

## **IAS (RADIUS) Server Implementation**

Some settings will not be used and these will be noted with (“\*”).

### **To configure user accounts and groups, do the following:**

1. Ensure that all users that are making remote access connections have a corresponding user account.
2. Set the remote access permission on user accounts to “Grant access” or “Deny access” to manage network access by user. Or, to manage network access by group, set the remote access permission on user accounts to “Control access through Remote Access Policy”.
3. Organize remote access users into the appropriate universal and nested groups in order to take advantage of group-based remote access policies.
4. If you are using CHAP, enable support for reversibly encrypted passwords in the appropriate domains. You can configure reversibly encrypted passwords by using Group Policy. For more information, see "Enable reversibly encrypted passwords in a domain" in Help and Support Center for Windows Server 2003.

### **To configure the primary IAS server on a domain controller, do the following:**

1. On the domain controller, install IAS by using “Add/Remove Windows Components”.
2. Configure the IAS server to read the properties of user accounts in the domain. For more information, see "Enable the IAS server to read user accounts in Active Directory" in Help and Support Center for Windows Server 2003.
3. If the IAS server authenticates connection attempts for user accounts in other domains, use the Active Directory Domains and Trusts snap-in to verify that these domains have a two-way trust with the domain in which the IAS server is a member. Next, configure the IAS server to read the properties of user accounts in other domains by adding the IAS server to the “RAS and IAS Servers” security group on all domain controllers with user account databases to be accessed by the IAS server.
4. Enable file logging for accounting and authentication events. You can log session information to text files in either IAS format or database-compatible format, or you can log to a server running SQL Server 2000 or later. In addition, you can configure which information you want to log. For more information, see "Remote Access Logging" in Help and Support Center for Windows Server 2003.

5. If needed, configure additional User Datagram Protocol (UDP) ports for authentication and accounting messages that are sent by RADIUS clients. By default, IAS uses UDP ports 1812 and 1645 for authentication and ports 1813 and 1646 for accounting.

6. Add the access servers as RADIUS clients of the IAS server. Verify that you are configuring the correct name or IP address and shared secrets. Enable the use of the “Message-Authenticator” attribute, but only when it is also supported by the RADIUS client.

\*7. Create remote access policies that reflect your network access usage scenarios.

\*8. If you have created new remote access policies, either delete the default remote access policies or move them so that they are the last policies to be evaluated.

