

# Configuring Microsoft RADIUS Server and Gx000 Authentication

---

## Configuration Notes

Revision 1.0

February 6, 2003



## Notice

---

Gemtek Systems reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Gemtek Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Gemtek Systems.

## Trademarks

---

The product described in this document is a licensed product of Gemtek Systems Holding BV.

Microsoft, Windows 95, Windows 98, Windows Millennium, Windows NT, Windows 2000, Windows XP, and MS-DOS are registered trademarks of the Microsoft Corporation.

Novell is a registered trademark of Novell, Inc.

MacOS is a registered trademark of Apple Computer, Inc.

Java is a trademark of Sun Microsystems, Inc.

Wi-Fi is a registered trademark of Wi-Fi Alliance.

All other brand and product names are trademarks or registered trademarks of their respective holders.

# Contents

---

Notice.....	5
Trademarks .....	5
<b>CONTENTS .....</b>	<b>6</b>
<b>ABOUT THIS GUIDE.....</b>	<b>7</b>
Purpose .....	7
Prerequisite Skills and Knowledge .....	7
Conventions Used in this Document .....	7
Help Us to Improve this Document!.....	7
<b>INTRODUCTION.....</b>	<b>8</b>
Configuring Microsoft RADIUS Server and Gx000 Authentication .....	8
<b>CONFIGURE THE RADIUS SERVER.....</b>	<b>9</b>
Add RADIUS Client to IAS.....	9
Add New Remote Access Policy to IAS .....	11
Configure Active Directory to Use Reversible Encrypted Passwords .....	13
Add Test User.....	15

## About this Guide

---

### Purpose

This document provides information and step-by-step procedures on Microsoft RADIUS server setup and Gemtek Systems Public Access Controller model G-4000/6000 to functioning properly.




### Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating systems under Microsoft Windows 95, 98, Millennium, 2000, NT, and Windows XP and general networking operations and troubleshooting knowledge.

### Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

	Very important information. Failure to observe this may result in damage.
	Important information that should be observed.
	Additional information that may be helpful but which is not required.
<b>bold</b>	Menu commands, buttons and input fields are displayed in bold

### Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the manual please send e-mail directly to:

[manuals@gemtek-systems.com](mailto:manuals@gemtek-systems.com)

## Introduction

---

### Configuring Microsoft RADIUS Server and Gx000 Authentication

The purpose of this document is to provide some configuration notes for how for correctly configure the **Microsoft RADIUS Server** for Gemtek Systems' **Public Access Controller** (model G4000 or G6000) product for successful functioning and user authentication.

The following conditions should be fulfilled:

- Have a **Microsoft Windows 2000 Server** or **Advanced Server** installed.
- Networking properly configured.



Microsoft **RADIUS Server** is the Internet Access Service (IAS) of Windows 2000 Server. The **IAS** uses the Active Directory Service (ADS) users database.

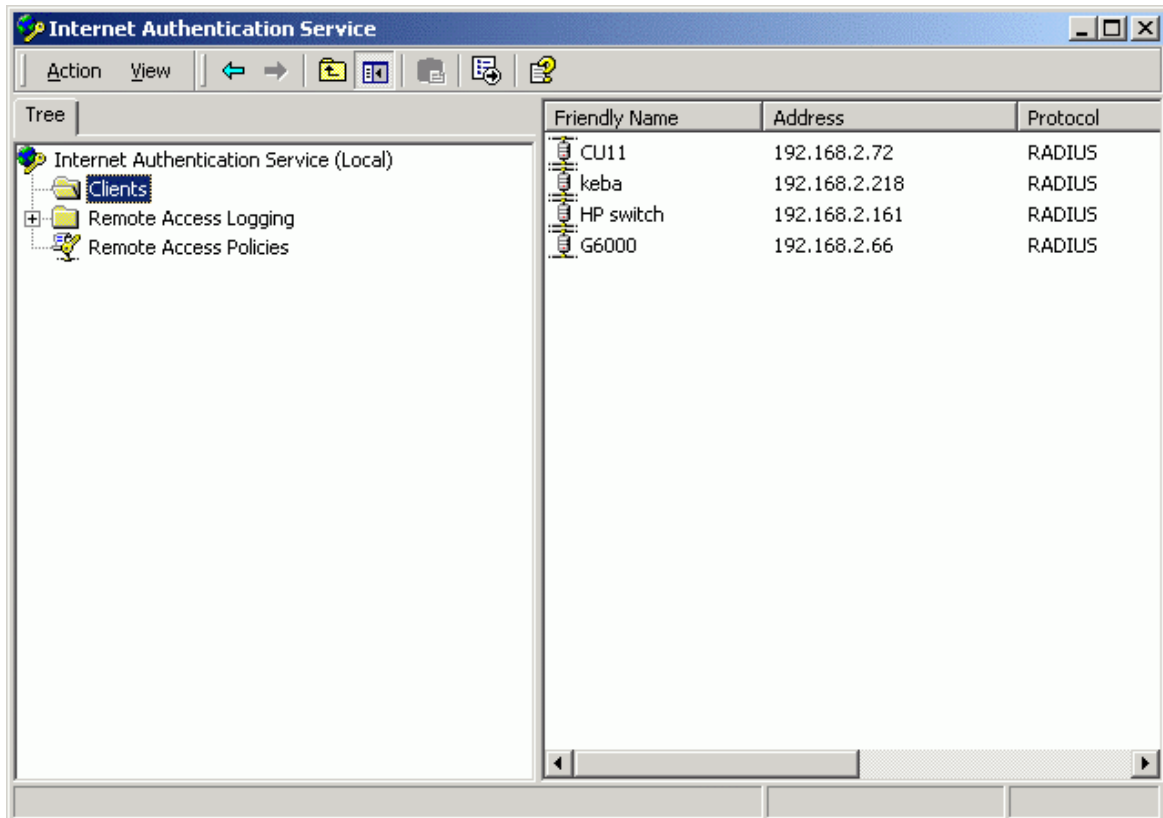
When these pre-conditions are accomplished please do the following steps.

## Configure the RADIUS Server

Instructions provided in the next sections helps to configure the RADIUS server and create test user, which is allowed to login to Public Access Controller using the RADIUS authentication.

### Add RADIUS Client to IAS

**Step 1** Open the **Administrative Tools->Internet Access Service:**

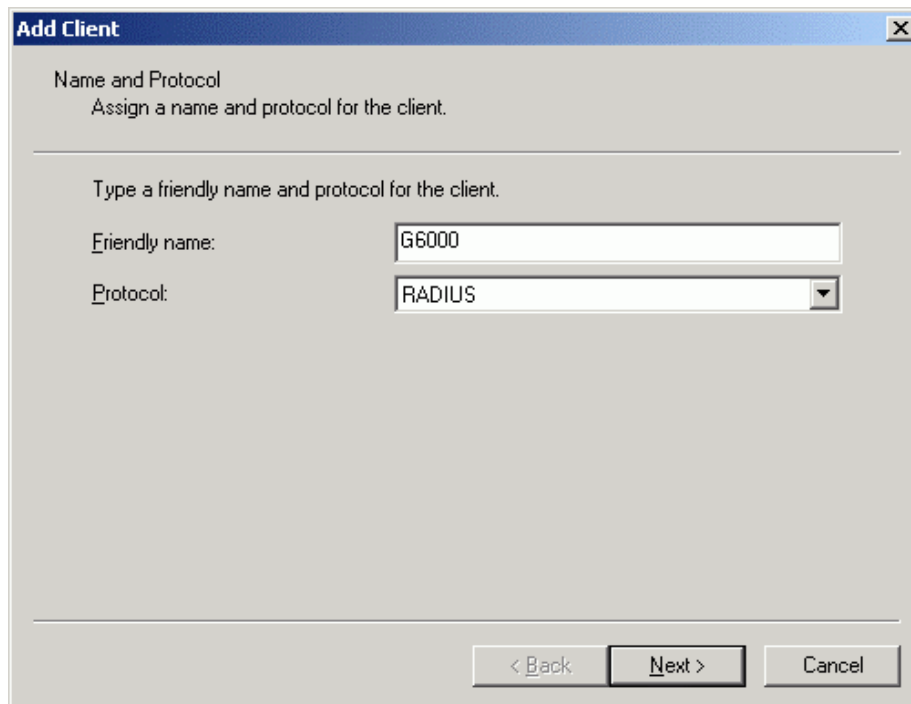


**Step 2** Select **Clients** tree menu item;



Client is the device or computer that requests **RADIUS** authentication. In our case this is the **G6000** device.

**Step 3** Select **Action | New Client** menu item and enter the **Friendly Name:** G6000:



**Add Client**

Name and Protocol  
Assign a name and protocol for the client.

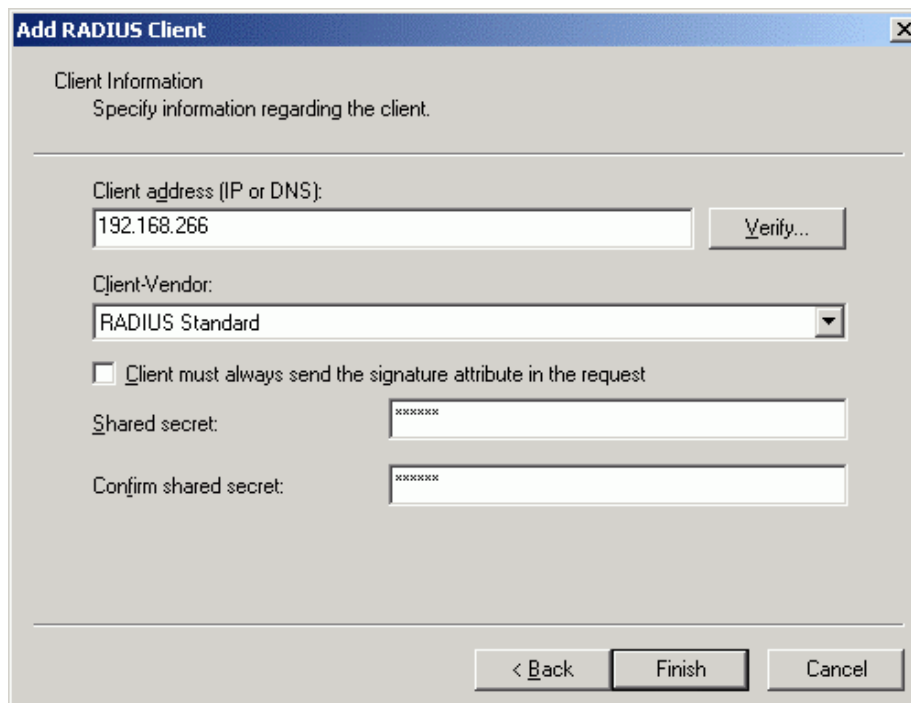
Type a friendly name and protocol for the client.

Friendly name: G6000

Protocol: RADIUS

< Back Next > Cancel

**Step 4** In **Protocol** drop-down list select **RADIUS** and click the **Next** button. The **Add RADIUS Client** window is displayed:



**Add RADIUS Client**

Client Information  
Specify information regarding the client.

Client address (IP or DNS): 192.168.266 Verify...

Client-Vendor: RADIUS Standard

Client must always send the signature attribute in the request

Shared secret: xxxxxxx

Confirm shared secret: xxxxxxx

< Back Finish Cancel

- Enter the **Client Address** (G6000 IP address);
- Under the **Client Vendor** select RADIUS Standard;
- Enter the **Shared Secret**;

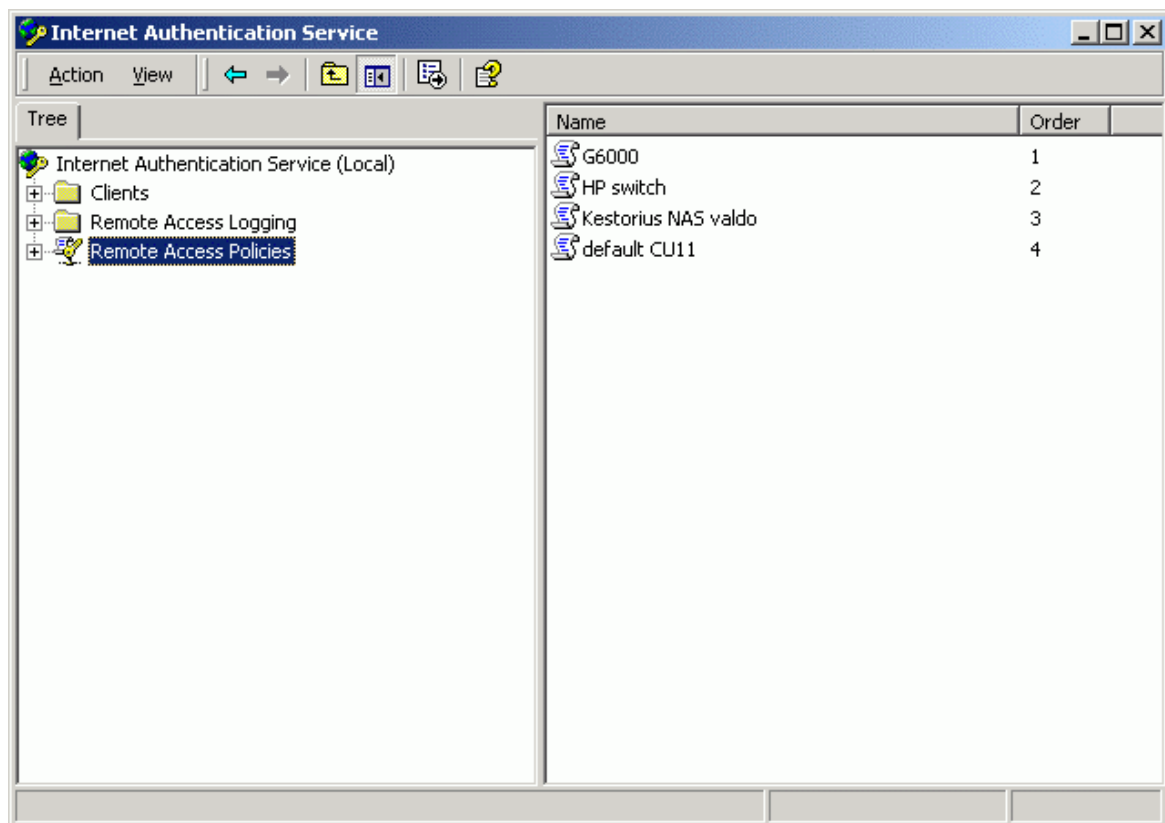


Shared secret must match the shared secret in the G6000 device RADIUS configuration settings. You can find this option in the Gx000 web management under the **network interface | RADIUS settings** menu.

**Step 5** Confirm the **Shared Secret** and click the **Finish** button to add RADIUS client to IAS.

## Add New Remote Access Policy to IAS

**Step 1** Select the **Remote Access Policies** tree menu item in the **Internet Authentication Service**:



**Step 2** From main menu select **Action | New Remote Access Policy** and enter the **Policy Name**;



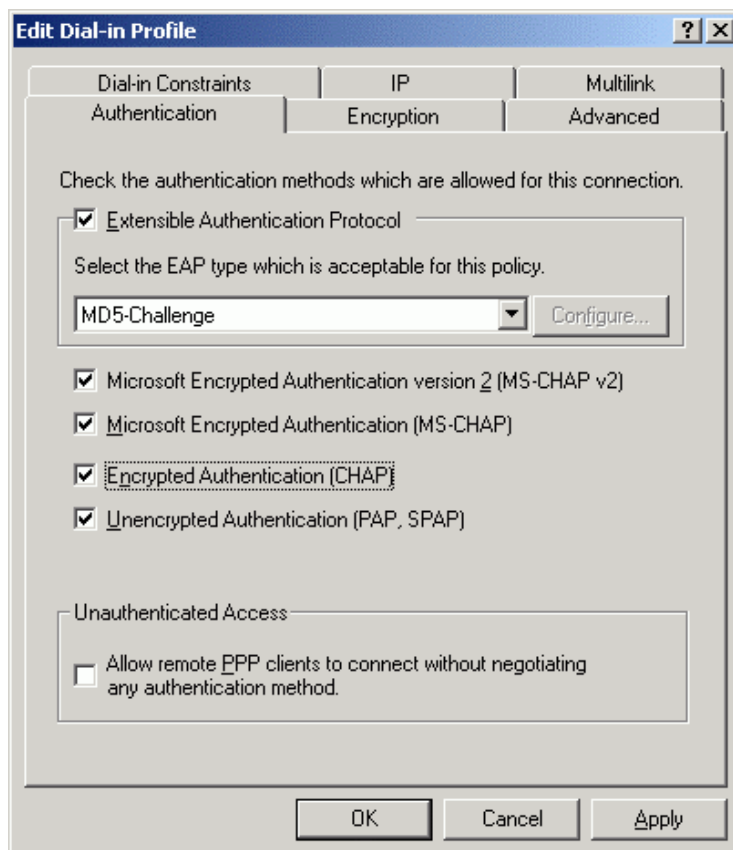
This one is not relevant. We can just enter **G6000**.

**Step 3** In **Add Remote Access Policy** dialog click the **Add...** button;

**Step 4** Select the **NAS-IP-Address** and click the **Add...** button;

**Step 5** In the **NAS-IP-Address** dialog box type G6000 IP address and click the **OK** button;

- Step 6** In the **Add Remote Access Policy** dialog click the **Next** button;
- Step 7** Select Grant Remote Access Permission and click Next;
- Step 8** Now click the **Edit Profile** button;
- Step 9** Select on **Authentication** tab in the **Edit Dial-in-Profile** window and check all authentication methods.
- Step 10** Check to select **Extensible Authentication Protocol** and in **EAP type** drop-down list select **MD5-Challenge**. Now the dialog should look like:



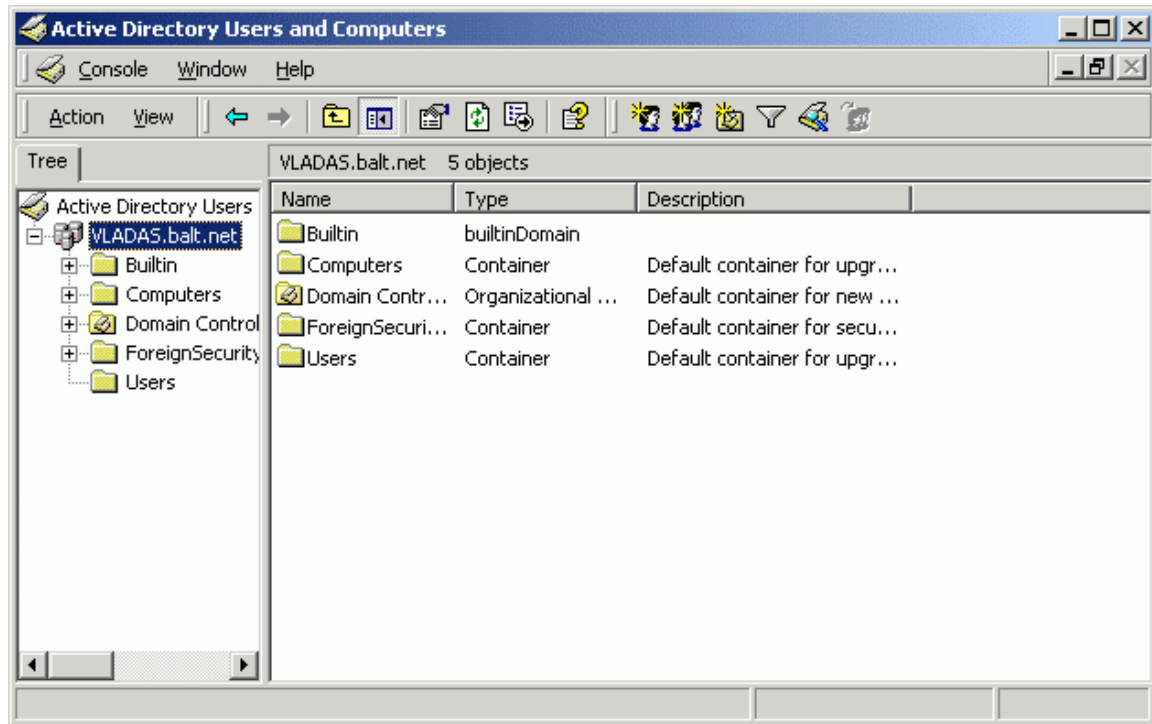
- Click the **OK** button to save settings;
- In **Add Remote Access Policy** dialog click the **Finish** button to finish adding the new Remote Access Policy Rule.



If there are multiple remote access policies configured make the new one policy the first. Use arrow buttons on the tool bar to move policy up until it becomes number 1 in the **Order** column.

## Configure Active Directory to Use Reversible Encrypted Passwords

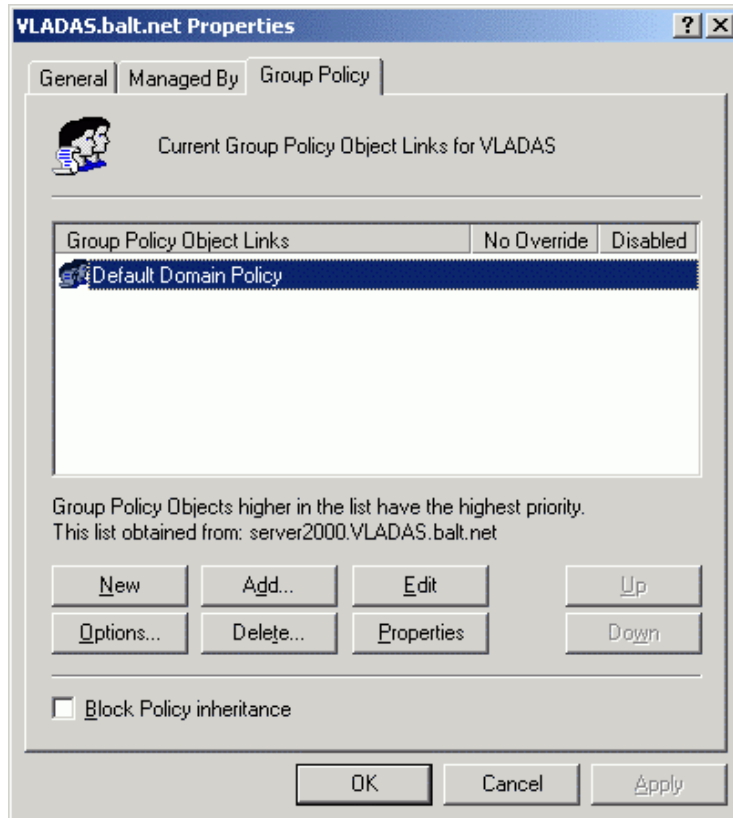
**Step 1** Open the **Administrative Tools** → **Active Users Directory and Computers**:



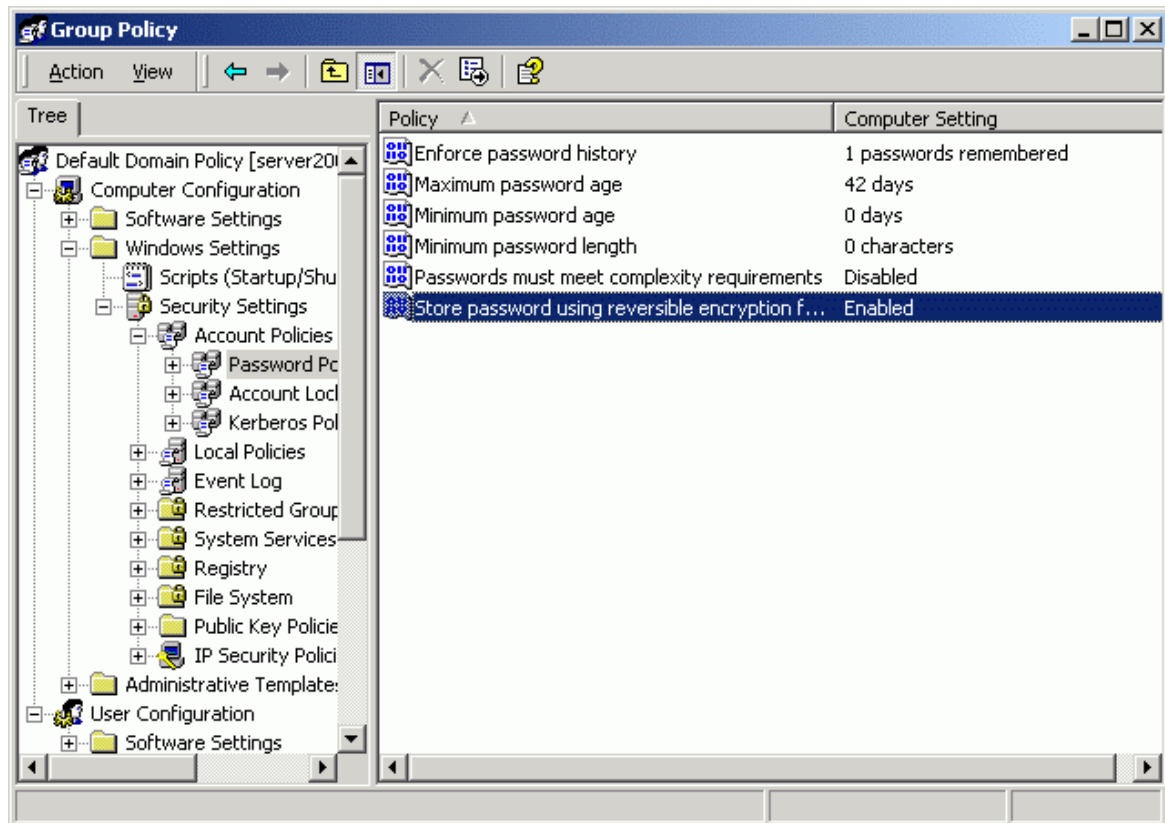
**Step 2** Select the server name from the **Active Directory Users** tree menu (in this demonstration case: VLADAS.balt.net).

**Step 3** Right-click on the selection and select the **Properties** menu;

**Step 4** Select the **Group Policy Tab**:



**Step 5** Select **Default Domain Policy** and click the **Edit** button. The **Group Policy** window opens:

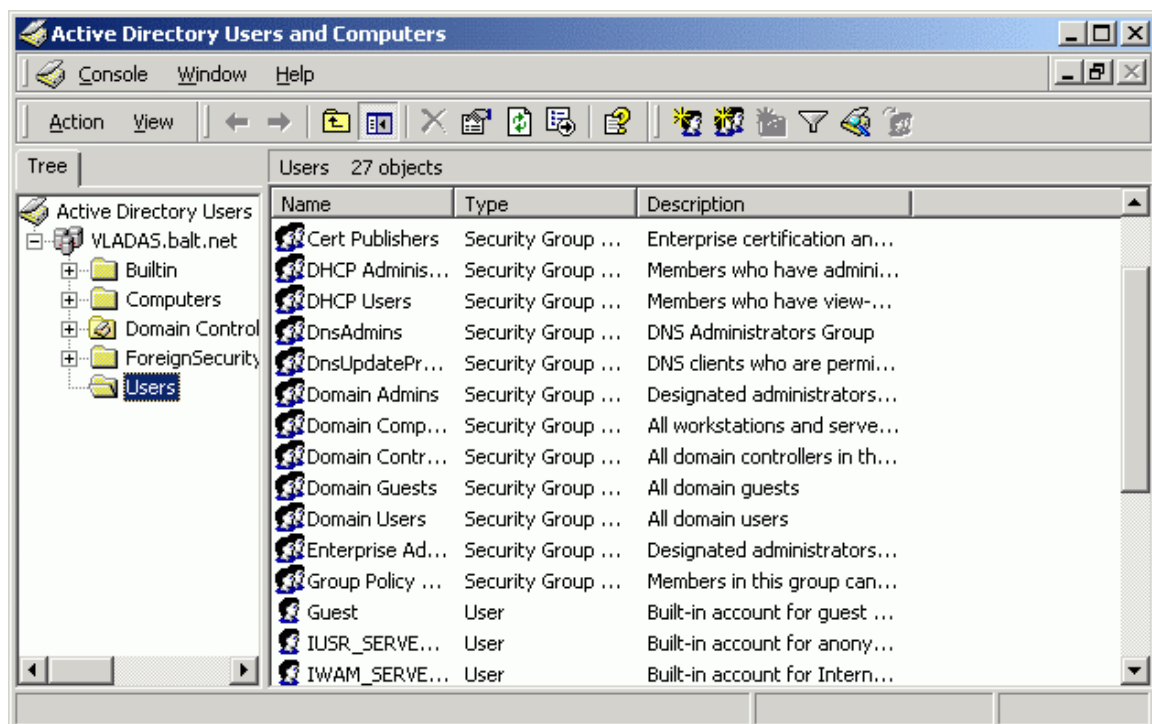


**Step 6** On the left pane select **Computer Configuration | Windows Settings | Security Settings | Accounts Policies | Password Policy** tree menu item and set **Store password using reversible encryption** value to **Enabled**;

**Step 7** Close the **Group Policy** window. Required configuration for active directory is set.

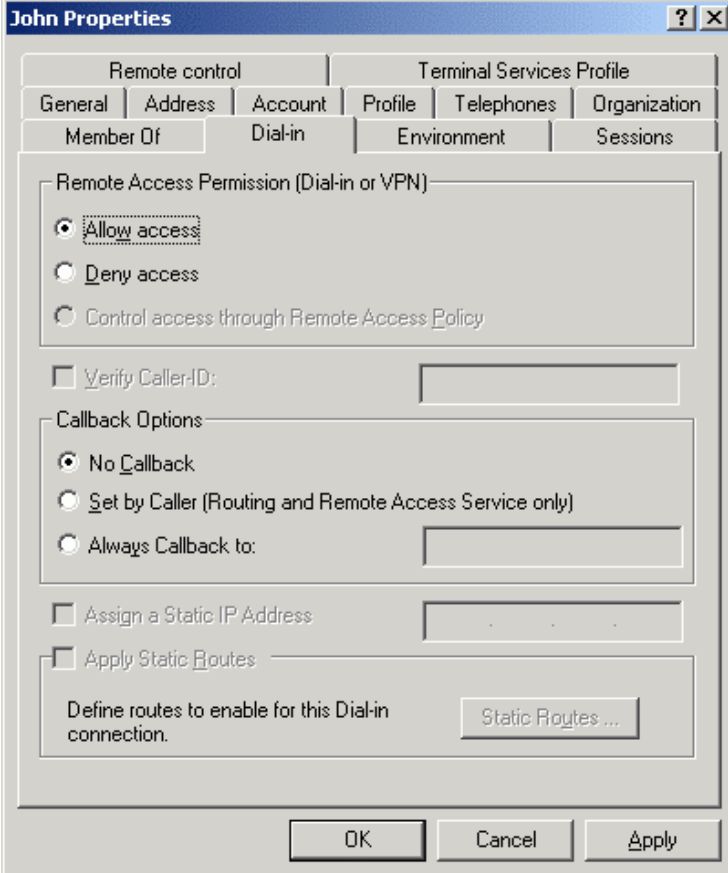
## Add Test User

**Step 1** Select **Users** in the **Active Directory Users and Computers** and add/set password for test user:



**Step 2** Select **Dial-in** tab in the new created user **Properties**;

**Step 3** Select **Allow** access radio button in the **Remote Access Permission (Dial-in or VPN)** section:



The screenshot shows the 'John Properties' dialog box with the 'Dial-in' tab selected. The 'Remote Access Permission (Dial-in or VPN)' section is expanded, showing three radio button options: 'Allow access' (selected), 'Deny access', and 'Control access through Remote Access Policy'. Below this are several checkboxes: 'Verify Caller ID' (unchecked), 'Assign a Static IP Address' (unchecked), and 'Apply Static Routes' (unchecked). The 'Callback Options' section is also expanded, showing three radio button options: 'No Callback' (selected), 'Set by Caller (Routing and Remote Access Service only)', and 'Always Callback to:'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

- Click the **OK** button. The test user is created.

Now you have the RADIUS Server configured and the test user created, which is allowed to login using **RADIUS** and **Gx000** device authentication.



**RADIUS Servers** from Gx000 device side is configured using the Web Management interface under the **network interface | RADIUS** menu.