy configuration tool. Navigate to the local policies/Account Policies/Password Policy container and change the setting to reflect Success, Failure.*

**Using Active Directory, 'Account Lockout Policies' can also be configured using Group Policies*