

The Microsoft Windows logo, consisting of four colored panes (orange, green, blue, yellow) arranged in a square.

Microsoft  
**Windows Server** 2003

## **Internet Authentication Service (IAS) Operations Guide**

---

Microsoft Corporation

Published: August 2005

Author: James McIllece

Editor: Scott Somohano

### **Abstract**

The Internet Authentication Service (IAS) Operations Guide provides administration information for IAS in the Windows Server 2003 and Windows Server 2003 with Service Pack 1 (SP1) operating systems. IAS is the Microsoft implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol, and can be configured to act as a RADIUS server and proxy, providing centralized network access management. You can also configure IAS to perform authorization locally while forwarding authentication requests to a remote RADIUS server group. In addition, you can customize the processing of accounting requests, processing them locally or forwarding them to other RADIUS servers.

**Microsoft**



*The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.*

*This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user.*

*Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.*

*© 2005 Microsoft Corporation. All rights reserved.*

*Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.*

*All other trademarks are property of their respective owners.*



# Contents

---

Internet Authentication Service (IAS) Operations Guide .....	7
Administering IAS.....	8
Introduction to Administering IAS.....	8
When to Use This Guide.....	9
How to Use This Guide.....	9
Best Practices for IAS .....	10
Managing IAS.....	13
Managing IAS servers.....	13
Administer IAS using tools .....	14
Enter the Netsh AAAA context on an IAS server .....	14
Manage multiple IAS servers with the IAS console .....	15
Manage an IAS server using Remote Desktop Connection .....	16
Configure IAS on a multihomed computer .....	17
Configure IAS UDP port information .....	18
Copy part of the IAS configuration to another server.....	19
Export an IAS server configuration for import on another server .....	21
Register an IAS server in another domain.....	22
To register an IAS server in another domain.....	22
Register an IAS server in the default domain .....	23
To register an IAS server in the default domain .....	23
Unregister an IAS server from the default domain.....	24
To unregister an IAS server from the default domain.....	25
Verify configuration after an IAS server IP address change.....	25

Verify configuration after renaming an IAS server .....	27
Managing certificates used with IAS .....	28
Change the cached TLS handle expiry .....	28
Configure the TLS handle expiry time on client computers .....	30
Configure the TLS handle expiry time on IAS servers .....	30
Configure certificates for PEAP and EAP .....	31
Configure client computer certificates .....	33
Configure client computers to authenticate IAS servers .....	35
Configure server certificates .....	36
Configure the ACL of the RAS and IAS Server certificate template .....	38
Configure user certificates .....	40
Obtain the SHA-1 hash of a trusted root CA certificate .....	41
Managing RADIUS clients .....	42
Set up RADIUS clients .....	43
Configure the network access server .....	44
Add the network access server as a RADIUS client in IAS .....	44
Set up RADIUS clients by IP address range .....	45
Managing remote access policies .....	47
Configure IAS for VLANs .....	48
Configure a remote access policy for VLANs .....	49
Configure the EAP payload size .....	51
Configure the Framed-MTU attribute .....	51
Configure the Ignore-User-Dialin-Properties attribute .....	52
Additional IAS Resources .....	53

# Internet Authentication Service (IAS) Operations Guide

---

The Internet Authentication Service (IAS) Operations Guide provides administration information for IAS in the Microsoft® Windows Server™ 2003 and Windows Server 2003 with Service Pack 1 (SP1) operating systems.

IAS is not included on computers running the Microsoft® Windows® Server 2003, Web Edition, operating system. For more information about Windows Server 2003, Web Edition, see [Overview of Windows Server 2003, Web Edition](http://go.microsoft.com/fwlink/?LinkId=9253) on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=9253>.

IAS is the Microsoft implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol, and can be configured to act as a RADIUS server and proxy, providing centralized network access management. When you configure IAS as a RADIUS server, network access servers that are configured as RADIUS clients in IAS forward connection requests to IAS for authentication and authorization. When you configure IAS as a proxy, IAS forwards authentication and accounting requests to other RADIUS servers in a remote RADIUS server group.

The network access servers that you can configure as RADIUS clients in IAS are wireless access points, virtual private network (VPN) servers, 802.1X authenticating switches, and dial-up servers.

You can also configure IAS to perform authorization locally while forwarding authentication requests to a remote RADIUS server group. In addition, you can customize the processing of accounting requests, processing them locally or forwarding them to other RADIUS servers.

With IAS in Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of RADIUS clients and remote RADIUS server groups. In addition, you can configure RADIUS clients by specifying an IP address range.

With IAS in Windows Server 2003, Standard Edition, you can configure a maximum of 50 RADIUS clients and a maximum of 2 remote RADIUS server groups. You can define a RADIUS client using a fully qualified domain name or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. If the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the Domain Name System (DNS) query.

**In this guide**

- [Administering IAS](#)

## Administering IAS

---

This guide provides administering information for IAS in the Microsoft Windows Server 2003 and Windows Server 2003 with Service Pack 1 (SP1) operating systems.

**In this guide**

- [Introduction to Administering IAS](#)
- [Best Practices for IAS](#)
- [Managing IAS](#)
- **Additional IAS Resources**

IAS is the Microsoft implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol, and can be configured to act as a RADIUS server and proxy, providing centralized network access management.

**Acknowledgements**

Produced by: Microsoft Windows Server User Assistance Team

Project Writer: James McIllece

Project Editor: Scott Somohano

Technical Reviewers: Majdi Badarin; Sam Salhi; Tom Baker

## Introduction to Administering IAS

---

This guide, in conjunction with the IAS procedural Help topics, explains how to administer IAS. The objectives, tasks, and procedures described in this guide and in procedural Help topics discuss actions that are part of the operating phase of the information technology (IT) life cycle.

To access the IAS procedural Help topics, open the IAS console and press F1.

Procedural topics are found at the following path in the IAS Help table of contents:

**Internet Authentication Service | How To.** The IAS product Help is also available on the Web at [Internet Authentication Service](http://go.microsoft.com/fwlink/?LinkId=20133) at <http://go.microsoft.com/fwlink/?LinkId=20133>.

If you are not familiar with this guide, review the following sections of this introduction.

## When to Use This Guide

This guide assumes a basic understanding of what IAS is, how it works, and why your organization uses it to manage network access, including the authentication, authorization, and accounting for network connections. You should also have a thorough understanding of how IAS is deployed and managed in your organization before performing any of the actions described in this guide.

This guide can be used by organizations that have deployed Windows Server 2003 and Windows Server 2003 with Service Pack 1 (SP1). It includes information that is relevant to different roles within an IT organization, including IT operations management and administrators.

This guide contains both high-level information and more detailed procedures that are designed for operators who have varied levels of expertise and experience. Although the procedures provide operator guidance from start to finish, operators must have a basic proficiency with the Microsoft Management Console (MMC) and snap-ins and know how to start administrative programs and access the command line and the netsh commands for AAAA.

If operators are not familiar with IAS, it might be necessary for IT planners or IT managers to review the relevant operations in this guide and provide the operators with parameters or data that must be entered when the operation is performed.

## How to Use This Guide

The operations areas are divided into the following types of content:

- Objectives are high-level goals for managing, monitoring, optimizing and securing IAS. Each objective consists of one or more high-level tasks that describe how the objective is accomplished.
- Tasks are used to group related procedures and provide general guidance for achieving the goals of an objective.
- Procedures provide step-by-step instructions for completing tasks.

If you are an IT manager who will be delegating tasks to operators within your organization, you will want to:

- Read through the objectives and tasks to determine how to delegate permissions and whether you need to install tools before operators perform the procedures for each task.
- Before assigning tasks to individual operators, ensure that you have all the tools installed where operators can use them.
- When necessary, create “tear sheets” for each task that operators perform in your organization. Cut and paste the task and its related procedures into a separate document, and then either print these documents or store them online, depending on the preference of your organization.

## Best Practices for IAS

---

This topic provides best practices for administering IAS based on recommendations from Microsoft Product Support Services:

- Use Terminal Services to access a remote IAS server.  

When you are administering an IAS server remotely, it is important not to send sensitive or confidential data (for example shared secrets or passwords) over the network in plaintext. When you use Terminal Services, data is not sent between client and server. Only the user interface of the server (for example, the operating system desktop and IAS console image) is sent to the Terminal Services client, which is named Remote Desktop Connection. The client sends keyboard and mouse input, which is processed locally by the server that has Terminal Services enabled. When Terminal Services users log on, they can view only their individual client sessions, which are managed by the server and are independent of each other. In addition, Remote Desktop Connection provides 128-bit encryption between client and server.
- Use the Runas command to administer local IAS servers  

You can use the Runas command to perform administrative tasks when you are logged on as a member of a group that does not have the required administrative credentials (such as the Users group or the Power Users group). Logging on to your server without administrative credentials is recommended because it protects the computer from a variety of possible security attacks, such as the accidental installation of a computer virus.
- Use IAS Logging

There are two types of logging in IAS:

- **Event logging for IAS.** You can use event logging to record IAS events in the system event log. This is used primarily for auditing and troubleshooting connection attempts.
- **Logging user authentication and accounting requests.** You can log user authentication and accounting requests to log files in text format or database format, or you can log to a stored procedure in a SQL Server 2000 database. Request logging is used primarily for connection analysis and billing purposes, and is also useful as a security investigation tool, providing you with a method of tracking down the activity an attacker.

To make the most effective use of IAS logging:

1. Turn on logging (initially) for both authentication and accounting records. Modify these selections after you have determined what is appropriate for your environment.
  2. Ensure that event logging is configured with a capacity that is sufficient to maintain your logs.
  3. Back up all log files on a regular basis, because they cannot be recreated when they are damaged or deleted.
  4. Use the RADIUS Class attribute to both track usage and simplify the identification of which department or user to charge for usage. Although the automatically generated Class attribute is unique for each request, duplicate records might exist in cases where the reply to the access server is lost and the request is resent. You might need to delete duplicate requests from your logs to accurately track usage.
  5. To provide failover and redundancy with SQL Server logging, follow the deployment instructions provided in the whitepaper [Deploying SQL Server Logging with Windows Server 2003 Internet Authentication Service \(IAS\)](http://go.microsoft.com/fwlink/?LinkId=41039) on the Web at <http://go.microsoft.com/fwlink/?LinkId=41039>.
  6. You can use the lasparse.exe tool in the \Support\Tools folder on the Windows Server 2003 operating system CD to view IAS logs.
- Install IAS on a domain controller

To optimize IAS authentication and authorization response times and minimize network traffic, install IAS on a domain controller. When universal principal names (UPNs) or Windows Server 2003 domains are used, IAS uses the global catalog to authenticate users. To minimize the time it takes to do this, install IAS on either a global catalog server or a server that is on the same subnet and Active Directory site. Sites differ from domains; sites represent the physical structure of your network, whereas domains represent the logical structure of your organization. For more

information, see [Sites overview](http://go.microsoft.com/fwlink/?LinkId=48970) on the Web at <http://go.microsoft.com/fwlink/?LinkId=48970>.

- Disable NAS notification forwarding

When you have remote RADIUS server groups configured and, in RADIUS proxy server Connection Request Policies, you clear the **Record accounting information on the servers in the following remote RADIUS server group** check box, these groups are still sent network access server (NAS) start and stop notification messages. This creates unnecessary network traffic. To eliminate this traffic, disable NAS notification forwarding for individual servers in each remote RADIUS server group by clearing the **Forward network start and stop notifications to this server** check box.

- Use universal groups

If you are using IAS in a large organization and are using remote access policies to restrict access for all but specified groups, create a universal group for all of the users for whom you want to allow access, and then create a remote access policy that grants access for this universal group. Do not put all of your users directly into the universal group, especially if you have a large number of them on your network. Instead, create separate groups that are members of the universal group, and add users to those groups.

- Use user principal names

Use a user principal name to refer to users whenever possible. A user can have the same user principal name regardless of domain membership. This practice provides scalability that might be required in organizations with a large number of domains.

- Increase the number of concurrent authentications

If the IAS server is on a computer other than a domain controller and it is receiving a very large number of authentication requests per second, you can improve performance by increasing the number of concurrent authentications between the IAS server and the domain controller.

To do this, edit the following registry key:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters.**

Add a new entry named **MaxConcurrentApi** and assign to it a value from 2 through 5.

# Managing IAS

---

By effectively managing your IAS deployment, you can provide secure network access for your organization, ensuring that authorized organization employees, business partners, and guests can access the network when and where they need to do so.

The following objectives are part of managing IAS:

- [Managing IAS servers](#)
- [Managing certificates used with IAS](#)
- [Managing RADIUS clients](#)
- [Managing remote access policies](#)

## Managing IAS servers

---

Managing IAS servers across your organization means providing IAS server availability, with approved and consistent network access policies configured across your IAS deployment.

When you manage IAS servers, you ensure that RADIUS clients have access to the servers, the IAS servers have permission to access your user accounts databases, and that RADIUS traffic is sent and received on the same UDP ports.

In addition, you can synchronize server configurations in whole or in part by using Netsh AAAA commands.

The following tasks for managing IAS servers are described in this objective:

- [Administer IAS using tools](#)
- [Configure IAS on a multihomed computer](#)
- [Configure IAS UDP port information](#)
- [Copy part of the IAS configuration to another server](#)
- [Export an IAS server configuration for import on another server](#)
- [Register an IAS server in another domain](#)
- [Register an IAS server in the default domain](#)
- [Unregister an IAS server from the default domain](#)
- [Verify configuration after an IAS server IP address change](#)

- [Verify configuration after renaming an IAS server](#)

## Administer IAS using tools

---

IAS provides two tools that you can use to administer IAS -- the IAS console and the netsh commands for authentication, authorization, accounting, and auditing (AAAA).

The following procedures show how to manage IAS using these tools:

- [Enter the Netsh AAAA context on an IAS server](#)
- [Manage multiple IAS servers with the IAS console](#)
- [Manage an IAS server using Remote Desktop Connection](#)

## Enter the Netsh AAAA context on an IAS server

---

You can use commands in the Netsh AAAA context to show and set the configuration of the authentication, authorization, accounting, and auditing (AAAA) database used by IAS and the Routing and Remote Access service. The AAAA database is also known as the IAS database (ias.mdb). The primary use of commands in the Netsh AAAA context is to:

- Export the configuration of one IAS server, including registry keys and the IAS database (ias.mdb), as a Netsh script using either the **dump** command or one of the **show** commands.
- Import the configuration to another IAS server using the **netsh exec** command, and a Netsh script that contains the **set config** command.

You can run these commands from the Windows Server 2003 family command prompt or from the command prompt for the Netsh AAAA context. For these commands to work at the Windows Server 2003 family command prompt, you must type **netsh aaaa** before typing commands and parameters.

There might be functional differences between Netsh context commands on Windows 2000 and the Windows Server 2003 family.

### Administrative Credentials

To perform this procedure, you must be a member of the Administrators group on the local computer.

▶ **To enter the Netsh AAAA context on an IAS server**

1. Open **Command Prompt**.
2. Type **netsh**, and then press ENTER.
3. Type **aaaa**, and then press ENTER.

## Manage multiple IAS servers with the IAS console

---

Use the instructions below to manage a local IAS server and remote IAS servers from the Microsoft Management Console (MMC) on the local IAS server.

Before performing the procedure below, you must install IAS on the local computer.

Depending on network conditions and the number of IAS servers you manage using the IAS console, response of the MMC console might be slow. In addition, IAS server configurations are sent over the network during a remote administration session using the IAS console. Ensure that your network is physically secure and that malicious users do not have access to this network traffic.

### Administrative Credentials

To perform this procedure, you must be a member of the Domain Admins group.

▶ **To manage multiple IAS servers with the IAS console**

1. To open MMC, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In **Add Standalone Snap-in**, double-click **Internet Authentication Service (IAS)**, and then click **Add**.
4. In **Internet Authentication Service**, verify that **Local computer (the one this console is running on)** is selected. Click **Finish**. The snap-in for the local IAS server is added to the console.
5. In **Add Standalone Snap-in**, click **Add**. In **Internet Authentication Service**, click **Another computer**, and then type the name of the remote IAS server that you want to manage. Click **Finish**.
6. Repeat steps 4 and 5 for each additional IAS server that you want to add to the

IAS snap-in. When you have added all the IAS servers you want to manage, click **Close**, and then click **OK**.

7. To save the IAS console for later use, click **File**, click **Save**, type a name for your IAS console, and then click **Save**.

## Manage an IAS server using Remote Desktop Connection

---

Using Remote Desktop Connection, you can remotely manage your IAS servers running Windows Server 2003 family operating systems. You can also remotely manage Windows Server 2003 family operating systems from a computer using Microsoft® Windows® XP Professional.

### Administrative Credentials

To perform this procedure, you must be a member of the Domain Admins group.

#### ▶ To manage an IAS server using Remote Desktop Connection

1. On each IAS server that you want to manage remotely, in **Control Panel** open **System**, click the **Remote** tab, and then click **Enable Remote Desktop on this computer**.
2. Click **Select Remote Users**. In **Remote Desktop Users**, to grant permission to a user to connect remotely to the IAS server, click **Add**, and then type the user name for the user's account. Click **OK**.
3. Repeat step 2 for each user for whom you want to grant remote access permission to the IAS server.
4. On each IAS server, if Windows Firewall is enabled, add an exception to Windows Firewall for Remote Desktop.
5. To connect to a remote IAS server that you have configured using the previous steps, click **Start**, point to **Programs** or **All Programs**, point to **Accessories**, point to **Communications**, and then click **Remote Desktop Connection**.
6. In **Computer**, type the IAS server name or IP address.
7. Click **Connect**. The **Log On to Windows** dialog box appears.
8. In the **Log On to Windows** dialog box, type your user name, password, and

domain (if required), and then click **OK**.

## Configure IAS on a multihomed computer

---

On an IAS server that has multiple network adapters installed, you might want to configure IAS to send RADIUS traffic only on a specific adapter.

For example, one network adapter installed in the IAS server might lead to a network segment that does not contain RADIUS clients, while a second network adapter provides IAS with a network path to its configured RADIUS clients. In this scenario it is important to direct IAS to use the second network adapter for all RADIUS traffic.

The method used to configure IAS to use a specific network adapter is to configure RADIUS ports using the syntax *IPAddress:UDPport*, where *IPAddress* is the IP address configured on the network adapter over which you want to send RADIUS traffic, and *UDPport* is the RADIUS port number that you want to use for RADIUS authentication or accounting traffic. The following characters can be used as delimiters for configuring port information:

- Address/port delimiter: colon (:)
- Port Delimiter: comma (,)
- Interface delimiter: semi-colon (;)

Make sure that your network access servers - RADIUS clients such as VPN servers, 802.1X authenticating switches, wireless access points, and dial-up servers - are configured with the same RADIUS UDP port numbers that you configure on your IAS servers. The RADIUS standard UDP ports defined in RFCs 2865 and 2866 are 1812 for authentication and 1813 for accounting; however some access servers are configured by default to use UDP port 1645 for authentication requests and UDP port 1646 for accounting requests.

### Administrative Credentials

To perform this procedure, you must be a member of the Administrators group.

#### To specify the network adapter and UDP ports that IAS uses for RADIUS traffic

1. Open the IAS console.
2. Right-click **Internet Authentication Service**, and then click **Properties**.

3. Click the **Ports** tab, and prepend the IP address for the network adapter you want to use for RADIUS traffic to the existing port numbers. For example, if you want to use the IP address **192.168.1.2** and RADIUS ports **1812** and **1645** for authentication requests, change the port setting from **1812,1645** to **192.168.1.2:1812,1645**.

If your RADIUS authentication and RADIUS accounting UDP ports vary from the default values provided (1812 and 1645 for authentication, and 1813 and 1646 for accounting), change the port settings accordingly.

4. To use multiple port settings for authentication or accounting requests, separate the port numbers with commas.

## Configure IAS UDP port information

---

Use this procedure to configure User Datagram Protocol (UDP) ports for RADIUS traffic.

You can use the following procedure to configure the ports that IAS uses for RADIUS authentication and accounting traffic.

The values of 1812 for authentication and 1813 for accounting are RADIUS standard ports defined in RFCs 2865 and 2866. However, many access servers use ports 1645 for authentication requests and 1646 for accounting requests by default. Whatever port numbers you decide to use, make sure that IAS and your access server are configured to use the same ones.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

### To configure IAS UDP port information using the Windows interface

1. Open the IAS console.
2. Right-click **Internet Authentication Service**, and then click **Properties**.
3. Click the **Ports** tab, and then examine the settings for ports. If your RADIUS authentication and RADIUS accounting UDP ports vary from the default values provided (1812 and 1645 for authentication, and 1813 and 1646 for accounting), type your port settings in **Authentication** and **Accounting**.

4. To use multiple port settings for authentication or accounting requests, separate the port numbers with commas.

## Copy part of the IAS configuration to another server

---

Use this procedure to copy part of an IAS server or proxy configuration to another IAS server or proxy.

After you have deployed IAS, you might find it necessary to revise the settings on one IAS server and to duplicate this revision at other IAS servers or proxies. For example, if you add a secure wireless deployment on your network, you need to create at least one new remote access policy for the deployment, and you need to add your wireless access points as RADIUS clients at the IAS servers that are to process connection requests from the access points.

To perform this revision you can reconfigure one IAS server and then copy the configuration changes to your other IAS servers by using the Netsh commands for AAAA.

By using the **show** command in Netsh AAAA, you can export the following individual parts of the IAS server configuration for import on other servers:

- **RADIUS clients.** The **netsh aaa show clients** command dumps the RADIUS client list of the IAS server on which the command is run. In the IAS console, this client list is displayed in **RADIUS Clients**.
- **Connection request processing settings.** The **netsh aaa show connection\_request\_policies** command dumps the connection request policies for the IAS server on which the command is run. In the IAS console, these policies are displayed in **Connection Request Processing** and include **Connection Request Policies** and **Remote RADIUS Server Groups**.
- **Logging.** The **netsh aaa show logging** command dumps the remote access logging configuration for the IAS server on which the command is run. In the IAS console, this information is displayed in **Remote Access Logging**.
- **Remote access policies.** The **netsh aaa remote\_access\_policies** command dumps the remote access policies for the IAS server on which the command is run. In the IAS console, this information is displayed in **Remote Access Policies**.

- **Server settings.** The `netsh aaa show server_settings` command displays the configuration of server settings for the IAS server on which the command is run. These settings include server description, settings for accounting and authorization events in the system event log, ports used by IAS for RADIUS authentication and accounting requests, and registry keys and their values. In the IAS console, this information is displayed in server **Properties**.

When you use the `netsh aaa show remote_access_policies` command, the following registry keys and values are included:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\ControlProtocols\BuiltIn\DefaultDomain\REG\_SZ**

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Policy\Allow LM Authentication\REG\_DWORD**

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Policy\Default User Identity\REG\_SZ**

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Policy\User Identity Attribute\REG\_DWORD**

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Policy\Override User-Name\REG\_DWORD**

#### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **▶ To copy part of the IAS configuration by using a command line**

1. Open Command Prompt.
2. At the command prompt, type `netsh`, and then press ENTER.
3. At the netsh prompt, type `aaa`, and then press ENTER.
4. At the netsh aaa prompt, type `show command > path\file.txt`, and then press ENTER.

In the preceding command, **command** is **clients** (to export the RADIUS client configuration to a file), **connection\_request\_policies** (to export the connection request policy configuration to a file), **logging** (to export the logging configuration to a file), **remote\_access\_policies** (to export the remote access policy configuration to a file), or **server\_settings** (to export the IAS server configuration to a file).

This stores configuration settings (including registry settings) in a text file. The path can be relative or absolute, or it can be a UNC path.

5. Copy the file you created to the destination computer.
6. At a command prompt on the destination computer, type **netsh exec** *path\file.txt*, and then press ENTER.
7. A message appears indicating whether the update was successful.

## Export an IAS server configuration for import on another server

---

Use this procedure to copy an IAS server or proxy configuration to another IAS server or proxy.

This procedure allows you to replicate the entire IAS configuration from one IAS server to another IAS server, including remote access policy, connection request policy, registry, and logging configuration.

You do not need to stop IAS on the destination computer to run the netsh exec command. When the command is run, IAS is automatically refreshed with the updated configuration settings.

Because IAS configurations are not encrypted in the text file, sending it over a network might pose a security risk.

Do not use this procedure if the source IAS database is a higher version number than the version number of the destination IAS database. You can view the version number of the IAS database from the display of the **netsh aaa show config** command.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### To copy an IAS server configuration to another IAS server using Netsh commands for AAAA

1. On the source IAS server, open Command Prompt.
2. At the command prompt, type **netsh aaa show config >path\file.txt**, and then press ENTER. This stores configuration settings (including registry settings) in a

text file. The path can be relative or absolute, or it can be a UNC path.

3. Copy the file you created to the destination IAS server.
4. At a command prompt on the destination IAS server, type **netsh exec path\file.txt**, and then press ENTER. A message appears indicating whether the update was successful.

## Register an IAS server in another domain

---

Use this procedure to register an IAS server in another Active Directory domain.

To provide an IAS server with permission to read the dial-in properties of user accounts in Active Directory, the IAS server must be registered in the domain where the accounts reside.

You can use this procedure to register an IAS server in a domain where the IAS server is not installed.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

## To register an IAS server in another domain

You can perform this procedure by using the following methods:

- [Using the Windows interface](#)
- [Using Netsh commands for RAS](#)

### ▶ To register an IAS server in another domain by using the Windows interface

1. Open Active Directory Users and Computers.
2. In the console tree for the domain where you want the IAS server to read user account information, click the **Users** folder.
3. In the details pane, right-click **RAS and IAS Servers**, and then click **Properties**.

4. In the **RAS and IAS Servers Properties** dialog box, on the **Members** tab, add each of the IAS servers, and then click **OK**.

▶ **To register an IAS server in another domain by using Netsh commands for RAS**

1. Open **Command Prompt**.
2. Where *Domain* is the DNS domain name of the domain and *IAS\_server* is the name of the IAS server computer, type the following at the command prompt:  
**netsh ras add registeredserverDomainIAS\_server**, and then press ENTER.

## Register an IAS server in the default domain

---

Use this procedure to register an IAS server in the default Active Directory domain.

IAS servers must be registered in Active Directory so that they have permission to read the dial-in properties of user accounts during the authorization process. Registering an IAS server adds the server to the **RAS and IAS Servers** group in Active Directory.

You can use this procedure to register an IAS server in the domain where the server is installed.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

## To register an IAS server in the default domain

You can perform this procedure by using the following methods:

- [Using the Windows interface](#)
- [Using Netsh commands for RAS](#)

▶ **To register an IAS server in the default domain by using the Windows interface**

1. Open the IAS console.
2. Right-click **Internet Authentication Service**, and then click **Register Server in Active Directory**.
3. The **Register Internet Authentication Service in Active Directory** dialog box opens. Click **OK**.

▶ **To register an IAS server in the default domain by using Netsh commands for RAS**

1. Open **Command Prompt**.
2. Type `netsh ras add registeredserver`, and then press ENTER.

## Unregister an IAS server from the default domain

---

Use this procedure when you do not want the IAS server to be able to read user account properties in Active Directory.

In the process of managing your IAS server deployment, you might find it useful to move an IAS server to another domain, to replace an IAS server, or to retire an IAS server.

When you move or decommission an IAS server, you should unregister the IAS server in the Active Directory domains where the IAS server has permission to read the properties of user accounts in Active Directory.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins group.

## To unregister an IAS server from the default domain

You can perform this procedure using the following methods:

- [Using the Windows interface](#)
- [Using a command line](#)

### ▶ To unregister an IAS server using the Windows interface

1. Open Active Directory Users and Computers, click **Users**, and then double-click **RAS and IAS servers**.
2. Click the **Members** tab, and then select the IAS server that you want to unregister.
3. Click **Remove**, click **Yes**, and then click **OK**.

### ▶ To unregister an IAS server using a command-line

1. Open Command Prompt.
2. At the command prompt, type **netsh**.
3. At the netsh prompt, type **ras delete registeredserver *server***, where *server* is the computer name of the IAS server that you want to unregister. If you want to unregister the local computer, the *server* parameter is not required.

## Verify configuration after an IAS server IP address change

---

Use this procedure to verify that your IAS deployment is configured properly after changing the IP address of an IAS server or proxy.

There might be circumstances where you need to change the IP address of an IAS server or proxy, such as when you move the server to a different IP subnet.

If you change an IAS server or proxy IP address, it is necessary to reconfigure portions of your IAS deployment.

Use the following general guidelines to assist you in verifying that an IP address change does not interrupt network access authentication, authorization, or accounting on your network.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **▶ To verify configuration after an IAS server IP address change**

1. Reconfigure all RADIUS clients, such as wireless access points and VPN servers, with the new IP address of the IAS server.
2. If the IAS server is a member of a remote RADIUS server group, reconfigure the IAS proxy with the new IP address of the IAS server.
3. If you have configured the IAS server to use SQL Server logging, verify that connectivity between the computer running SQL Server 2000 and the IAS server is still functioning properly.
4. If you have deployed IPsec to secure RADIUS traffic between your IAS server and an IAS proxy or other servers or devices, reconfigure the IPsec policy to use the new IP address of the IAS server.
5. If the IAS server is multihomed and you have configured the server to bind to a specific network adapter, reconfigure IAS port settings with the new IP address.

#### **▶ To verify configuration after an IAS proxy IP address change**

1. Reconfigure all RADIUS clients, such as wireless access points and VPN servers, with the new IP address of the IAS proxy.
2. If the IAS proxy is multihomed and you have configured the proxy to bind to a specific network adapter, reconfigure IAS port settings with the new IP address.
3. Reconfigure all members of all remote RADIUS server groups with the proxy server IP address. To accomplish this task, at each IAS server that has the IAS proxy configured as a RADIUS client, configure the new IP address for the IAS proxy in **RADIUS clients** in the IAS console.
4. If you have configured the IAS proxy to use SQL Server logging, verify that connectivity between the computer running SQL Server 2000 and the IAS proxy is still functioning properly.

## Verify configuration after renaming an IAS server

---

Use this procedure to verify that your IAS deployment is configured properly after changing the name of an IAS server or proxy.

There might be circumstances where you need to change the name of an IAS server or proxy, such as when you redesign the naming conventions for your servers.

If you change an IAS server or proxy name, it is necessary to reconfigure portions of your IAS deployment.

Use the following general guidelines to assist you in verifying that a server name change does not interrupt network access authentication, authorization, or accounting on your network.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

### ▶ To verify configuration after an IAS server or proxy name change

1. If the IAS server is a member of a remote RADIUS server group and the group is configured with computer names rather than IP addresses, reconfigure the remote RADIUS server group with the new IAS server name.
2. If certificate-based authentication methods are deployed at the IAS server, the name change invalidates the server certificate. You can request a new certificate from the certification authority (CA) administrator or, if the computer is a domain member computer and you autoenroll certificates to domain members, you can refresh Group Policy to obtain a new certificate through autoenrollment.
3. After you have a new server certificate, request that the CA administrator revoke the old certificate.

After the old certificate is revoked, IAS will continue to use it until the old certificate expires. By default, the old certificate remains valid for a maximum time of one week and 10 hours. This time period might be different depending on whether the Certificate Revocation List (CRL) expiry and the Transport Layer Security (TLS) cache time expiry have been modified from their defaults. The

default CRL expiry is one week; the default TLS cache time expiry is 10 hours.

If you want to configure IAS to use the new certificate immediately, however, you can manually reconfigure remote access policies with the new certificate.

4. After the old certificate expires, IAS automatically begins using the new certificate.
5. If you have configured the IAS server to use SQL Server logging, verify that connectivity between the computer running SQL Server 2000 and the IAS server is still functioning properly.

## Managing certificates used with IAS

---

If you deploy a certificate-based authentication method, such as EAP-TLS or PEAP-MS-CHAP v2, you must enroll a server certificate to all of your IAS servers that meets the minimum certificate requirements and is issued by a trusted root certification authority (CA) that is trusted by client computers. The minimum certificate requirements are described in the section "Configure certificates for PEAP and EAP."

The following objectives assist in managing IAS server certificates in deployments where the trusted root CA is a third-party CA, such as Verisign, or a CA that you have deployed for your public key infrastructure (PKI) using Certificate Services in Windows Server 2003.

The following objectives are part of managing IAS server certificates:

- [Change the cached TLS handle expiry](#)
- [Configure certificates for PEAP and EAP](#)
- [Obtain the SHA-1 hash of a trusted root CA certificate](#)

## Change the cached TLS handle expiry

---

During the initial authentication processes for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS), and Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2),

the IAS server caches a portion of the connecting client's TLS connection properties. The client also caches a portion of the IAS server's TLS connection properties.

Each individual collection of these TLS connection properties is called a TLS handle.

Client computers can cache the TLS handles for multiple authenticators, while IAS servers can cache the TLS handles of many client computers.

The cached TLS handles on the client and server allows the reauthentication process to occur more rapidly. For example, when a wireless computer reauthenticates with an IAS server, the IAS server can examine the TLS handle for the wireless client and can quickly determine that the client connection is a reconnect. The IAS server authorizes the connection without performing full authentication.

Correspondingly, the client examines the TLS handle for the IAS server, determines that it is a reconnect, and does not need to perform server authentication.

On computers running Windows XP and Windows Server 2003, the default TLS handle expiry is 10 hours.

In some circumstances, you might want to increase or decrease the TLS handle expiry time.

An example of when you might want to decrease the TLS handle expiry time is in a scenario where a user's certificate is revoked by an administrator and the certificate has expired. In this scenario, the user can still connect to the network if an IAS server has a cached TLS handle that has not expired. Reducing the TLS handle expiry might help prevent such users with revoked certificates from reconnecting.

The best solution to this scenario is to disable the user account in Active Directory, or to remove the user account from the Active Directory group that is granted permission to connect to the network in remote access policy. The propagation of these changes to all domain controllers might also be delayed, however, due to replication latency.

Use the following tasks to configure the TLS handle expiry:

- [Configure the TLS handle expiry time on client computers](#)
- [Configure the TLS handle expiry time on IAS servers](#)

## Configure the TLS handle expiry time on client computers

---

Use this procedure to change the amount of time that client computers cache the Transport Layer Security (TLS) handle of an IAS server.

After successfully authenticating an IAS server, client computers cache TLS connection properties of the IAS server as a TLS handle. The TLS handle has a default duration of 10 hours (36,000,000 milliseconds). You can increase or decrease the TLS handle expiry time by using the following procedure.

This procedure must be performed on an IAS server, not on a client computer.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

### ▶ To configure the TLS handle expiry time on client computers by using the Windows interface

1. On an IAS server, open Registry Editor.
2. Browse to the registry key  
**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL**
3. On the **Edit** menu, click **New**, and then click **Key**.
4. Type **ClientCacheTime**, and then press ENTER.
5. Right-click **ClientCacheTime**, click **New**, and then click **DWORD Value**.
6. Type the amount of time, in milliseconds, that you want client computers to cache the TLS handle of IAS servers after the first successful authentication attempt by the IAS server.

## Configure the TLS handle expiry time on IAS servers

---

Use this procedure to change the amount of time that IAS servers cache the Transport Layer Security (TLS) handle of client computers.

After successfully authenticating an access client, IAS servers cache TLS connection properties of the client computer as a TLS handle. The TLS handle has a default duration of 10 hours (36,000,000 milliseconds). You can increase or decrease the TLS handle expiry time using the following procedure.

This procedure must be performed on an IAS server, not on a client computer.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **► To configure the TLS handle expiry time on IAS servers using the Windows interface**

1. On an IAS server, open Registry Editor.
2. Browse to the registry key  
**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL**
3. On the **Edit** menu, click **New**, and then click **Key**.
4. Type **ServerCacheTime**, and then press ENTER.
5. Right-click **ServerCacheTime**, click **New**, and then click **DWORD Value**.
6. Type the amount of time, in milliseconds, that you want IAS servers to cache the TLS handle of a client computer after the first successful authentication attempt by the client.

## **Configure certificates for PEAP and EAP**

---

When you use Extensible Authentication Protocol (EAP) with a strong EAP type —such as TLS with smart cards or certificates — both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements in order to allow the server and the client to use them for successful authentication.

One such requirement is that the certificate must be configured with one or more purposes that are specified in Enhanced Key Usage (EKU) extensions that correlate to the certificate use. For example, a certificate used for the authentication of a client to a server must be configured with the Client Authentication purpose. Similarly, a certificate used for the authentication of a server must be configured with the Server Authentication purpose. When certificates are used for authentication, the authenticator examines the

client certificate to find the correct purpose object identifier in its EKU extensions. For example, the object identifier for the Client Authentication purpose is 1.3.6.1.5.5.7.3.2.

You can customize certificates issued by Certificate Services, including both how certificates are issued and what they contain, by using Certificate Templates. In Certificate Templates, you can use a default template, such as the Computer template, to define the template that the CA uses to assign certificates to computers. You can also create a certificate template and assign purposes in EKU extensions to the certificate. By default, the Computer template includes the Client Authentication purpose and the Server Authentication purpose in EKU extensions.

The certificate template that you create can include any purpose for which the certificate will be used. For example, if you use smart cards for authentication, you can include the Smart Card Logon purpose in addition to the Client Authentication purpose.

When using IAS, you can configure IAS to check certificate purposes before granting network authorization. IAS can check additional EKUs and Issuance Policy purposes (also known as Certificate Policies).

Some non-Microsoft CA software might contain a purpose named All, which represents all possible purposes. This is indicated by a blank (or null) EKU extension. Although All means all possible purposes, the All purpose cannot be substituted for the Client Authentication purpose, the Server authentication purpose, or any other purpose related to network access authentication.

All certificates that are used for network access authentication must meet the requirements for X.509 certificates and work for connections that use Secure Sockets Layer-Transport Level Security (SSL/TLS). After this minimum requirement is met, both client and server certificates have additional requirements.

With EAP-TLS or PEAP-TLS, the server accepts the user or client authentication attempt when the user or computer certificate meets the following requirements:

- The user or computer certificate on the client is issued by an enterprise certification authority (CA) or is mapped to a user or computer account in Active Directory.
- The user or computer certificate on the client chains to a trusted root CA, includes the Client Authentication purpose in EKU extensions (the object identifier for Client Authentication is 1.3.6.1.5.5.7.3.2), and fails neither the checks that are performed by CryptoAPI nor the Certificate object identifier checks that are specified in IAS remote access policy.
- The registry-based certificates used by an 802.1X client are not smart card-logon or password-protected certificates.

- For user certificates, the Subject Alternative Name (SubjectAltName) extension in the certificate contains the user principal name (UPN).
- For computer certificates, the Subject Alternative Name (SubjectAltName) extension in the certificate must contain the client's fully qualified domain name (FQDN), which is also called the DNS name.

Clients can be configured to validate server certificates by using the **Validate server certificate** option. With PEAP-EAP-MS-CHAPv2, PEAP-EAP-TLS, or EAP-TLS as the authentication method, the client accepts the server's authentication attempt when the certificate meets the following requirements:

- The Subject name contains a value. If you issue a certificate to your IAS server that has a blank Subject, the certificate is not available to authenticate your IAS server.
- The computer certificate on the server chains to a trusted root CA and does not fail any of the checks that are performed by CryptoAPI and specified in the remote access policy.
- The IAS or VPN server computer certificate is configured with the Server Authentication purpose in EKU extensions (the object identifier for Server Authentication is 1.3.6.1.5.5.7.3.1).
- The server certificate is configured with a required cryptographic service provider (CSP) value of Microsoft RSA SChannel Cryptographic Provider.
- The Subject Alternative Name (SubjectAltName) extension, if used, must contain the DNS name of the server.

You can use the following tasks to configure certificates for PEAP and EAP:

- [Configure client computer certificates](#)
- [Configure client computers to authenticate IAS servers](#)
- [Configure server certificates](#)
- [Configure the ACL of the RAS and IAS Server certificate template](#)
- [Configure user certificates](#)

## Configure client computer certificates

---

Use this procedure to configure client certificates for use with PEAP and EAP.

With PEAP-TLS and EAP-TLS, clients display a list of all installed certificates in the Certificates snap-in, with the following exceptions:

- Wireless clients do not display registry-based and smart card-logon certificates.
- Wireless clients and VPN clients do not display password-protected certificates.
- Certificates that do not contain the Client Authentication purpose in EKU extensions are not displayed.

If you are running an enterprise certification authority (CA) on a computer running Windows Server 2003, Standard Edition, you can use the Computer certificate template for computer certificates.

If you are running an enterprise certification authority (CA) on a computer running any of the following operating systems, you can use the Workstation Authentication template for computer certificates:

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- The 64-bit version of Windows Server 2003, Enterprise Edition
- The 64-bit version of Windows Server 2003, Datacenter Edition

When you configure client computer certificates using this procedure, they meet the minimum client certificate requirements for PEAP-TLS and EAP-TLS.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **▶ To configure client computer certificates using the Windows interface**

1. On the computer running Certificate Services, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In **Available StandaloneSnap-ins**, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. Click **Certificate Templates**. In the **Certificate Templates** details pane, right-click the **Computer** or **Workstation Authentication** certificate template, and then click **Duplicate Template**.
5. In **Properties of New Template**, on the **General** tab, in **Template Display Name**, type a name for the template.
6. Select a **Validity period** and a **Renewal period**, or keep the defaults.

7. Click the **Subject Name** tab, and then verify that **Build from this Active Directory information** is selected.
8. For computer certificates, the Subject Alternative Name (SubjectAltName) extension in the certificate must contain the client's fully qualified domain name (FQDN), which is also called the DNS name. In **Include this information in alternate subject name**, select **DNS name**.
9. In **Subject name format**, select **Fully distinguished name**.
10. Click the **Extensions** tab. In **Extensions included in this template**, click **Application Policies**, and then click **Edit**.
11. In **Edit Application Policies Extension**, click **Server Authentication**, click **Remove**, and then click **OK**.
12. Use Certificate Services Help to learn how to configure autoenrollment of the client computer certificate to domain member client computers.
13. Use the CA Web Enrollment tool Help to learn how to manually enroll certificates to non-domain member client computers, if applicable to your deployment.

## Configure client computers to authenticate IAS servers

---

Use this procedure to configure client computers to authenticate IAS servers.

When you deploy certificate-based authentication methods that provide mutual authentication, client computers can authenticate IAS servers during the connection and authentication process. When you deploy authentication methods that provide mutual authentication, it is recommended that you configure clients to authenticate IAS servers. When clients are configured to authenticate IAS servers, clients are protected from connecting to unauthorized, or rogue, servers.

Certificate-based authentication methods that support mutual authentication are PEAP-TLS, PEAP-MS-CHAP v2, and EAP-TLS.

You can use this procedure to configure client computers to authenticate IAS servers when you deploy one of these authentication methods.

You can also configure the **Validate server certificate** option on domain member client computers by using Group Policy.

### Administrative credentials

To complete this procedure, you must be a member of the Administrators group on a client computer.

▶ **To configure client computers to authenticate IAS servers using the Windows interface**

1. Open **Network Connections**, right-click the network connection that you want to configure, and then click **Properties**.
2. In connection **Properties**, click the **Authentication** tab, and then click **Properties**.
3. In **Smart Card or other Certificate Properties**, click **Validate server certificate**.

## Configure server certificates

---

Use this procedure to configure IAS server certificates for use with PEAP and EAP.

With PEAP-MS-CHAP v2, PEAP-TLS, and EAP-TLS, servers display a list of all installed certificates in the computer's certificate store, with the following exceptions:

- Certificates that do not contain the Server Authentication purpose in EKU extensions are not displayed.
- Certificates that do not contain a Subject name are not displayed.
- Servers do not display registry-based and smart card-logon certificates.

If you are running an enterprise certification authority (CA) on a computer running Windows Server 2003, Standard Edition, you can use the Computer certificate template for server certificates.

If you are running an enterprise certification authority (CA) on a computer running any of the following operating systems, you can use the RAS and IAS Server template for server certificates:

- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition
- The 64-bit version of Windows Server 2003, Enterprise Edition

- The 64-bit version of Windows Server 2003, Datacenter Edition.

When you configure server computer certificates using this procedure, they meet the minimum server certificate requirements for PEAP-MS-CHAP v2, PEAP-TLS, and EAP-TLS. In some cases, the values indicated in this procedure are already selected in the template and you will not have to change settings when configuring the template.

If the forest or domain functional level of your network is Windows 2000 mixed, see [Configure the ACL of the RAS and IAS Server certificate template](#).

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### ▶ To configure server certificates using the Windows interface

1. On the server running Certificate Services, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In **Available StandaloneSnap-ins**, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. Click **Certificate Templates**. In the **Certificate Templates** details pane, right-click the **Computer** or **RAS and IAS Server** certificate template, and then click **Duplicate Template**.
5. In **Properties of New Template**, on the **General** tab, in **Template Display Name**, type a name for the template.
6. Select a **Validity period** and a **Renewal period**, or keep the defaults.
7. Click the **Subject Name** tab, and then verify that **Build from this Active Directory information** is selected.
8. In **Subject name format**, select a value other than **None**.
9. For server certificates, the Subject Alternative Name (SubjectAltName) extension in the certificate, if used, must contain the server's fully qualified domain name (FQDN), which is also called the DNS name. In **Include this information in alternate subject name**, select **DNS name**.
10. The server certificate must be configured with a required cryptographic service provider (CSP) value of **Microsoft RSA SChannel Cryptographic Provider**. To configure the CSP value, click the **Request Handling** tab, and then click **CSPs**.

11. In **CSP Selection**, select **Requests must use one of the following CSPs**.
12. In **CSPs**, select the **Microsoft RSA SChannel Cryptographic Provider** checkbox. Clear all other checkboxes in **CSPs**.
13. Use Certificate Services Help to learn how to configure autoenrollment of the server computer certificate to domain member server computers.
14. Use the CA Web Enrollment tool Help to learn how to manually enroll certificates to non-domain member server computers, if applicable to your deployment.

## Configure the ACL of the RAS and IAS Server certificate template

---

Use this procedure to configure the RAS and IAS Server certificate template in a Windows 2000 mixed domain where the IAS server is a member server and is not a domain controller.

If you have a Windows 2000 mixed domain where you have deployed Certificate Services on a computer running Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition and you want to use the RAS and IAS Server certificate template, you must configure the template for use.

When the domain functional level is Windows 2000 mixed, IAS servers do not carry the Security Identifier (SID) of the RAS and IAS servers certificate template on their tokens. Because of this, IAS servers cannot enroll a server certificate. Without a valid server certificate, connection requests using all certificate-based authentication methods (PEAP-TLS, PEAP-MS-CHAP v2, EAP-TLS) will fail, because the IAS server cannot be authenticated by clients connecting to the network.

If your server running IAS is not a domain controller but is a member of a domain with a Windows 2000 mixed functional level, you must add the server to the access control list (ACL) of the RAS and IAS Server certificate template. You must also configure the correct permissions for autoenrollment.

Do not perform this procedure unless all of the following are true:

- Your server running IAS is not a domain controller.
- Your server running IAS is a domain member.

- The domain to which the IAS server belongs has a Windows 2000 mixed functional level.

You can use the following two procedures for adding individual IAS servers to the ACL and for adding groups of IAS servers to the ACL.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **▶ To add an individual server to the ACL for the RAS and IAS Server certificate template using the Windows interface**

1. On the server running Certificate Services, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In **Available Standalone Snap-ins**, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. Click **Certificate Templates**. In the **Certificate Templates** details pane, right-click the **RAS and IAS Servers** template, and then click **Properties**.
5. In **RAS and IAS Server Properties**, click the **Security** tab, and then click **Add**.
6. In **Select Users, Computers, or Groups**, type the name of the IAS server that you want to add to the template Security properties, and then click **OK**.

#### **▶ To add multiple servers to the ACL for the RAS and IAS Server certificate template using the Windows interface**

1. In **Active Directory Users and Computers**, create a new global or universal group for IAS servers.
2. To the group you just created, add all computers that are IAS servers and members of a domain with a Windows 2000 mixed functional level, but that are not domain controllers.
3. Open **Certificate Templates**. In the **Certificate Templates** details pane, right-click the **RAS and IAS Servers** template, and then click **Properties**.
4. In **RAS and IAS Server Properties**, click the **Security** tab, and then click **Add**.
5. In **Select Users, Computers, or Groups**, type the name of the group that you want to add to the template Security properties, and then click **OK**.
6. In **RAS and IAS Server Properties**, in **Group or user names**, click the name of

the group you just added to the **Security** properties.

7. In **Permissions for Authenticated Users**, select the **Allow** check box to grant **Read, Enroll**, and **Autoenroll** permissions to the group.

## Configure user certificates

---

Use this procedure to configure user certificates for use with PEAP and EAP.

When you configure user certificates with this procedure, the certificates meet the minimum user certificate requirements for PEAP-TLS and EAP-TLS.

In Windows Server 2003, Standard Edition, you can autoenroll computer certificates and server certificates.

In Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition, you can also autoenroll user certificates.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### To configure user certificates using the Windows interface

1. On the computer running Certificate Services, click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. In **Available Standalone Snap-ins**, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. Click **Certificate Templates**. In the **Certificate Templates** details pane, right-click the **User** certificate template, and then click **Duplicate Template**.
5. In **Properties of New Template**, on the **General** tab, in **Template Display Name**, type a name for the template.
6. Select a **Validity period** and a **Renewal period**, or keep the defaults.
7. Click the **Subject Name** tab, and then verify that **Build from this Active Directory information** is selected.
8. In **Subject name format**, select **Fully distinguished name**.

9. For user certificates, the Subject Alternative Name (SubjectAltName) extension in the certificate must contain the user principal name (UPN). In **Include this information in alternate subject name**, select **User principal name (UPN)**.
10. Use Certificate Services Help to learn how to configure autoenrollment of the user certificate to domain users.

## Obtain the SHA-1 hash of a trusted root CA certificate

---

Use this procedure to obtain the Secure Hash Algorithm (SHA-1) hash of a trusted root certification authority (CA) from a certificate installed on the local computer.

In some circumstances, such as when deploying Group Policy or Wireless Provisioning Services (WPS) technology, it is necessary to designate a certificate using the SHA-1 hash of the certificate.

When using Group Policy or WPS technology, you can designate one or more trusted root CA certificates that clients must use in order to authenticate the IAS server certificate during the process of mutual authentication with EAP and PEAP. To designate a trusted root CA certificate that clients must use to validate the server certificate, you can enter the SHA-1 hash of the certificate.

This procedure demonstrates how to obtain the SHA-1 hash of a trusted root CA certificate using the Certificates snap-in.

### Administrative credentials

To complete this procedure, you must be a member of the Users group on the local computer.

#### To obtain the SHA-1 hash of a trusted root CA certificate using the Windows interface

1. Open the **Certificates** snap-in for the Local Computer certificate store.
2. In the left pane, double-click **Certificates(Local Computer)**, and then double-click the **Trusted Root Certification Authorities** folder.
3. The **Certificates** folder is a subfolder of the **Trusted Root Certification Authorities** folder. Click the **Certificates** folder.

4. In the details pane, browse to the certificate for your trusted root CA. Double-click the certificate. The **Certificate** dialog box opens.
5. In the **Certificate** dialog box, click the **Details** tab.
6. In the list of fields, select **Thumbprint**.
7. In the lower pane, the hexadecimal string that is the SHA-1 hash of your certificate is displayed. Select the SHA-1 hash and press the Windows keyboard shortcut for the Copy command (CTRL+C) to copy the hash to the Windows clipboard.
8. Open the location and place the cursor to which you want to paste the SHA-1 hash, and then press the Windows keyboard shortcut for the Paste command (CTRL+V).

## Managing RADIUS clients

---

You can configure any of the following types of RADIUS clients in IAS:

- Virtual Private Network (VPN) servers
- Wireless access points
- 802.1X authenticating switches
- Dial-up servers
- IAS proxies

To use IAS to manage network access, you must configure one or more RADIUS clients in IAS.

If you are configuring an IAS proxy as a RADIUS client on an IAS server, the IAS proxy must also be configured with RADIUS clients that forward connection requests to the proxy. The proxy forwards the connection request to a remote RADIUS server group based on the connection request processing rules defined on the proxy.

When you manage network access by configuring all of your network access servers as RADIUS clients in IAS, management of network access policy at all RADIUS clients is performed once in the IAS console rather than at each individual access server or proxy.

You can configure IAS in Windows Server 2003, Standard Edition, with a maximum of 50 RADIUS clients. You can define a RADIUS client by using a fully qualified domain name

or an IP address, but you cannot define groups of RADIUS clients by specifying an IP address range. If the fully qualified domain name of a RADIUS client resolves to multiple IP addresses, the IAS server uses the first IP address returned in the DNS query.

With IAS in Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, you can configure an unlimited number of RADIUS clients. In addition, you can configure RADIUS clients by specifying an IP address range. This allows you to add a large number of RADIUS clients (such as access points) to the IAS console at one time, rather than adding each RADIUS client individually.

The following objectives are part of managing RADIUS clients:

- [Set up RADIUS clients](#)
- [Set up RADIUS clients by IP address range](#)

## Set up RADIUS clients

---

When you add a new network access server (VPN server, wireless access point, authenticating switch, or dial-up server) to your network, you must add the server as a RADIUS client in IAS, and then configure the RADIUS client to communicate with the IAS server.

This step is also necessary when your IAS server is a member of a remote RADIUS server group configured on an IAS proxy. In this circumstance, you must configure the IAS proxy as a RADIUS client at the IAS server.

### Task requirements

The following are required to perform the procedures for this task:

- You must have at least one network access server (VPN server, wireless access point, authenticating switch, or dial-up server) or IAS proxy physically installed on your network.

To complete this task, perform the following procedures:

1. [Configure the network access server](#)
2. [Add the network access server as a RADIUS client in IAS](#)

## Configure the network access server

---

Use this procedure to configure network access servers for use with IAS.

When you deploy network access servers (NASs) as RADIUS clients, you must configure the clients to communicate with the IAS servers where the NASs are configured as clients.

This procedure provides general guidelines on the settings you should use to configure your NASs; for specific instructions on how to configure the device you are deploying on your network, see your NAS product documentation.

### To configure the network access server

1. In **RADIUS settings**, select **RADIUS authentication** on User Datagram Protocol (UDP) port **1812** and RADIUS accounting on UDP port **1813**.
2. In **Authentication server** or **RADIUS server**, specify your IAS server by IP address or fully qualified domain name (FQDN), depending on the requirements of the NAS.
3. In **Secret** or **Shared secret**, type a strong password. When you configure the NAS as a RADIUS client in IAS, you will use the same password, so do not forget it.
4. If you are using PEAP or EAP as an authentication method, configure the NAS to use EAP authentication.
5. If you are configuring a wireless access point, in SSID, specify a Service Set Identifier (SSID), which is an alphanumeric string that serves as the network name. This name is broadcast by access points to wireless clients and is visible to users at your Wi-Fi hotspots.
6. If you are configuring a wireless access point, in **802.1X and WEP**, enable IEEE 802.1X authentication if you want to deploy PEAP-MS-CHAP v2 or EAP-TLS.

## Add the network access server as a RADIUS client in IAS

---

Use this procedure to add a network access server as a RADIUS client in IAS.

You can use this procedure to configure a network access server (NAS) as a RADIUS client in the IAS console.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **▶ To add a network access server as a RADIUS client in IAS using the Windows interface**

1. Open the IAS console.
2. Right-click **RADIUS Clients**, and then click **New RADIUS Client**.
3. The New RADIUS Client Wizard opens. In **New RADIUS Client**, type a friendly name for the NAS, and then type the NAS IP address or fully qualified domain name (FQDN). If you enter the FQDN, click **Verify** if you want to verify that the name is correct and maps to a valid IP address. Click **Next**.
4. In **Client-Vendor**, specify the NAS manufacturer name. If you are not sure of the NAS manufacturer name, select **RADIUS standard**.
5. In **Shared secret**, type the strong password that is also entered on the NAS. Retype the shared secret in the confirmation text box.
6. If you are using any authentication methods other than EAP and PEAP, and if your NAS supports use of the message authenticator attribute, select **Request must contain the Message Authenticator attribute**.
7. Click **Finish**. Your NAS appears in the list of RADIUS clients configured at the IAS server.

## **Set up RADIUS clients by IP address range**

---

Use this procedure to configure two or more network access servers as RADIUS clients in IAS by using an IP address range.

If you are running Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, you can configure RADIUS clients by IP address range. This allows

you to add a large number of RADIUS clients (such as access points) to the IAS console at one time, rather than adding each RADIUS client individually.

You cannot configure RADIUS clients by IP address range if you are running IAS in Windows Server 2003, Standard Edition.

Use this procedure to add as RADIUS clients a group of network access servers (NASs) that are all configured with IP addresses from the same IP address range.

All of the RADIUS clients in the range must use the same configuration and shared secret.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **To set up RADIUS clients by IP address range using the Windows interface**

1. Open the IAS console.
2. Right-click **RADIUS Clients**, and then click **New RADIUS Client**.
3. The New RADIUS Client Wizard opens. In **New RADIUS Client**, type a friendly name for the collection of NASs.
4. In **Client address (IP or DNS)**, type the IP address range for the RADIUS clients using Classless Inter-Domain Routing (CIDR) notation. For example, if the IP address range for the NASs is 10.10.0.0, type **10.10.0.0/16**.
5. In **Client-Vendor**, specify the NAS manufacturer name. If you are not sure of the NAS manufacturer name, select **RADIUS standard**.
6. In **Shared secret**, type the strong password that is also entered on the NAS. Retype the shared secret in the confirmation text box.
7. If you are using any authentication methods other than EAP and PEAP, and if your NASs support use of the message authenticator attribute, select **Request must contain the Message Authenticator attribute**.
8. Click **Finish**. The NASs appear in the list of RADIUS clients configured at the IAS server.

## Managing remote access policies

---

This section provides information about how to manage IAS remote access policies in the Microsoft Windows Server 2003 and Windows Server 2003 with Service Pack 1 operating systems.

By using remote access policies in IAS you can define network access authorization rules that are applied to every connection request at network access servers that are configured as RADIUS clients on the IAS server.

After IAS authenticates users or computers connecting to your network, it performs authorization to determine whether the user or computer should be granted permission to connect.

Authorization is performed when IAS checks the dial-in properties of user accounts in Active Directory and when IAS evaluates the connection request against the remote access policies configured in the IAS console. These policies are evaluated in listed order from first to last. If there is a remote access policy that matches the connection request, IAS uses the policy to determine whether to grant or deny access to the user or computer connection.

For example, if you configure a remote access policy that grants network access permission to members of the Wireless group in Active Directory, Wireless group members are authorized to connect when they attempt to do so — assuming that all conditions of the remote access policy are matched by the connection attempt.

You can also specify connection restrictions in IAS remote access policy that are applied after the connection is authorized. For example, you can define IP filters for the connection that define the network resources to which the user has permission to connect.

When you configure multiple remote access policies in IAS, it is important to view the policies in overview as a collection of rules, and to ensure that rules created in one policy do not unintentionally counteract the rules in a different policy.

For example, a member of the Domain Users group might also be a member of the Wireless Users group that is created (by you or by another Administrator) in Active Directory. Perhaps your organization has limited wireless resources, so members of the Domain Users group are denied access when connecting through wireless access points; however, members of the Wireless Users group are granted access when connecting via wireless. If the remote access policy that denies wireless access to Domain Users is evaluated before the Wireless Users policy is evaluated, IAS denies access to members of the Wireless Users group when they attempt to connect via wireless - even though your intention is to grant them access.

The solution to this problem is to move the Wireless Users remote access policy higher in the list of policies in the IAS console so that it is evaluated before the Domain Users policy is evaluated. In this circumstance, when a member of the Wireless Users group attempts to connect, IAS evaluates the Wireless Users policy first and then authorizes the connection. When IAS receives a wireless connection attempt from a member of the Domain Users group that is not also a member of the Wireless Users group, the connection attempt does not match the Wireless Users policy, so that policy is not evaluated by IAS. Instead, IAS moves down to the Domain Users wireless policy - and denies the connection to the member of the Domain User group.

For simplicity of administration in domains with a Windows 2000 native or Windows Server 2003 domain functional level, it is recommended that all user accounts in Active Directory have the **Remote Access Permission (Dial-in or VPN)** option set to **Control access through Remote Access Policy**.

The following objectives are part of managing IAS remote access policies:

- [Configure IAS for VLANs](#)
- [Configure the EAP payload size](#)
- [Configure the Ignore-User-Dialin-Properties attribute](#)

## Configure IAS for VLANs

---

This section provides information about how to manage remote access policy for virtual local area networks (VLANs) in the Windows Server 2003 and Windows Server 2003 with Service Pack 1 operating systems.

By using VLAN-aware network access servers and Internet Authentication Service (IAS) in Windows Server 2003, you can provide groups of users with access only to the network resources that are appropriate for their security permissions. For example, you can provide visitors with wireless access to the Internet without allowing them access to your organization network.

In addition, VLANs allow you to logically group network resources that exist in different physical locations or on different physical subnets. For example, members of your sales department and their network resources, such as client computers, servers, and printers, might be located in several different buildings at your organization, but you can place all of these resources on one VLAN using the same IP address range. The VLAN then functions, from the end-user perspective, as a single subnet.

You can also use VLANs when you want to segregate a network between different groups of users. After you have determined how you want to define your groups, you can create security groups in Active Directory and add members to the groups.

Use the following procedure to configure a remote access policy using VLANs:

- [Configure a remote access policy for VLANs](#)

## Configure a remote access policy for VLANs

---

Use this procedure to configure a remote access policy that assigns users to a VLAN.

When you use VLAN-aware network hardware, such as routers, switches, and access controllers, you can configure remote access policy to instruct the access servers to place members of Active Directory groups on VLANs.

When you configure the profile of an IAS remote access policy for use with VLANs, you must configure the attributes Tunnel-Medium-Type, Tunnel-Pvt-Group-ID, Tunnel-Type, and Tunnel-Tag. This ability to group network resources logically with VLANs provides flexibility when designing and implementing network solutions.

You can use the following procedure to create a remote access policy that assigns users to a VLAN. This procedure is provided as a guideline; your network configuration might require different settings than those provided below.

### Administrative credentials

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

### ▶ To configure a remote access policy for VLANs using the Windows interface

1. Create a new remote access policy. In the IAS console, right-click **Remote Access Policies**, and then click **New Remote Access Policy**. Use the **New Remote Access Policy Wizard** to create a policy.
2. For **How do you want to set up this policy?** select **Use the wizard to set up a typical policy for a common scenario**.
3. In **Policy name**, type a name for your policy. For example, type **Sales policy**.
4. In **Select the method of access for which you want to create a policy**, select the appropriate type of access, such as **Wireless** or **Ethernet**.

5. In **Grant access based on the following**, click **Group**, and then click **Add**. In **Enter the object name to select**, type the name of a security group that you defined when configuring Active Directory. For example, if you created a group named **Sales**, type **Sales**, and then click **OK**.
6. In **Authentication Methods**, select the authentication method that you would like to enforce for users who will be placed on this VLAN. Your choices will differ based upon the access method you have chosen for the policy, such as **Wireless** or **VPN**. When you have completed configuring an authentication method, click **Finish**.
7. After you have completed creating the policy and have closed the wizard, you need to configure additional items for the remote access policy. In the IAS console, click **Remote Access Policies**, and then double-click the policy you just created.
8. In the policy **Properties** dialog box, for **Policy conditions**, click **Add**.
9. In **Attribute Types**, click **Day-And-Time-Restrictions**, and then click **Add**. In **Time of day restraints**, select **Permitted**, configure the days and times that access is permitted, and then click **OK**.
10. In the policy **Properties** dialog box, click **Grant remote access permission**.
11. Click **Edit Profile**, and then click the **Advanced** tab. By default, the Service-Type attribute appears in **Attributes** with a value of **Framed**. By default, for policies with access methods of VPN and dial-up, the Framed-Protocol attribute appears in **Attributes** with a value of **PPP**. To specify additional connection attributes required for VLANs, click **Add**, and then add the following attributes:
  - a. **Tunnel-Medium-Type**. Select a value appropriate to the previous selections you have made. For example, if the remote access policy you are configuring is a wireless policy, select **Value: 802 (Includes all 802 media plus Ethernet canonical format)**.
  - b. **Tunnel-Pvt-Group-ID**. Enter the integer that represents the VLAN number to which group members will be assigned.
  - c. **Tunnel-Type**. Select **Virtual LANs (VLAN)**.
  - d. **Tunnel-Tag**. Obtain this value from your hardware documentation.

## Configure the EAP payload size

---

In some cases, routers or firewalls drop packets because they are configured to discard packets that require fragmentation.

When you deploy IAS with remote access policies that use the Extensible Authentication Protocol (EAP) with Transport Layer Security (TLS), or EAP-TLS, as an authentication method, the default maximum transmission unit (MTU) that IAS uses for EAP payloads is 1500 bytes.

This maximum size for the EAP payload can create RADIUS messages that require fragmentation by a router or firewall between the IAS server and a RADIUS client. If this is the case, a router or firewall positioned between the RADIUS client and the IAS server might silently discard some fragments, resulting in authentication failure and the inability of the access client to connect to the network.

Use the following procedure to lower the maximum size that IAS uses for EAP payloads by adjusting the Framed-MTU attribute in the profile of a remote access policy to a value no greater than 1344:

- [Configure the Framed-MTU attribute](#)

## Configure the Framed-MTU attribute

---

Use this procedure to lower the maximum EAP payload size by using the Framed-MTU attribute in the profile of a remote access policy in IAS.

This procedure demonstrates how to lower the EAP payload size by configuring the Framed-MTU attribute in the profile of a remote access policy in the IAS console.

You should perform this procedure if you have routers or firewalls that are not capable of performing fragmentation.

The recommended Framed-MTU value in this circumstance is 1344 bytes or less.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

### **► To configure the Framed-MTU attribute using the Windows interface**

1. Open the IAS console.

2. Click **Remote Access Policies**, and in the details pane double-click the policy that you want to configure.
3. In the policy **Properties** dialog box, click **Edit Profile**.
4. In **Edit Dial-in Profile**, click the **Advanced** tab, and then click **Add**.
5. In **Attribute**, click **Framed-MTU**, and then click **Add**.
6. In **Attribute Value**, type a value equal to or less than **1344**, and then click **OK**.

## Configure the Ignore-User-Dialin-Properties attribute

---

Use this procedure to configure an IAS remote access policy to ignore the dial-in properties of user accounts in Active Directory.

User accounts in Active Directory have dial-in properties that IAS evaluates during the authorization process unless the **Remote Access Permission (Dial-in or VPN)** property of the user account is set to **Control access through Remote Access Policy**.

There are two circumstances where you might want to configure IAS to ignore the dial-in properties of user accounts in Active Directory:

- When you want to simplify IAS authorization by using remote access policy but not all of your user accounts have the remote access permission property set to **Control access through Remote Access Policy**. For example, some user accounts might have the **Remote Access Permission (Dial-in or VPN)** property of the user account set to **Deny access** or **Allow access**.
- When other dial-in properties of user accounts are not applicable to the connection type configured in the remote access policy. For example, properties other than the remote access permission setting are applicable only to dial-in or VPN connections, but the remote access policy you are creating is for wireless or authenticating switch connections.

You can use this procedure to configure a remote access policy with the Ignore-User-Dialin-Properties attribute. If a connection request matches the remote access policy where this attribute value is set to **True**, IAS does not use dial-in properties of the user account in Active Directory to determine whether the user or computer is authorized to

access the network; only the settings in the remote access policy are used to determine authorization.

### **Administrative credentials**

To complete this procedure, you must be a member of the Domain Admins or Enterprise Admins group.

#### **▶ To configure the Ignore-User-Dialin-Properties attribute using the Windows interface**

1. Open the IAS console.
2. In the console tree, click **Remote Access Policies**.
3. Right-click the policy for which you want to configure the attribute, and then click **Properties**.
4. Click **Edit Profile**, click the **Advanced** tab, and then click **Add**.
5. In the list of available RADIUS attributes, double-click the **Ignore-User-Dialin-Properties** attribute.
6. In **Boolean Attribute Information**, for **Select the attribute value**, click **True**, and then click **OK**.
7. Click **Close**, and then click **OK** twice to return to the IAS console.

## **Additional IAS Resources**

---

For general information about how IAS works, see the following resources:

- [IAS Technical Reference](http://go.microsoft.com/fwlink/?linkid=47247) at <http://go.microsoft.com/fwlink/?linkid=47247>
- [Windows Server 2003 Internet Authentication Service](http://go.microsoft.com/fwlink/?LinkId=20133) at <http://go.microsoft.com/fwlink/?LinkId=20133>
- [Deploying Internet Authentication Service \(IAS\)](http://go.microsoft.com/fwlink/?linkid=47246) at <http://go.microsoft.com/fwlink/?linkid=47246>
- [Deploying SQL Server Logging with Windows Server 2003 Internet Authentication Service \(IAS\)](http://go.microsoft.com/fwlink/?LinkId=41039) at <http://go.microsoft.com/fwlink/?LinkId=41039>
- [Deploying Windows Server 2003 Internet Authentication Service \(IAS\) with Virtual Local Area Networks \(VLANs\)](http://go.microsoft.com/fwlink/?LinkId=47291) at <http://go.microsoft.com/fwlink/?LinkId=47291>

For specific information about troubleshooting IAS problems, see the following resources:

- [IAS Troubleshooting](http://go.microsoft.com/fwlink/?LinkId=48831) at <http://go.microsoft.com/fwlink/?LinkId=48831>

For development information about IAS, see the following resources:

- [Internet Authentication Service Extensions](http://go.microsoft.com/fwlink/?LinkId=34431) at <http://go.microsoft.com/fwlink/?LinkId=34431>
- [Internet Authentication Service Reference](http://go.microsoft.com/fwlink/?LinkId=34429) at <http://go.microsoft.com/fwlink/?LinkId=34429>