Knowledge Base

HOW TO: Enforce a Remote Access Security Policy in Windows 2000

PSS ID Number: 313082

Article Last Modified on 11/19/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Small Business Server 2000

This article was previously published under Q313082

IN THIS TASK

SUMMARY

This step-by-step article describes how to enforce a remote access security policy in a Windows 2000-based Native-mode domain.

In a Windows 2000-based Native-mode domain, you can use the following three remote access policy behaviors:

NOTE: This method of enforcing a remote access security policy also applies to a stand-alone Windows 2000-based remote access server.

- **Explicit allow**: The remote access policy is set to Grant remote access permission and the connection attempt matches the policy conditions.
- **Explicit deny**: The remote access policy is set to Deny remote access permission and the connection attempt matches the policy conditions.
- **Implicit deny**: The connection attempt does not match any remote access policy conditions.

To enforce a remote access policy:

1. Configure the remote access policy conditions.
2. Configure the user account dial-in settings.

back to the top

How to Configure a Remote Access Policy

The default Windows 2000 remote access policy is set to **Allow access if dial-in permission is enabled**. To enforce your remote access security policy, remove the default policy, and then create new remote access policies:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Expand ***server name*** where *server name* is the name of the server, and then click **Remote Access Policies**.

   NOTE: If you have not configured remote access, click **Configure and Enable Routing and Remote Access** on the **Action** menu, and then follow the steps of the Routing and Remote Access Server Setup Wizard.
3. In the console pane, right-click **Allow access if dial-in permission is enabled**, and then click **Delete**. When you receive the "Delete Policy" message, click **Yes**.
4. On the **Action** menu, click **New Remote Access Policy**.
5. Create a new remote access policy. The following example illustrates a remote access policy that explicitly allows remote access to one group during certain days, implicitly blocks access to the same group on other days, and explicitly blocks remote access to a second group.

   Example:

   a. In the **Policy friendly name** box, type `test policy`, and then click **Next**.
   b. Click **Add**, click **Windows-Groups**, click **Add**, and then click **Add**.
   c. Click **Domain Users**, click **Add**, click **OK**, click **OK**, and then click **Next**.

      NOTE: The Domain Users group is used for example purposes only. It is advantageous to create a specific group that you can use to control remote access permissions.
   d. Click **Grant remote access permission**, and then click **Next**.
   e. Click **Edit Profile**, click to select the **Restrict access to the following days and times** check box, and then click **Edit**.
   f. Click **Denied**, click **Monday through Friday from 8:00 A.M. to 4:30 P.M.**, click **Permitted**, and then click **OK**.
   g. Click **OK**, click **OK**, and then click **Finish**.

      Members of the Domain Users group are *explicitly* allowed remote access permissions from Monday through Friday from 8:00 A.M. to 4:30 P.M., and these members are *implicitly* denied remote access during other days and times.
   h. On the **Action** menu, click **New Remote Access Policy**.
   i. In the **Policy friendly name** box, type `test block policy`, and then click **Next**.
   j. Click **Add**, click **Windows-Groups**, click **Add**, and then click **Add**.

k. Click **Domain Admins**, click **Add**, click **OK**, click **OK**, and then click **Next**.

l. Click to select the **Deny remote access permission** check box if it is not already selected, click **Next**, and then click **Finish**.

Members of the Domain Admins group are *explicitly* denied remote access.

6. When you finish creating remote access policies, quit the Routing and Remote Access snap-in.

back to the top

How to Configure the User Account Dial-In Setting

Specify that remote access permissions are controlled by the remote access policy:

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then perform one of the following actions:
   - If the computer is an Active Directory domain controller, double-click **Active Directory Users and Computers**.

     In the console tree, click ***domain*** where *domain* is the name of the domain, click **Users**, and then click **Users**.

     -or-
   - If the computer is a stand-alone Windows 2000 server, double-click **Computer Management**.

     In the console tree, click **System Tools**, click **Local Users and Groups**, and then click **Users**.
2. Right-click the user account that you want, and then click **Properties**.
3. On the **Dial-in** tab, click **Control access through Remote Access Policy**, and then click **OK**.

   NOTE: If the **Control access through Remote Access Policy** option is unavailable (dimmed), Active Directory may be running in Mixed mode.For additional information about dial-in options that are unavailable when Active Directory is running in Mixed mode, click the article number below to view the article in the Microsoft Knowledge Base:

   193897 Dial-In Options Unavailable with Active Directory in Mixed Mode
4. Quit either Computer Management or Active Directory Users and Computers.

back to the top

Troubleshooting

If you do not use groups to specify remote access permissions in your policy configuration, ensure that the Guest account is disabled, and that you set its remote access permission to **Deny access**:

1. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then perform one of the following actions:
   - If the computer is an Active Directory domain controller, double-click **Active Directory Users and Computers**.

     In the console tree, click ***domain*** where *domain* is the name of the domain, click **Users**, and then click **Users**.

     -or-
   - If the computer is a stand-alone Windows 2000 server, double-click **Computer Management**.

     In the console tree, click **System Tools**, click **Local Users and Groups**, and then click **Users**.
2. Right-click the **Guest** user account, and then click **Properties**.
3. On the **Dial-in** tab, click **Deny access**, and then click **OK**.
   - On a domain controller, right-click **Guest**, point to **All Tasks**, and then click **Disable Account**. When you receive the "Object Guest has been disabled" message, click **OK**.
   - On a stand-alone Windows 2000 server, right-click **Guest**, and then click **Properties**. Click to select the **Account is disabled** check box, and then click **OK**.
4. Quit either Computer Management or Active Directory Users and Computers.

back to the top

REFERENCES

For additional information about remote access policies, click **Start**, and then click **Help**. Click the **Index** tab, type `ras policies`, and then click **Display** to view the available topics.

back to the top

Keywords: kbenv kbhowto kbHOWTOmaster kbnetwork KB313082
Technology: kbSBServ2000 kbSBServSearch kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbZNotKeyword3
