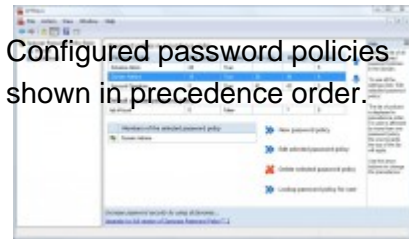


# Specops Password Policy™ Basic



**Introduction** Specops Password Policy Basic is used to configure fine-grained password policies in Windows Server 2008. Specops Password Policy Basic is a feature limited and **free** version of [Specops Password Policy](#).

Fine-grained password policies is a new feature in Windows Server 2008 that can be used to specify multiple password policies and apply different password restrictions and account lockout policies to different sets of users within a single domain. Password policies apply only to user objects (or inetOrgPerson objects if they are used instead of user objects) and global security groups. Fine-grained password policy cannot be applied to an organizational unit (OU) directly.

**Note!** To be able to use the fine-grained password policy feature, the ENTIRE domain must be running in Windows Server 2008 mode and all domain controllers must be Windows 2008 servers.

**What functionality does this feature provide?**



**Storing fine-grained password policies** A Password Settings object (PSO) has attributes for all the

settings that can be defined in the Default Domain Policy (except Kerberos settings). These settings include attributes for the following password settings:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Passwords must meet complexity requirements
- Store passwords using reversible encryption

These settings also include attributes for the following account lockout settings:

- Account lockout duration
- Account lockout threshold
- Reset account lockout after

In addition, a PSO has the following two new attributes:

- PSO link. This is a multivalued attribute that is linked to users and/or group objects.
- Precedence. This is an integer value that is used to resolve conflicts if multiple PSOs are applied to a user or group object.

## **RSOP**

A user or group object can have multiple PSOs linked to it, either because of membership in multiple groups that each have different PSOs applied to them or because multiple PSOs are applied to the object directly. However, only one PSO can be applied as the effective password policy. Only the settings from that PSO can affect the user or group. The settings from other PSOs that are linked to the user or group cannot be merged in any way.

The RSOP can only be calculated for a user object. The PSO can be applied to user object in either of the following two ways:

1. Directly, a PSO is linked to the user
2. Indirectly, a PSO is linked to group(s) that user is a member of

If multiple PSOs are linked to a user or group, the resultant PSO that is applied is determined as follows:

1. A PSO that is linked directly to the user object is the resultant PSO. If more than one PSO is linked directly to the user object, a warning message is logged in the event log and the PSO with the lowest precedence value is the resultant PSO.
2. If no PSO is linked to the user object, the global security group memberships of the user, and all PSOs that are applicable to the user based on those global group memberships, are compared. The PSO with the lowest precedence value is the resultant PSO.
3. If no PSO is obtained from conditions (1) and (2), the Default Domain Policy is applied.