Remote access account lockout

Updated: January 21, 2005

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

Remote access account lockout

You can use the remote access account lockout feature to specify how many times a remote access authentication fails against a valid user account before the user is denied access. Remote access account lockout is especially important for remote access virtual private network (VPN) connections over the Internet. An attacker on the Internet can attempt to access an organization intranet by sending credentials (valid user name, guessed password) during the VPN connection authentication process. During a dictionary attack, the attacker sends hundreds or thousands of credentials by using a list of passwords based on common words or phrases.

With remote access account lockout enabled, a dictionary attack is thwarted after a specified number of failed attempts. As the network administrator, you must decide on two remote access account lockout variables:

1. The number of failed attempts before future attempts are denied.

   After each failed attempt, a failed attempts counter for the user account is incremented. If the user account's failed attempts counter reaches the configured maximum, future attempts to connect are denied.

   A successful authentication resets the failed attempts counter when its value is less than the configured maximum. In other words, the failed attempts counter does not accumulate beyond a successful authentication.

2. How often the failed attempts counter is reset.

   The failed attempts counter is periodically reset to 0. If an account is locked out after the maximum number of failed attempts, the failed attempts counter is automatically reset to 0 after the reset time.

You enable the remote access account lockout feature by changing settings in the registry on the computer that provides the authentication. If the remote access server is configured for Windows Authentication, modify the registry on the remote access server computer. If the remote access server is configured for RADIUS authentication and Internet Authentication Service (IAS) is being used, modify the registry on the IAS server.

Caution

- Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.

To enable remote access account lockout, you must set the **MaxDenials** entry in the registry to **1** or greater. **MaxDenials** is the maximum number of failed attempts before the account is locked out. You set the **MaxDenials** entry in the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout

By default, **MaxDenials** is set to **0**, which means that remote access account lockout is disabled.

To modify the amount of time before the failed attempts counter is reset, you must set the **ResetTime (mins)** entry in the registry to the required number of minutes. You set the **ResetTime (mins)** entry in the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout

By default, **ResetTime (mins)** is set to **0xb40**, or 2,880 minutes (48 hours).

Manually resetting an account that is locked out

To manually reset a user account that has been locked out before the failed attempts counter is automatically reset, delete the following registry subkey that corresponds to the user's account name:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout\ *domain name:user name*

When the lockout count for a user account is reset to 0 due to either a successful authentication or an automatic reset, the registry subkey for the user account is deleted.

Notes

- Remote access account lockout is not related to the **Account locked out** setting on the **Account** tab on the properties of a user account.

- The remote access account lockout feature does not distinguish between malicious users who attempt to access your intranet and authentic users who attempt remote access but have forgotten their current passwords. Users who have forgotten their current password typically try the passwords that they remember and, depending on the number of attempts and the **MaxDenials** setting, may have their accounts locked out.

- If you enable the remote access account lockout feature, a malicious user can deliberately force an account to be locked out by attempting multiple authentications with the user account until the account is locked out, thereby preventing the authentic user from being able to log on.

Community Additions