



## Windows Fine-Grained Password Policies

### ***What are Fine-Grained Password Policies?***

Fine-Grained Password Policies (FGPP) is a new feature introduced with the release of Windows Server 2008. FGPP enables administrators to create multiple password and account lockout policies within a domain. This capability allows different levels of security to be applied to specific users or groups.

### ***Why should you use Fine-Grained Password Policies?***

FGPP eliminates the need for additional domains or customized password filter DLLs to handle different password/account lockout domain policies.<sup>1</sup> Using FGPP, administrators can create unique password/account lockout policies for different requirements, such as a hardened FGPP for privileged users (such as administrators and help desk personnel) or enabling dissimilar requirements for different commands that are being joined under a single domain.

### ***What do you need to implement Fine-Grained Password Policies?***

- FGPP can only be used in a domain that has been set to a 2008 Functional Level Domain.
- FGPP can only be applied to individual users or groups. Domains designed with an OU structure will need to implement logical group representations of the OUs.
- FGPP requires at least the use of the Microsoft tools, ADSI Edit and the Active Directory Users and Computers console (ADUC). There are also third party tools and scripts available to assist administrators.

### ***Which users should have a restrictive FGPP?***

Any user or group that has privileged access should have a stronger password and account lockout policy. This would include all levels of system administrators, delegated users such as help desk personnel and application administrators, and computer operators. Microsoft's *Windows Server 2008 Security Guide* provides a list of privileged users that should have more restrictive policies.

### ***What settings are included in Fine-Grained Password Policies and how should I configure them?***

Table 1 lists the password and account lockout settings that are configurable using FGPP. In addition, Table 1 provides an example of how different settings can be configured for two different categories of users. This example is based on the Enterprise Client (EC) and Specialized Security-Limited Functionality (SSLF) security baselines located in Microsoft's

---

<sup>1</sup> FGPP does not provide the option of changing the default complexity rules set by Microsoft. However, FGPP will not interfere with custom created password filters that modify password complexity settings.



## Systems and Network Analysis Center Information Assurance Directorate



*Windows Server 2008 Security Guide*. This is only an example as configuration of these settings will be dependent on the needs of the individual enterprise.

**Table 1: FGPP Configurable password and account lockout settings with example configuration guidance**

FGPP Setting	General Users (Use EC Recommendations)	Privileged Users (Use SSLF Recommendations)
Enforce password history	24	24
Maximum password age	90	90
Minimum password age	1	1
Minimum password length	8	12
Passwords must meet complexity requirements	TRUE	TRUE
Store passwords using reversible encryption	FALSE	FALSE
Account lockout duration	15 minutes	15 minutes
Account lockout threshold	50 attempts	10 attempts
Reset account lockout after	15 minutes	15 minutes

Since multiple password and account lockout policies can be created, it is possible that more than one policy can be applied to a user. To resolve multiple policies, each password and account lockout policy must be given a unique administrator defined precedence value. The precedence value must be a positive number, with the lowest number given the highest rank.

### ***Where can I get more information on Fine-Grained Password Policies?***

Microsoft's Technet Library has a guide that provides detailed instructions for creating and applying FGPP. The *AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide* can be found at <http://technet.microsoft.com/en-us/library/cc770842.aspx>.

### ***Summary***

FGPP is a new capability available to help administrators enhance the security of their networks once they implement 2008 Functional Level Domains.

Microsoft, Windows, Windows Vista, and Windows Server are either registered trademarks or are trademarks of Microsoft Corporation in the U.S. and/or other countries. The Systems and Network Analysis Center Information Assurance Directorate, Windows Fine-Grained Password Policies fact sheet is an independent publication and is not affiliated with, nor has it been authorized, sponsored, or otherwise approved by Microsoft Corporation.