Enable Remote Dial in Access For Groups using NPS

-

To enable remote access by using the remote access properties of a user account

1. In either **Local Users and Groups** on a stand-alone computer, or in **Active Directory Users and Computers** on a member of a domain, right-click the user account and then click **Properties**.
2. Select the **Dial-in** tab.
3. In the **Network Access Permission** section, select **Allow access**.
4. If you have the appropriate hardware support and want to restrict the user to calling from only an approved phone number, select **Verify Caller-ID** and enter the phone number.
5. If you want the remote access server to call the user back to complete the connection, configure the appropriate **Callback Option**.
6. If you want the computer to use a specific IP address instead of having the RRAS server allocate the address to the computer, select **Assign Static IP Addresses**, and then click **Static IP Addresses** to configure the address that you want to use.
7. If you need to configure the connection with specific static routes to enable access to certain network resources, then select **Apply Static Routes**, and then click **Static Routes** to configure the routes that you want to use.

To enable remote access by using an NPS remote access network policy

1. On the computer running NPS, in Server Manager, expand **Network Policy and Access Services**, expand **NPS**, expand **Policies**, and then click **Network Policies**.
2. In the **Actions** pane, click **New**

   The **New Network Policy** wizard appears.

3. Type a name for the policy, for example, **Grant Access to Members of CorpRemoteAccessUsers Group**.
4. For **Type of network access server**, select **Remote Access Server (VPN-Dial up)**, and then click **Next**.
5. On the **Specify Conditions** page, click **Add**
6. On the **Select condition** dialog box, select **User Groups**, and then click **Add**
7. On the **User Groups** dialog box, click **Add Groups**, type or browse to the group you want to add, and then click **OK**

   The domain/group name appears in the **User Groups** dialog box.

8. Click **OK** The **User Groups** condition with the domain/group name appears on the **Specify Conditions** wizard page.
9. Click **Next**.
10. On the **Specify Access Permission** wizard page, select **Access granted**, and then click **Next**.
11. On the **Configure Authentication Methods** wizard page, specify the authentication methods to be used when this policy is used to configure a connection to the RRAS server. When you have selected and configured the methods, click **Next**.

    Security Note

    We recommend that you use only one of the EAP authentication methods or MS-CHAP-v2.

12. On the **Configure Constraints** wizard page, specify parameters that you want to enforce on the connection. For **Idle Timeout** and **Session Timeout**, the connection is dropped if either timeout value is reached. For the other constraints, the connection request must match the configured parameter, or the connection attempt is rejected. Click **Next**.
13. On the **Configure Settings** wizard page you can configure Remote Authentication Dial-In User Service (RADIUS) attributes that are sent to the client to configure its use of the connection. If your network uses Network Access Protection (NAP) to help enforce network client health, then you can configure the connection to allow only limited access to a remediation server group until the client is verified as compliant with the NAP policy. You can also configure whether the client can use multiple connections to increase available bandwidth and how that bandwidth is managed. Finally, you can configure IP filters to restrict network traffic that can be sent or received, the encryption that is used for the connection, and how the client receives its IP address configuration for the connection.
14. On the **Completing New Network Policy** wizard page, confirm your settings. Click **Previous** to return to any page to adjust any settings. Click **Finish** on this page when you are done.

    The policy is saved, and appears in the **Network Policies** list. The policy is assigned a **Processing Order**. Policies are evaluated in the order shown in this column. The first policy to match the conditions of the connection request is the one used to authorize and configure the connection. When troubleshooting connection failures, ensure that the policy order is not causing an unexpected policy to be used.