Knowledge Base

HOW TO: Configure Remote Access Client Account Lockout in Windows 2000

PSS ID Number: 310302

Article Last Modified on 11/5/2003

The information in this article applies to:

- Microsoft Windows 2000 Server

This article was previously published under Q310302

IN THIS TASK

SUMMARY

This step-by-step article describes how you can configure the remote access client account lockout feature. Remote Access clients include direct dial-in and VPN clients. Windows 2000 supports account lockout for RAS clients. Account lockout is a valuable security feature that prevents intruders from trying multiple passwords in an attempt to violate the internal network. A malicious user can launch a dictionary attack where hundreds or even thousands of credentials are tried by using a list of common words or phrases.

back to the top

Configuring Remote Access Client Account Lockout Feature

The Remote Access client account lockout feature is managed separately from the account lockout settings that are maintained in Active Directory Users and Computers. RAS client account lockout settings are controlled by manually editing the registry. Note that the account lockout settings does not distinguish between a legitimate user that mistypes a password and an attacker that is trying to "crack" an account.

The advantage of enabling account lockout is that brute force attacks are unlikely to be successful because the account is locked long before the random guesses are successful. However, an attacker can create a denial of service condition that intentionally locks out user accounts.

The account lockout configuration for Remote Access clients include the following components:

- The number of failed logon attempts before the account is locked out.
- The amount of time that must pass before the account lockout timer is reset.

If you are using Windows Authentication on the Remote Access server, you will configure the registry on the RAS server. If you use RADIUS for Remote Access authentication, configure the registry on the Windows 2000 Internet Authentication Server (IAS) server.

back to the top

Enable Remote Access Client Account Lockout

To enable RAS client account lockout and reset time:

1. Click **Start**, click **Run**, type `regedt32`, and then click **OK**.
2. View the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout
3. Double-click on the **MaxDenials** value. The default value is **0**, which indicates that account lockout is disabled. Enter a new number for the number of failed attempts before the account is locked out. Click **OK**.
4. Double-click the **ResetTime (mins)** entry. The default value is **0xb40** which is Hexadecimal for 2,880 minutes (two days). You can change this value to meet your own network's security requirements. Click **OK**.

back to the top

Manually Unlock Remote Access Client Account Lockout

If the account is locked out, the user can try to log on again after the lockout timer has run out. If you need to manually unlock the account, you will have to delete a registry entry.

To manually unlock the account lockout:

- View the following registry key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout
- Find the domain name: user name entry, and then delete the entry. The user can now try to log on again.

back to the top

Keywords: kbhowto kbHOWTOmaster KB310302
Technology: kbwin2000Search kbwin2000Serv kbwin2000ServSearch