



Operating System

Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows

Microsoft Corporation

Published: October 2003

Updated: October 2005

Abstract

This article describes how to deploy IEEE 802.1X authentication for wired networks using authenticating switches, wired client computers running Microsoft® Windows® XP, Windows Server™ 2003, or Windows 2000, and a wired authentication infrastructure consisting of Windows Server 2003 or Windows 2000 Active Directory® directory service domain controllers, certification authorities, and Internet Authentication Service servers.

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 document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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.

© 2003 Microsoft Corporation. All rights reserved.

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

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction.....	1
Wired Deployment Steps	4
Step 1: Configuring Active Directory for Accounts and Groups.....	4
Step 2: Configuring the Primary IAS Server	6
Step 2a: Configuring IAS.....	6
Step 2b: Configuring a Wired Remote Access Policy	9
Step 3: Configuring the Secondary IAS Server	11
Step 4: Deploying and Configuring Your Authenticating Switches	12
Step 5: Configuring Wired Client Computers for PEAP-MS-CHAP v2	13
Step 6: Configure a certificate infrastructure for EAP-TLS	14
Step 6a: Installing a Certificate Infrastructure	16
Step 6b: Installing Computer Certificates	17
Step 6c: Installing User Certificates	18
Step 7: Installing Computer Certificates on Wired Client Computers for EAP-TLS.....	20
Step 8: Installing User Certificates on Wired Client Computers for EAP-TLS	20
Floppy Disk-Based Installation	21
Step 9: Configuring Wired Client Computers for EAP-TLS	22
Step 10: Configuring Wired Client Computers for EAP-MD5 CHAP	23
Step 11: Verifying Wired Connections	23
Additional Intranet Wired Deployment Configurations	24
Internet Access for Business Partners.....	24
Using Guest Access	24
Using Validated Access.....	24
Using a Third-Party CA.....	25
Certificates on IAS Servers	25
Certificates on Wired Client Computers	26
Cross-Forest Authentication	26
Configuring the Active Directory Forests for Accounts and Groups.....	28
Configuring the Primary IAS Server on a Computer in the First Forest.....	28
Configuring the Secondary IAS Server on Another Computer in the First Forest	29

Configuring the Primary IAS Server on a Computer in the Second Forest.....	29
Configuring the Secondary IAS Server on Another Computer in the Second Forest	29
Configuring the Primary IAS RADIUS Proxy	30
Configuring the Secondary IAS RADIUS Proxy	30
Configuring RADIUS Authentication and Accounting on the Authenticating Switches	30
Using RADIUS Proxies to Scale Authentications	31
Configuring Active Directory for User Accounts and Groups	32
Configuring IAS as a RADIUS Server on Multiple Computers.....	32
Configuring the Primary IAS RADIUS Proxy	33
Configuring the Secondary IAS RADIUS Proxy	33
Configuring RADIUS Authentication and Accounting on the Authenticating Switches	33
Using Computer-only Authentication	34
Summary	35
Related Links	36

Introduction

This article describes how to create an infrastructure for authentication, authorization, and accounting of 802.1X-authenticated wired connections to an organization using Windows wired clients. The configuration described in this article uses the following:

- Wired client computers running Windows.

Windows XP and Windows Server 2003 have built-in support for IEEE 802.1X authentication using the Extensible Authentication Protocol (EAP). Windows 2000 supports IEEE 802.1X authentication when [Windows 2000 Service Pack 4 \(SP4\)](#) is installed.

- At least two Internet Authentication Service (IAS) servers.

At least two IAS servers (one primary and one secondary) are used to provide fault tolerance for Remote Authentication Dial-In User Service (RADIUS)-based authentication. If only one RADIUS server is configured and it becomes unavailable, wired clients cannot connect. By using two IAS servers and configuring all authenticating switches (the RADIUS clients) for both the primary and secondary IAS servers, the RADIUS clients can detect when the primary RADIUS server is unavailable and automatically fail over to the secondary IAS server.

You can use either Windows Server 2003 or Windows 2000 Server IAS. IAS servers running Windows 2000 must have SP4 installed. IAS is not included with Windows Server 2003, Web Edition.

- Active Directory service domains.

Active Directory domains contain the user accounts, computer accounts, and dial-in properties that each IAS server requires to authenticate credentials and evaluate authorization. While not a requirement, to both optimize IAS authentication and authorization response times and minimize network traffic, IAS should be installed on Active Directory domain controllers.

You can use either Windows Server 2003 or Windows 2000 Server domain controllers. Windows 2000 domain controllers must have SP4 or later installed.

- Computer certificates installed on the IAS servers.

Depending on the wired authentication method you use, you must install computer certificates on the IAS servers.

- For EAP-TLS authentication, a certificate infrastructure.

When the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication protocol is used with computer and user certificates on wired clients, a certificate infrastructure, also known as a public key infrastructure (PKI), is needed to issue certificates.

- For Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) authentication, root certification authority (CA) certificates on each wired client.

PEAP-MS-CHAP v2 is a password-based authentication method for wired connections. Depending on the issuer of the IAS server computer certificates, you might also have to install root CA certificates on each wired client.

- Wired access remote access policy.

A remote access policy is configured for wired connections so that employees can access the organization intranet.

- Multiple authenticating switches.

Multiple third-party authenticating switches provide wired access in different buildings of an organization. The authenticating switches must support IEEE 802.1X and RADIUS. Not all network switches are authenticating switches. You might have to either replace or upgrade your existing switches.

Figure 1 shows a typical wired configuration.

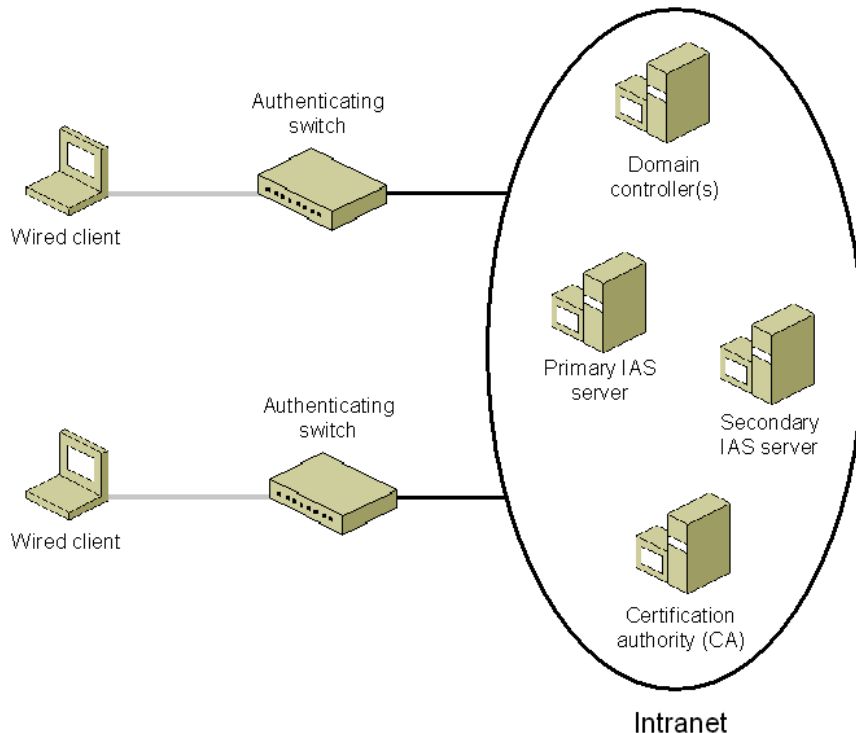


Figure 1 Typical wired configuration

The configuration is very similar to the authentication infrastructure for secure wireless access and both types of network access can use the same authentication infrastructure.

For background information about 802.1X, EAP, RADIUS, and certificates, see the article "[Windows XP Wireless Deployment Technology and Component Overview](http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.mspx)" at <http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.mspx>.

With wired connections, you have your choice of the following authentication methods:

- PEAP-MS-CHAP v2, which uses password-based credentials and requires computer certificates on the IAS servers.
- EAP-TLS, which uses certificate-based credentials and requires user and computer certificates on the wired client computers and computer certificates on the IAS servers.

- EAP-Message Digest 5 Challenge Handshake Authentication Protocol (MD5 CHAP), which uses passwords.

Wired Deployment Steps

For this configuration, complete the following steps:

1. Configure Active Directory for accounts and groups.
2. Configure the primary IAS server on a computer.
3. Configure the secondary IAS server on another computer.
4. Deploy and configure your authenticating switches.
5. Configure wired client computers for PEAP-MS-CHAP v2.
6. Configure a certificate infrastructure for EAP-TLS.
7. Install computer certificates on wired client computers (EAP-TLS).
8. Install user certificates on wired client computers (EAP-TLS).
9. Configure wired client computers for EAP-TLS.
10. Configure wired client computers for EAP-MD5 CHAP.
11. Verify wired connections.

Note There is currently no support for Group Policy-based configuration of wired client 802.1X authentication settings. The Wireless Network (IEEE 802.11) Policies Group Policy settings are for wireless network connections only.

Step 1: Configuring Active Directory for Accounts and Groups

To configure Active Directory user and computer accounts and groups for wired access, do the following:

1. If you are using Windows 2000 domain controllers, install Windows 2000 SP4 or later on all domain controllers.
2. Ensure that all users that are making wired connections have a corresponding user account.
3. Ensure that all computers that are making wired connections have a corresponding computer account.
4. Set the remote access permission on user and computer accounts to the appropriate setting (either **Allow access** or **Control access through Remote Access Policy**). The remote access permission setting is on the **Dial-in** tab on the properties of a user or computer account in the Active Directory Users and Computers snap-in.
5. Organize your wired access user and computer accounts into the appropriate groups. For a native-mode domain, you can use universal and nested global groups. For example, create a universal group named WiredUsers that contains global groups of wired user and computer accounts for intranet access.

Best Practice Use a native-mode domain and universal groups and global groups to organize your wired accounts into a single group.

If you are using EAP-MD5 CHAP authentication, then you must do the following:

- Enable storage of a reversibly encrypted form of the account's password in your domains.

To verify the challenge response sent from the wired client, the RADIUS server must use the plain-text version of the password. By default, Windows domains store a one-way encrypted form of the account password. Therefore, Windows domains must be configured to store a version of the password using two-way (reversible) encryption. The account password is stored in an encrypted form. When authenticating, the account password is converted to its plain-text form using reversible encryption.

- Force a reset of the account passwords so that the new passwords are stored in a reversibly encrypted form.

When you enable passwords to be stored in a reversibly encrypted form, the current passwords are not in a reversibly encrypted form and are not automatically changed. Because you cannot change passwords using EAP-MD5 CHAP, you must reset user account passwords and then communicate those new passwords to the entities using those accounts, rather than setting account passwords to be changed the next time each account logs on. This is described in the "To reset a user account password" procedure in this section.

For the passwords of computer accounts, you must wait until the computers change their passwords before requiring authentication for wired connections. By default, computer account passwords are automatically changed every 30 days. You can wait 30 days after enabling the storage of reversibly encrypted passwords before requiring authentication for wired connections, or you can set the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge (REG_DWORD data type) to the number of days within which you want the computers to reset their passwords. After that number of days has passed, you can then require authentication for wired connections.

❑ To enable reversibly encrypted passwords in a domain

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click **Active Directory Users and Computers**, right-click the domain name, and then click **Properties**.
3. On the **Group Policy** tab, click **Default Domain Policy** or the appropriate Group Policy object, and then click **Edit**.
4. In the console tree, open **Computer Configuration, Windows Settings, Security Settings, Account Policies**, and then click **Password Policy**.
5. In the details pane, double-click **Store passwords using reversible encryption for all users in the domain**.
6. Click **Enabled**, and then click **OK**.

Perform this procedure for each domain system container as appropriate.

❑ To reset a user account password

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, double-click **Active Directory Users and Computers**, and then open the

domain system container that contains the user accounts whose passwords you want to reset.

3. In the details pane, right-click the user account whose password you want to reset, and then click **Reset Password**.
4. Type and confirm the password.

Because of the additional overhead associated with managing account passwords and settings for EAP-MD5 CHAP, the use of PEAP-MS-CHAP v2 or EAP-TLS is recommended.

Step 2: Configuring the Primary IAS Server

Configuring the primary IAS server on a computer involves the following:

- Configuring IAS to be able to access account information, logging, UDP ports, and for the RADIUS clients corresponding to the authenticating switches.
- Configuring a remote access policy for wired access.

Step 2a: Configuring IAS

To configure the primary IAS server on a computer, do the following:

1. If you are using computer certificate autoenrollment and Windows 2000 IAS, force a refresh of computer Group Policy by typing **secedit /refreshpolicy machine_policy** from a command prompt. If you are using computer certificate autoenrollment and Windows Server 2003 IAS, force a refresh of computer Group Policy by typing **gpupdate /target:computer** from a command prompt.
2. If you are using PEAP-MS-CHAP v2 authentication and have obtained a computer certificate from a commercial CA, use the Certificates snap-in to import it into the Certificates (Local Computer)\Personal\Certificates folder. To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. It is also possible to import a certificate by double-clicking a certificate file that is stored in a folder or sent in an email message. Although this works for certificates created with Windows CAs, this method does not work for third-party CAs. The recommended method of importing certificates is to use the Certificates snap-in.
3. Install IAS as an optional networking component.
4. If you are using Windows 2000 IAS, install Windows 2000 SP4 or later.
5. The primary IAS server computer must be able to access account properties in the appropriate domains. If IAS is being installed on a domain controller, no additional configuration is required in order for IAS to access account properties in the domain of the domain controller.

If IAS is not installed on a domain controller, you must configure the primary IAS server computer to read the properties of user accounts in the domain. For more information, see the "Enable the IAS server to read user accounts in Active Directory" procedure in this section.

If the IAS server authenticates and authorizes wired connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the IAS server computer is a member. Next, configure the IAS server computer to read the properties of user accounts in other domains. For more information, see the "Enable the IAS server to read user objects in Active Directory" procedure in this section.

If there are accounts in other domains, and those domains do not have a two-way trust with the domain in which the IAS server computer is a member, you must configure a RADIUS proxy between the two untrusted domains. If there are accounts in other Active Directory forests, you must configure a RADIUS proxy between the forests. For more information, see “Cross-Forest Authentication” in this article.

6. If you want to store authentication and accounting information for connection analysis and security investigation purposes, enable logging for accounting and authentication events. Windows 2000 IAS can log information to a local file. Windows Server 2003 IAS can log information to a local file and to a Structured Query Language (SQL) server database. For more information, see the topic titled "Configure log file properties" in Windows 2000 Help and the topic titled "Configure logging for user authentication and accounting" in Windows Server 2003 Help and Support.
7. If needed, configure additional UDP ports for authentication and accounting messages that are sent by RADIUS clients (the authenticating switches). For more information, see the "Configure IAS port information" procedure in this section. By default, IAS uses UDP ports 1812 and 1645 for authentication messages and UDP ports 1813 and 1646 for accounting messages.
8. Add the authenticating switches as RADIUS clients of the IAS server. For more information, see the "Add RADIUS clients" procedure in this section. Verify that you are configuring the correct name or IP address and shared secret for each authenticating switch.

Use a different shared secret for each authenticating switch. Each shared secret should be a random sequence of upper and lowercase letters, numbers, and punctuation that is at least 22 characters long. To ensure randomness, use a random character generation program to create shared secrets to configure on the IAS server and the authenticating switch.

To ensure the maximum security for RADIUS messages, it is recommended that you use Internet Protocol security (IPSec) Encapsulating Security Payload (ESP) with certificate authentication to provide data confidentiality, data integrity, and data origin authentication for RADIUS traffic sent between the IAS servers and the authenticating switches. Windows 2000 and Windows Server 2003 support IPSec. The authenticating switches must also support IPSec.

❑ **Enable the IAS server to read user accounts in Active Directory**

To register the IAS server in the default domain using Internet Authentication Service:

1. Log on to the IAS server with an account that has domain administrator permissions.
2. Open the Internet Authentication Service snap-in.
3. Right-click Internet Authentication Service, and then click **Register Server in Active Directory**.
When the **Register Internet Authentication Service in Active Directory** dialog box appears, click **OK**.

To register the IAS server in the default domain using the Netsh tool:

1. Log on to the IAS server with an account that has domain administrator permissions.
2. Open a command prompt.
3. At the command prompt, type: **netsh ras add registeredserver**

To register the IAS server in the default domain using Active Directory Users and Computers:

1. Log on to the IAS server with an account that has domain administrator permissions.
2. Open the Active Directory Users and Computers snap-in.
3. In the console tree, click the **Users** folder in the appropriate domain.
4. In the details pane, right-click **RAS and IAS Servers**, and then click **Properties**.
5. In the **RAS and IAS Servers Properties** dialog box, on the **Members** tab, add the IAS server.

To register the IAS server in another domain using Active Directory Users and Computers:

1. Log on to the IAS server with an account that has domain administrator permissions.
2. Open the Active Directory Users and Computers snap-in.
3. In the console tree, click the **Users** folder in the appropriate domain.
4. In the details pane, right-click **RAS and IAS Servers**, and then click **Properties**.
5. In the **RAS and IAS Servers Properties** dialog box, on the **Members** tab, add each of the appropriate IAS servers.

To register the IAS server in another domain using the Netsh tool:

1. Log on to the IAS server with an account that has domain administrator permissions.
2. Open a command prompt.
3. At the command prompt, type **netsh ras add registeredserver Domain IASServer** in which *Domain* is the DNS domain name of the domain and *IASServer* is the name of the IAS server computer.

❑ **Configure IAS port information**

1. Open the Internet Authentication Service snap-in.
2. Right-click **Internet Authentication Service**, and then click **Properties**.
3. For Windows 2000 IAS, click the **RADIUS** tab. For Windows Server 2003, click the **Ports** tab. Examine the settings for ports. If your RADIUS authentication and RADIUS accounting UDP ports differ from the default values provided (1812 and 1645 for authentication and 1813 and 1646 for accounting), in **Authentication** and **Accounting**, type your port settings.

To use multiple ports for authentication or accounting requests, separate the ports with commas.

❑ **Add RADIUS clients**

1. Open the Internet Authentication Service snap-in.
2. For Windows 2000 IAS, in the console tree, right-click **Clients**, and then click **New Client**. For Windows Server 2003 IAS, in the console tree, right-click **RADIUS Clients**, and then click **New RADIUS Client**.
3. In **Friendly name**, type a descriptive name.
4. In **Protocol**, click **RADIUS**, and then click **Next**.
5. In **Client address (IP or DNS)**, type the DNS name or IP address for the client. If you are using a DNS name, click **Verify**. In the **Resolve DNS Name** dialog box, click **Resolve**, and then select the IP address you want to associate with that name from **Search Results**.

6. If you are planning to use authenticating switch-specific remote access policies for configuration purposes (for example, a remote access policy that contains vendor-specific attributes), click **Client Vendor**, and select the manufacturer's name. If you do not know the manufacturer or it is not in the list, click **RADIUS Standard**.
7. In **Shared secret**, type the shared secret for the client, and then type it again in **Confirm shared secret**.
8. Click **Finish**.

Best Practices If possible, use IPSec ESP to provide data confidentiality for RADIUS traffic between the authenticating switch and the IAS servers. Use at least 3DES encryption and, if possible, certificates for Internet Key Exchange (IKE) main mode authentication. For information about configuring IPSec for the IAS servers, see IPSec Help in Windows 2000 or Windows Server 2003. For information about configuring IPSec for the authenticating switches, see the documentation provided with the switch.

Use shared secrets that consist of a random sequence of upper and lower case letters, numbers, and punctuation at least 22 characters long and use a different shared secret for each authenticating switch. If possible, use a random string-generating computer program to create the shared secret.

Step 2b: Configuring a Wired Remote Access Policy

To configure a wired remote access policy for the primary IAS server, do the following:

1. For Windows 2000 IAS, create a new remote access policy for wired intranet access with the following settings:

Policy name: Wired access to intranet (example)

Conditions: NAS-Port-Type=Ethernet, Windows-Groups=WiredUsers

Permissions: Select **Grant remote access permission**.

Profile, **Authentication** tab: If you are using PEAP-MS-CHAP v2 authentication, select **Extensible Authentication Protocol** and the **Protected EAP (PEAP)** EAP type, and then click **Configure**. In the **Protected EAP Properties** dialog box, select the appropriate computer certificate and ensure that **Secured password (EAP-MSCHAP v2)** is selected as the EAP type.

If you are using EAP-TLS authentication, select **Extensible Authentication Protocol** and the **Smart Card or other Certificate** EAP type. Clear all other check boxes. If you have multiple computer certificates installed on the IAS server, click **Configure**, and then select the appropriate computer certificate. If the intended computer certificate is not displayed, then the certificate does not support the Microsoft RSA SChannel Provider.

If you are using EAP-MD5 CHAP authentication, select **Extensible Authentication Protocol** and the **MD5 Challenge** EAP type. Clear all other check boxes.

Profile, **Encryption** tab: Select all check boxes. The settings on the **Encryption** tab correspond to the MS-MPPE-Encryption-Policy and MS-MPPE-Encryption-Types RADIUS attributes and might be supported by the authenticating switch. If these attributes are not supported, clear all the check boxes except **No encryption**.

For more information, see the "Add a remote access policy" procedure in this section.

2. For Windows Server 2003 IAS, use the New Remote Access Policy Wizard to create a common remote access policy with the following settings:
 - Policy name: Wired access to intranet (example)
 - Access Method: Ethernet
 - User or Group Access: Group with the WiredUsers group selected (example group name)
 - Authentication Methods: **Protected EAP (PEAP)** type (for EAP-MS-CHAP v2), **Smart Card or other Certificate** type (for EAP-TLS), or **MD-5 Challenge** type (for EAP-MD5 CHAP)
3. If the authenticating switches require vendor specific attributes (VSAs), you must add the VSAs to the remote access policy. For more information, see the "Configure vendor-specific attributes for a remote access policy" procedure in this section.
4. For Windows 2000 IAS, delete the default remote access policy named **Allow access if dial-in permission is enabled**. To delete a remote access policy, right-click the policy name in the Internet Authentication Service snap-in and click **Delete**.

Best Practice If you are managing the remote access permission of user and computer accounts on a per-account basis, use remote access policies that specify a connection type. If you are managing the remote access permission through the remote access policy, use remote access policies that specify a connection type and group. The recommended method is to manage remote access permission through the remote access policy.

❑ **Add a remote access policy**

1. Open the Internet Authentication Service snap-in.
2. In the console tree, right-click **Remote Access Policies**, and then click **New Remote Access Policy**.

❑ **Configure vendor-specific attributes for a remote access policy**

1. Open the Internet Authentication Service snap-in.
2. In the console tree, click **Remote Access Policies**.
3. In the details pane, double-click the policy for which you want to configure a vendor-specific attribute (VSA).
4. Click **Edit Profile**, click the **Advanced** tab, and then click **Add**.
5. Look at the list to see whether your vendor-specific attribute is already in the list of available RADIUS attributes. If it is, double-click it, and then configure it as specified in your authenticating switch documentation.
6. If the vendor-specific attribute is not in the list of available RADIUS attributes, click the **Vendor-Specific** attribute, and then click **Add**.
7. In the **Multivalued Attribute Information** dialog box, click **Add**.
8. Specify the vendor for your authenticating switch. To specify the vendor by selecting the name from the list, click **Select from list**, and then select the vendor of the authenticating switch for which you are configuring the VSA. If the vendor is not listed, specify the vendor by typing the vendor code.
9. To specify the vendor by typing the vendor code, click **Enter Vendor Code** and then type the vendor

code in the space provided. See RFC 1007 for a list of SMI Network Management Private Enterprise Codes.

10. Specify whether the attribute conforms to the VSA format specified in RFC 2865. If you are not sure, see your authenticating switch documentation.
11. If your attribute conforms, click **Yes. It conforms**, and then click **Configure Attribute**. In **Vendor-assigned attribute number**, type the number assigned to the attribute (this should be an integer from 0 to 255). In **Attribute format**, specify the format for the attribute, and then in **Attribute value**, type the value you are assigning to the attribute.
12. If the attribute does not conform, click **No. It does not conform**, and then click **Configure Attribute**. In **Hexadecimal attribute value**, type the value for the attribute.

Best Practice Investigate whether the authenticating switches need VSAs and configure them during the configuration of the remote access policy. If you configure the VSAs after you configure the authenticating switches, you have to re-synchronize the configuration of the primary IAS server to the secondary IAS server.

Step 3: Configuring the Secondary IAS Server

To configure the secondary IAS server on another computer, do the following:

1. If you are using computer certificate autoenrollment and Windows 2000 IAS, force a refresh of computer Group Policy by typing **secedit /refreshpolicy machine_policy** from a command prompt. If you are using computer certificate autoenrollment and Windows Server 2003 IAS, force a refresh of computer Group Policy by typing **gpupdate /target:computer** from a command prompt.
2. If you are using PEAP-MS-CHAP v2 authentication and have obtained a computer certificate from a commercial CA, use the Certificates snap-in to import it into the Certificates (Local Computer)\Personal\Certificates folder.
3. Install IAS as an optional networking component.
4. If you are using Windows 2000 IAS, install Windows 2000 SP4 or later.
5. The secondary IAS server computer must be able to access account properties in the appropriate domains. If IAS is being installed on a domain controller, no additional configuration is required in order for IAS to access account properties in the domain of the domain controller.

If IAS is not installed on a domain controller, you must configure the secondary IAS server computer to read the properties of user accounts in the domain. For more information, see the "Enable the IAS server to read user accounts in Active Directory" procedure previously described.

If the secondary IAS server authenticates and authorizes connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the secondary IAS server computer is a member. Next, configure the secondary IAS server computer to read the properties of user accounts in other domains. For more information, see the "Enable the IAS server to read user objects in Active Directory" procedure previously described.

If there are accounts in other domains, and those domains do not have a two-way trust with the domain in which the secondary IAS server computer is a member, you must configure a RADIUS proxy between the two untrusted domains. If there are accounts in other Active Directory forests, you

must configure a RADIUS proxy between the forests. For more information, see "Cross-Forest Authentication" in this article.

6. To copy the configuration of the primary IAS server to the secondary IAS server, type **netsh aaa show config > path\file.txt** at a command prompt on the primary IAS server. This stores the configuration settings, including registry settings, in a text file. The path can be relative, absolute, or a network path.
7. Copy the file created in step 7 to the secondary IAS server. At a command prompt on the secondary IAS server, type **netsh exec path\file.txt**. This command imports all the settings configured on the primary IAS server to the secondary IAS server.

Note You cannot copy the IAS settings from an IAS server running Windows Server 2003 to an IAS server running Windows 2000 Server.

Best Practice If you change the IAS server configuration in any way, use the Internet Authentication Service snap-in to change the configuration of the primary IAS server and then use steps 7 and 8 in the previous procedure to synchronize those changes on the secondary IAS server.

Step 4: Deploying and Configuring Your Authenticating Switches

Deploy your authenticating switches to provide network access for your wired network. Configure your authenticating switches to support 802.1X authentication and RADIUS. Configure the RADIUS settings on your authenticating switches with the following:

1. The IP address or name of a primary RADIUS server, the shared secret, UDP ports for authentication and accounting, and failure detection settings.
2. The IP address or name of a secondary RADIUS server, the shared secret, UDP ports for authentication and accounting, and failure detection settings.

To balance the load of RADIUS traffic between the two IAS servers, configure half of the authenticating switches with the primary IAS server as the primary RADIUS server and the secondary IAS server as the secondary RADIUS server and the other half of the authenticating switches with the secondary IAS server as the primary RADIUS server and the primary IAS server as the secondary RADIUS server.

For more information, see the documentation for the authenticating switch. For information about Cisco switches, see the [Cisco Switches Web page](http://www.cisco.com/en/US/products/hw/switches/index.html) at <http://www.cisco.com/en/US/products/hw/switches/index.html>. For information about configuring Foundry Networks authenticating switches, see the [802.1X Port Authentication with Microsoft's Active Directory white paper](http://www.foundry.com/solutions/appNotes/8021xportAuth.html) at <http://www.foundry.com/solutions/appNotes/8021xportAuth.html>. For information about 3COM switches, see [3COM Switches \(Workgroup/Desktop\) Web page](http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=4&selcat=LAN+Switches+%28Workgroup%2FDesktop%29) at http://www.3com.com/products/en_US/prodlist.jsp?tab=cat&pathtype=purchase&cat=4&selcat=LAN+Switches+%28Workgroup%2FDesktop%29.

If the authenticating switches require vendor specific attributes (VSAs), you must add the VSAs to the remote access policies of the IAS servers. For more information, see the "Configure vendor-specific attributes for a remote access policy" procedure previously described. If you add VSAs to the remote

access policy on the primary IAS server, perform steps 7 and 8 of the “Step 4: Configuring the secondary IAS server” section to copy the primary IAS server configuration to the secondary IAS server.

Step 5: Configuring Wired Client Computers for PEAP-MS-CHAP v2

To manually configure PEAP-MS-CHAP v2 authentication on a wired client running Windows XP with SP2, Windows XP with SP1, or Windows Server 2003, do the following:

1. Obtain properties of the connection in the Network Connections folder.
2. Click the **Authentication** tab and select **Enable network access control using IEEE 802.1X** and the **Protected EAP** EAP type.
3. Click **Properties**. In the **Protected EAP Properties** dialog box, select **Validate server certificate** to validate the computer certificate of the IAS server (enabled by default). If you want to specify the names of the authentication servers that must perform validation, select **Connect to these servers** and type the names. In **Select Authentication Method**, click **Secured password (EAP-MSCHAP v2)**.

To configure PEAP-MS-CHAP v2 authentication on a wired client running Windows 2000 and Windows SP4, do the following:

1. Obtain properties of the connection in the Dial-up and Network Connections folder.
2. Click the **Authentication** tab and select **Enable network access control using IEEE 802.1X** and the **Protected EAP** EAP type.
3. Click **Properties**. In the **Protected EAP Properties** dialog box, select **Validate server certificate** to validate the computer certificate of the IAS server (enabled by default). If you want to specify the names of the authentication servers that must perform validation, select **Connect to these servers** and type the names. In **Select Authentication Method**, click **Secured password (EAP-MSCHAP v2)**.

Notes By default, the PEAP-MS-CHAP v2 authentication uses your Windows logon credentials for authentication. If you are connecting to a wired network that uses PEAP-MS-CHAP v2 and you want to specify different credentials, click **Configure** and clear the **Automatically use my Windows logon name and password** check box.

Although the **Protected EAP Properties** dialog box for Windows XP with SP2, Windows XP with SP1, Windows Server 2003, and Windows 2000 with SP4 has an **Enable Fast Reconnect** check box, IAS in Windows 2000 does not support fast reconnect. IAS in Windows Server 2003 does support fast reconnect.

If the root CA certificate of the issuer of the computer certificates installed on the IAS servers is already installed as a root CA certificate on your wired clients, no other configuration is necessary. If your issuing CA is a Windows 2000 Server or Windows Server 2003 online root enterprise CA, then the root CA certificate is automatically installed on each domain member through computer configuration Group Policy.

To verify, obtain the properties of the computer certificate on the IAS server using the Certificates snap-in and view the certificate chain from the **Certification Path** tab. The certificate at the top of the path is the root CA certificate. Use the Certificates snap-in of a wired client for each Windows operating system to ensure that this certificate is in the list of trusted root certification authorities in the Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates folder.

If it is not, you must install the root CA certificate(s) of the issuer(s) of the computer certificates of the IAS servers on each wired client for the Windows operating systems that do not contain them.

The easiest way to install a root CA certificate on all your wired clients is to do the following:

1. Using the Certificates snap-in on an IAS server, export the root CA certificate of the issuing CA of computer certificates on the IAS servers to a file (*.PB7). You can find the root CA certificate in the Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates folder.
2. Open the Active Directory Users and Computers snap-in.
3. In the console tree, double-click **Active Directory Users and Computers**, right-click the appropriate domain system container, and then click **Properties**.
4. On the **Group Policy** tab, click the appropriate Group Policy object (the default object is **Default Domain Policy**), and then click **Edit**.
5. In the console tree, open **Computer Configuration**, then **Windows Settings**, then **Security Settings**, and then **Public Key Policies**.
6. Right-click **Trusted Root Certification Authorities**, and then click **Import**.
7. In the Certificate Import Wizard, specify the file that was saved in Step 1.
8. Repeat steps 3-7 for all appropriate system containers.

The next time the wired client computers update their computer configuration Group Policy, the root CA certificate of the issuing CA of computer certificates on the IAS servers is installed in their local computer certificate store.

Alternately, you can use the Certificates snap-in to import the root CA certificates to the Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates folder on each wired client computer.

Step 6: Configure a certificate infrastructure for EAP-TLS

Table 1 summarizes the certificates needed for the different types of authentication.

Authentication Type	Certificates on Wired client	Certificates on IAS Server
PEAP-MS-CHAP v2	Root CA certificates for issuers of IAS server computer certificates	Computer certificates
EAP-TLS	Computer certificates User certificates Root CA certificates for issuers of IAS server computer certificates	Computer certificates Root CA certificates for issuers of wired client computer and user certificates
EAP-MD5 CHAP	None	None

Table 1 Authentication types and certificates

If you use the EAP-TLS or PEAP-MS-CHAP v2 authentication method for your wired connections, you must install computer certificates on the IAS servers.

For PEAP-MS-CHAP v2, you do not have to deploy a certificate infrastructure to issue computer and user certificates for each wired client computer. Instead, you can obtain individual certificates for each IAS server in your organization from a commercial certification authority and install them on the IAS servers. For more information, see "Step 3: Configuring the Primary IAS Server" and "Step 4: Configuring the Secondary IAS Server" in this article. Windows wired clients include a number of root CA certificates for well known and

trusted commercial CAs. If you obtain computer certificates from a commercial CA for which there is already an installed root CA certificate, there are no additional certificates to install on the Windows wired clients. If you obtain computer certificates from a commercial CA for which there is not already an installed root CA certificate, you must install the root CA certificates for the issuers of the computer certificates installed on the IAS servers on each Windows wired client. For more information, see "Step 10: Configuring Wired Client Computers for PEAP-MS-CHAP v2" in this article.

For computer authentication with EAP-TLS, you must install a computer certificate, also known as a machine certificate, on the wired client computer. A computer certificate installed on the wired client computer is used to authenticate the wired client computer so that the computer can obtain network connectivity to the organization intranet and computer configuration Group Policy updates prior to user login. For user authentication with EAP-TLS after a network connection is made and the user logs in, you must use a user certificate on the wired client computer.

The computer certificate is installed on the IAS server computer so that during EAP-TLS authentication, the IAS server has a certificate to send to the wired client computer for mutual authentication, regardless of whether the wired client computer authenticates with a computer certificate or a user certificate. The computer and user certificates submitted by the wired client and IAS server during EAP-TLS authentication must conform to the requirements specified in "Using a Third-Party CA" in this article.

In Windows Server 2003, Windows XP, and Windows 2000, you can view the certificate chain from the **Certification Path** tab in the properties of a certificate in the Certificates snap-in. You can view the installed root CA certificates in the Trusted Root Certification Authorities\Certificates folder and you can view the intermediate CA certificates in the Intermediate Certification Authorities\Certificates folder.

In a typical deployment, the certificate infrastructure is configured using a single root CA in a three-level hierarchy consisting of root CA/intermediate CAs/issuing CAs. Issuing CAs are configured to issue computer certificates or user certificates. When the computer or user certificate is installed on the wired client, the issuing CA certificate, intermediate CA certificates, and the root CA certificate is also installed. When the computer certificate is installed on the IAS server computer, the issuing CA certificate, intermediate CA certificates, and the root CA certificate is also installed. The issuing CA for the IAS server certificate can be different than the issuing CA for the wired client certificates. In this case, both the wired client and the IAS server computer have all the required certificates to perform certificate validation for EAP-TLS authentication.

Best Practices If you are using EAP-TLS authentication, use both user and computer certificates for both user and computer authentication.

If you are using EAP-TLS authentication, do not also use PEAP-TLS. Allowing both protected and unprotected authentication traffic for the same type of network connection renders the protected authentication traffic susceptible to spoofing attacks.

If you already have a certificate infrastructure for EAP-TLS authentication and are using RADIUS for dial-up or virtual private network (VPN) remote access connections, you can skip some of the certificate infrastructure steps. You can use the same certificate infrastructure for wired connections. However, you must ensure that computer certificates are installed for computer authentication. For computers running Windows XP with no service packs installed, you must have user certificates stored on the computer for user authentication (rather than using smart cards). For computers running Windows Server 2003, Windows XP with SP2, Windows XP with SP1, or Windows 2000, you can use either user certificates stored on the computer or a smart card for user authentication.

Step 6a: Installing a Certificate Infrastructure

When installing a certificate infrastructure, use the following best practices:

- Plan your public key infrastructure (PKI) before deploying CAs.
- The root CA should be offline and its signing key should be secured by a Hardware Security Module (HSM) and kept in a vault to minimize potential for key compromise.
- Enterprise organizations should not issue certificates to users or computers directly from the root CA, but rather should deploy the following:
 - An offline root CA
 - Offline intermediate CAs
 - Online issuing CAs (using Windows Server 2003 or Windows 2000 Certificate Services as an enterprise CA)

This CA hierarchy provides flexibility and insulates the root CA from attempts to compromise its private key by malicious users. The offline root and intermediate CAs do not have to be Windows Server 2003 or Windows 2000 CAs. Issuing CAs can be subordinates of a third party intermediate CA.

- Backing up the CA database, the CA certificate, and the CA keys is essential to protect against the loss of critical data. The CA should be backed up on a regular basis (daily, weekly, monthly) based on the number of certificates issued over the same interval. The more certificates issued, the more frequently you should back up the CA.
- You should review the concepts of security permissions and access control in Windows, since enterprise CAs issue certificates based on the security permissions of the certificate requester.

Additionally, if you want to take advantage of autoenrollment for computer certificates, use Windows 2000 or Windows Server 2003 Certificate Services and create an enterprise CA at the issuer CA level. If you want to take advantage of autoenrollment for user certificates, use Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, Certificate Services and create an enterprise CA at the issuer CA level.

For more information, see the topic titled "Checklist: Deploying certification authorities and PKI for an intranet" in Windows 2000 Server Help or the topic titled "Checklist: Creating a certification hierarchy with an offline root certification authority" in Windows Server 2003 Help and Support.

For additional information about PKI and the Windows 2000 Certificate Services, including deployment instructions and best practices, see the [Windows 2000 Security Services Web Site](http://www.microsoft.com/windows2000/technologies/security/default.asp) at <http://www.microsoft.com/windows2000/technologies/security/default.asp>. For additional information about Windows Server 2003 security services, including deployment instructions and best practices, see the [Windows Server 2003 Security Services Web site](http://www.microsoft.com/windowsserver2003/technologies/security/default.mspx) at <http://www.microsoft.com/windowsserver2003/technologies/security/default.mspx>.

By default, the IAS server checks for certificate revocation for all the certificates in the certificate chain sent by the wired client during the EAP-TLS authentication process. If certificate revocation fails for any of the certificates in the chain, the connection attempt is not authenticated and is denied. The certificate revocation check for a certificate can fail because of the following:

- The certificate has been revoked.

The issuer of the certificate has explicitly revoked the certificate.

- The certificate revocation list (CRL) for the certificate is not reachable or available.

CAs maintain CRLs and publish them to specific CRL distribution points. The CRL distribution points are included in the CRL Distribution Points property of the certificate. If the CRL distribution points cannot be contacted to check for certificate revocation, then the certificate revocation check fails.

Additionally, if there are no CRL distribution points in the certificate, the IAS server cannot verify that the certificate has not been revoked and the certificate revocation check fails.

- The publisher of the CRL did not issue the certificate.

Included in the CRL is the publishing CA. If the publishing CA of the CRL does not match the issuing CA for the certificate for which certificate revocation is being checked, then the certificate revocation check fails.

- The CRL is not current

Each published CRL has a range of valid dates. If the CRL **Next update** date has passed, the CRL is considered invalid and the certificate revocation check fails. New CRLs should be published before the expiration date of the last published CRL.

Certificate revocation checking behavior for IAS can be modified with registry settings. For more information, see the ["Troubleshooting Windows XP IEEE 802.11 Wireless Access"](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.mspx) article at <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.mspx>.

Because certificate revocation checking can prevent wired access due to the unavailability or expiration of CRLs for each certificate in the certificate chain, design your PKI for high availability of CRLs. For instance, configure multiple CRL distribution points for each CA in the certificate hierarchy and configure publication schedules that ensure that the most current CRL is always available.

Certificate revocation checking is only as accurate as the last published CRL. For example, if a certificate is revoked, by default the new CRL containing the newly revoked certificate is not automatically published. CRLs are typically published based on a configurable schedule. This means that the revoked certificate can still be used to authenticate because the published CRL is not current; it does not contain the revoked certificate and can therefore still be used to create wired connections. To prevent this from occurring, the network administrator must manually publish the new CRL with the newly revoked certificate. Windows XP and Windows 2003 support delta CRLs, which allows the revocation information to be updated more frequently.

By default the IAS server uses the CRL distribution points in the certificates. However, it is also possible to store a local copy of the CRL on the IAS server. In this case, the local CRL is used during certificate revocation checking. If a new CRL is manually published to the Active Directory, the local CRL on the IAS server is not updated. The local CRL is updated when it expires. This can create a situation wherein a certificate is revoked, the CRL is manually published, but the IAS server still allows the connection because the local CRL has not yet been updated.

Step 6b: Installing Computer Certificates

If you are using a Windows Server 2003 or Windows 2000 Certificate Services enterprise CA as an issuing CA, you can install a computer certificate on the IAS server by configuring Group Policy for the autoenrollment of computer certificates for computers in an Active Directory system container.

❑ To configure computer certificate enrollment for an enterprise CA

1. Open the Active Directory Users and Computers snap-in.
2. In the console tree, double-click **Active Directory Users and Computers**, right-click the domain name to which your CA belongs, and then click **Properties**.
3. On the **Group Policy** tab, click the appropriate Group Policy object (the default object is **Default Domain Policy**), and then click **Edit**.
4. In the console tree, open **Computer Configuration**, then **Windows Settings**, then **Security Settings**, then **Public Key Policies**, and then **Automatic Certificate Request Settings**.
5. Right-click **Automatic Certificate Request Settings**, point to **New**, and then click **Automatic Certificate Request**.
6. The Automatic Certificate Request wizard appears. Click **Next**.
7. In **Certificate templates**, click **Computer**, and then click **Next**.
Your enterprise CA appears on the list.
8. Click the enterprise CA, click **Next**, and then click **Finish**.
9. To immediately obtain a computer certificate for the CA that is running Windows 2000 Server, type the following at a command prompt:

```
secedit /refreshpolicy machine_policy
```

10. To immediately obtain a computer certificate for the CA that is running Windows Server 2003, type the following at a command prompt:

```
gpupdate /target:computer
```

After the domain is configured for autoenrollment, each computer that is a member of the domain requests a computer certificate when computer Group Policy is refreshed. By default, the Winlogon service polls for changes in Group Policy every 90 minutes. To force a refresh of computer Group Policy, restart the computer or type **secedit /refreshpolicy machine_policy** (for a computer running Windows 2000) or **gpupdate /target:computer** (for a computer running Windows XP or Windows Server 2003) at a command prompt.

Perform this procedure for each domain system container as appropriate.

Best Practices If you use a Windows Server 2003 or Windows 2000 enterprise CA as an issuing CA, configure autoenrollment of computer certificates to install computer certificates on all computers. Ensure that all appropriate domain system containers are configured for autoenrollment of computer certificates either through the inheriting of group policy settings of a parent system container or explicit configuration.

Step 6c: Installing User Certificates

If you are using a Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, enterprise CA as an issuing CA, you can install user certificates through autoenrollment. Only Windows XP and Windows Server 2003 wired clients support user certificate autoenrollment.

❑ To configure user certificate enrollment for an enterprise CA

1. 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. Under **Snap-in**, double-click **Certificate Templates**, click **Close**, and then click **OK**.
4. In the console tree, click **Certificate Templates**. All of the certificate templates will be displayed in the details pane.
5. In the details pane, click the **User** template.
6. On the **Action** menu, click **Duplicate Template**.
7. In the **Display Name** field, type **WiredUser** (example name).
8. Make sure that the **Publish Certificate in Active Directory** check box is selected.
9. Click the **Security** tab.
10. In the **Group or user names** field, click **Domain Users**.
11. In the **Permissions for Domain Users** list, select the **Read**, **Enroll**, and **Autoenroll** permission check boxes and then click **OK**.
12. Open the Certification Authority snap-in.
13. In the console tree, open **Certification Authority**, then the CA name, then **Certificate Templates**.
14. On the **Action** menu, point to **New**, and then click **Certificate to Issue**.
15. Click **WiredUser** (example) and click **OK**.
16. Open the Active Directory Users and Computers snap-in.
17. In the console tree, double-click **Active Directory Users and Computers**, right-click the domain system container that contains user accounts, and then click **Properties**.
18. On the **Group Policy** tab, click the appropriate Group Policy object (the default object is **Default Domain Policy**), and then click **Edit**.
19. In the console tree, open **User Configuration**, then **Windows Settings**, then **Security Settings**, then **Public Key Policies**.
20. In the details pane, double-click **Autoenrollment Settings**.
21. Click **Enroll certificates automatically**.
22. Select the **Renew expired certificates, update pending certificates, and remove revoked certificates** check box.
23. Select the **Update certificates that use certificate templates** check box and click **OK**.

Perform steps 17-23 for each domain system container as appropriate.

Best Practices If you use a Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition, enterprise CA as an issuing CA, configure autoenrollment of user certificates to install user certificates on all computers. Ensure that all appropriate domain system containers are configured for autoenrollment of user certificates either through the inheriting of group policy settings of a parent system container or explicit configuration.

Step 7: Installing Computer Certificates on Wired Client Computers for EAP-TLS

For computer authentication with EAP-TLS, you must install a computer certificate on the wired client computer.

To install a computer certificate on a wired client computer running Windows Server 2003, Windows XP, or Windows 2000, connect to the organization intranet using an unauthenticated Ethernet port and do the following:

- If the domain is configured for autoenrollment of computer certificates, each computer that is a member of the domain requests a computer certificate when computer Group Policy is refreshed. To force a refresh of computer Group Policy for a computer running Windows Server 2003 or Windows XP, restart the computer or type **gpupdate /target:computer** at a command prompt. To force a refresh of computer Group Policy for a computer running Windows 2000, restart the computer or type **secedit /refreshpolicy machine_policy** at a command prompt.
- If the domain is not configured for autoenrollment, you can request a "Computer" certificate using the Certificates snap-in or you can execute a CAPICOM script to install a computer certificate.

An enterprise organization's information technology (IT) group can install a computer certificate before the computer is delivered to its user.

For information about CAPICOM, search for CAPICOM at <http://msdn.microsoft.com>.

Step 8: Installing User Certificates on Wired Client Computers for EAP-TLS

For user authentication with EAP-TLS, you must use a locally installed user certificate or a smart card. The locally installed user certificate must be obtained through autoenrollment, Web enrollment, by requesting the certificate using the Certificates snap-in, by importing a certificate file, or by running a CAPICOM program or script.

The easiest methods of installing user certificates assume that network connectivity already exists, such as using an unauthenticated Ethernet port. When the user connects to the intranet using an unauthenticated Ethernet port, they can obtain a user certificate through autoenrollment or by submitting a user certificate request using Web enrollment or the Certificate Manager. For more information about requesting a user certificate, see the "Submit a user certificate request via the Web" and "Request a certificate" procedures in this section.

Alternately, the user can run a CAPICOM program or script provided by the network administrator. The execution of the CAPICOM program or script can be automated through the user logon script.

If you have configured autoenrollment of user certificates, then the wired user must update User Configuration Group Policy to obtain a user certificate.

If you are not using autoenrollment for user certificates, use one of the following procedures to obtain a user certificate.

□ **Submit a user certificate request via the Web**

1. Open Internet Explorer.
2. In Internet Explorer, connect to **http://servername/certsrv**, where *servername* is the name of the server where the CA you want to access is located.
3. Click **Request a certificate**, and then click **Next**.

4. On the **Choose Request Type** Web page, under **User certificate request**, select the type of certificate you want to request, and click **Next**.
5. Do one of the following from the **Identifying Information** Web page:
 - If you see the message "All the necessary identifying information has already been collected. You may now submit your request," click **Submit**.
 - Enter your identifying information for the certificate request, and click **Submit**.
6. If you see the **Certificate Issued** Web page, click **Install this certificate**.
7. Close Internet Explorer.

❑ **Request a certificate**

1. Open an MMC console that contains **Certificates – Current User**.
2. In the console tree, right-click **Personal**, then point to **All Tasks**, and then click **Request New Certificate** to start the Certificate Request wizard.
3. In the Certificate Request Wizard, select the following information:
 - The type of certificate you want to request.
 - If you have selected the **Advanced** check box:
 - The cryptographic service provider (CSP) you are using.
 - The key length (measured in bits) of the public key associated with the certificate.
 - Do not enable strong private key protection.
 - If you have more than one CA available, select the name of the CA that will issue the certificate.
4. Type a friendly name for your new certificate.
5. After the Certificate Request Wizard has successfully finished, click **OK**.

Floppy Disk-Based Installation

Another method of installing a user certificate is to export the user certificate onto a floppy disk and import it from the floppy disk onto the wired client computer. For a floppy disk-based enrollment, perform the following:

1. Obtain a user certificate for the wired client's user account from the CA through Web-based enrollment. For more information, see the "Submit a user certificate request via the Web" procedure previously described.
2. Export the user certificate of the wired client's user account to a .pfx file. For more information, see the "Export a certificate" procedure in this section. Within the Certificate Manager Export wizard, export the private key and select **Delete the private key if the import is successful**. Save this file to a floppy disk and deliver it to the user of the wired client computer.
3. On the wired client computer, import the user certificate. For more information, see the "Import a certificate" procedure in this section.

❑ **Export a certificate**

1. Open an MMC console containing **Certificates - Current User**.

2. Open **Personal**, and then open **Certificates**.
3. In the details pane, right-click the certificate you want to export, point to **All Tasks**, and then click **Export**.
4. In the Certificate Export Wizard, click **Yes, export the private key**. (This option will appear only if the private key is marked as exportable and you have access to the private key.) Click **Next**.
5. Select **Personal Information Exchange – PKCS #12 (.PFX)** as the export file format and click **Next**.
6. On the **Password** page, type a password in **Password** and **Confirm password** to protect the private key in the certificate and then click **Next**.
7. On the **File to Export** page, type the certificate filename or click **Browse** to specify the name and location of the certificate file. Click **Next**.
8. On the **Completing the Certificate Export Wizard** page, click **Finish**.

Import a certificate

1. Open an MMC console containing **Certificates - Current User**.
2. Open **Personal**, and then open **Certificates**.
3. In the details pane, right-click the certificate you want to export, point to **All Tasks**, and then click **Import**.
4. Type the file name containing the certificate to be imported. (You can also click **Browse** and navigate to the file.)
5. If it is a PKCS #12 file, do the following:
 - Type the password used to encrypt the private key.
 - Do not enable strong private key protection.
 - (Optional) If you want to back up or transport your keys at a later time, select the **Mark key as exportable** check box.
6. Do one of the following:
 - If the certificate should be automatically placed in a certificate store based on the type of certificate, select **Automatically select the certificate store based on the type of certificate**.
 - If you want to specify where the certificate is stored, select **Place all certificates in the following store**, click **Browse**, and select the certificate store to use.

Step 9: Configuring Wired Client Computers for EAP-TLS

To manually configure EAP-TLS authentication on a wired client running Windows XP with SP2, Windows XP with SP1, Windows Server 2003, or Windows 2000, do the following:

1. Obtain properties of the connection in the Network Connections folder.
2. Click the **Authentication** tab and select **Enable network access control using IEEE 802.1X** and the **Smart Card or other Certificate** EAP type. This is enabled by default.
3. Click **Properties**. In the properties of the **Smart Card or other Certificate** EAP type, select **Use a certificate on this computer** to use a registry-based user certificate or **Use my smart card** for a

smart card-based user certificate.

If you want to validate the computer certificate of the IAS server, select **Validate server certificate** (enabled by default). If you want to specify the names of the authentication servers that must perform validation, select **Connect to these servers** and type the names.

4. Click **OK** to save changes to the Smart Card or other Certificate EAP type.

To configure EAP-TLS authentication on a wired client running Windows XP with no service packs installed, do the following:

1. Obtain properties of the connection in the Network Connections folder.
2. Click the **Authentication** tab, and then select **Enable network access control using IEEE 802.1X** and the **Smart Card or other Certificate** EAP type. This is enabled by default.
3. Click **Properties**. In the properties of the **Smart Card or other Certificate** EAP type, select **Use a certificate on this computer**.

If you want to validate the computer certificate of the IAS server, select **Validate server certificate** (enabled by default).

If you want to ensure that the server's DNS name ends in a specific string, select **Connect only if server name ends with** and type the string. For typical deployments where more than one IAS server is used, type the part of the DNS name that is common to all of the IAS servers. For example, if you have two IAS servers named IAS1.example.microsoft.com and IAS2.example.microsoft.com, then type the string "example.microsoft.com". Ensure that you type the correct string, otherwise, authentication will fail.

4. Click **OK** to save changes to the Smart Card or other Certificate EAP type.

Note Wireless clients can be configured with 802.1X configuration settings using the Wireless Network (IEEE 802.11) Policies Group Policy extension provided in Windows Server 2003. These Group Policy settings only apply to wireless network connections and cannot be used to configure 802.1X settings for wired network connections.

Step 10: Configuring Wired Client Computers for EAP-MD5 CHAP

To manually configure EAP-MD5 CHAP authentication on a wired client running Windows XP, Windows Server 2003, or Windows 2000, do the following:

1. Obtain properties of the connection in the Network Connections folder.
2. Click the **Authentication** tab and select **Enable network access control using IEEE 802.1X** and the **MD-5 Challenge** EAP type.
3. Click **OK** to save changes to the **Authentication** tab.

Step 11: Verifying Wired Connections

After your wired clients are configured, connect them to their switches and verify that they are being authenticated. If none of the wired clients are being authenticated, try setting the HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\SupplicantMode registry value to 3 (REG_DWORD data type). The default value of SupplicantMode for wired connections is 2.

Additional Intranet Wired Deployment Configurations

This section describes the following additional intranet wired deployment configurations:

- Internet access for business partners
- Using a third-party CA
- Cross-forest authentication
- Using RADIUS proxies to scale authentications
- Using computer-only authentication

Internet Access for Business Partners

The following is the behavior of most authenticating switches in use today with respect to the receipt of RADIUS Access-Accept and Access-Reject messages:

- When the authenticating switch receives an Access-Accept message, the connection is allowed.
- When the authenticating switch receives an Access-Reject message, the connection is denied.

To allow a business partner, vendor, or other non-employee to gain access to a separate network using the same wired infrastructure that allows employees to access to the organization intranet, the connection request must result in an Access-Accept message from the RADIUS server. To get an Access-Accept message from the RADIUS server, you must either use guest access or the business partner, vendor, or other non-employee must have a valid account and certificates.

Using Guest Access

Guest access occurs when wired clients are connected without sending a user identity. The wired client does not provide a user name or credentials to the authenticating switch. Therefore, the authenticating switch does not include user identity (the User-Name attribute) or credential attributes in the Access-Request message. When the IAS server receives an Access-Request message that contains no user identity or credentials attributes, it verifies whether unauthenticated access is enabled for the remote access policy that matches the connection attempt. If a user identity attribute is not included, the IAS server uses the Guest account to obtain user account dial-in properties and group membership. If a user identity attribute is included but credential attributes are not, the IAS server uses the indicated account to obtain user account dial-in properties and group membership.

Restricted network access for guest access clients is supported on authenticating switches by using IP filtering or VLANs. To specify a virtual LAN identifier for unauthenticated access, configure the Tunnel-Type and Tunnel-Pvt-Group-ID attributes on the advanced properties of the appropriate remote access policy.

For more information about unauthenticated and guest access with IAS, see Windows 2000 Server Help or Windows Server 2003 Help and Support.

Using Validated Access

For validated access for business partners, vendors, or other non-employees, you must create computer and user accounts and issue certificates for each business partner, vendor, or other non-employee. Next, create groups with these accounts as members so that you can manage access using group-based remote

access policies. For example, create a WiredInternetUsers group that contains global groups of business partner, vendor, or other non-employee user and computer accounts.

To configure a wired remote access policy for Internet access for business partners, vendors, or other non-employees, create a new custom remote access policy for wired Internet access with the following settings:

- Policy name: Wired access to Internet (example)
- Conditions: NAS-Port-Type=Ethernet, Windows-Groups=WiredInternetUsers
- Permissions: Select **Grant remote access permission**.
Profile, **Authentication** tab: Select **EAP Methods** and the appropriate EAP type.
- Profile, **Encryption** tab: Select all check boxes. The settings on the **Encryption** tab correspond to the MS-MPPE-Encryption-Policy and MS-MPPE-Encryption-Types RADIUS attributes and might be supported by the authenticating switch. If these attributes are not supported, clear all the check boxes except **No encryption**.
- Profile, **Advanced** tab (if the authenticating switch supports VLANs):
 - Add the Tunnel-Type attribute with the value of "Virtual LANs (VLAN)".
 - Add the Tunnel-Pvt-Group-ID attribute with the value of the VLAN ID of the VLAN that is connected to the Internet.

If the authenticating switches require vendor specific attributes (VSAs), you must add the VSAs to the appropriate remote access policies. For more information, see the "Configure vendor-specific attributes for a remote access policy" procedure previously described.

Using a Third-Party CA

You can use third-party CAs to issue certificates for wired access as long as the certificates installed can be validated and have the appropriate properties.

Certificates on IAS Servers

For the computer certificates installed on the IAS servers, the following must be true:

- They must be installed in the Local Computer certificate store.
- They must have a corresponding private key. When you view the properties of the certificate with the Certificate snap-in, you should see the text **You have a private key that corresponds to this certificate** on the **General** tab.
- The cryptographic service provider for the certificates supports SChannel. If not, the IAS server cannot use the certificate and it is not selectable from the properties of the **Smart Card or Other Certificate** EAP type from the **Authentication** tab on the properties of a profile for a remote access policy.
- They must contain the Server Authentication certificate purpose (also known as an Enhanced Key Usage [EKU]). An EKU is identified using an object identifier (OID). The OID for Server Authentication is "1.3.6.1.5.5.7.3.1".
- They must contain the fully qualified domain name (FQDN) of the computer account of the IAS server computer in the Subject Alternative Name property.

Additionally, the root CA certificates of the CAs that issued the wired client computer and user certificates must be installed in the Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates folder.

Certificates on Wired Client Computers

For the user and computer certificates installed on wired client computers, the following must be true:

- They must have a corresponding private key.
- They must contain the Client Authentication EKU (OID "1.3.6.1.5.5.7.3.2")
- Computer certificates must be installed in the Local Computer certificate store.
- Computer certificates must contain the FQDN of the wired client computer account in the Subject Alternative Name property.
- User certificates must be installed in the Current User certificate store.
- User certificates must contain the user principal name (UPN) of the user account in the Subject Alternative Name property.

Additionally, the root CA certificates of the CAs that issued the IAS server computer certificates must be installed in the Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates folder.

Cross-Forest Authentication

Because IAS uses Active Directory to validate credentials and obtain user and computer account properties, a RADIUS proxy must be placed between the authenticating switches and the IAS server computers when the user and computer accounts for wired client computers and users exist in the following authentication databases:

- Two different Active Directory forests that do not trust each other (cross-forest).
- Two different domains that do not trust each other.
- Two different domains that have a one-way trust.

The following discussion assumes a cross-forest configuration.

When an access client sends user credentials, a user name is often included. Within the user name are two elements:

- Identification of the user account name
- Identification of the user account location

For example, for the user name user1@microsoft.com, user1 is the user account name and microsoft.com is the location of the user account. The identification of the location of the user account is known as a realm. There are different forms of realm names:

- The realm name can be a prefix.

For microsoft\user1, "microsoft" is the name of a Windows NT® 4.0 domain.

- The realm name can be a suffix.

For user1@microsoft.com, "microsoft.com" is either a DNS domain name or the name of an Active Directory-based domain.

Note You do not need to use a RADIUS proxy if you are using PEAP-MS-CHAP v2 and Windows NT 4.0-style user names (for example, microsoft\user1).

The user name is passed from the wired client to the authenticating switch during the authentication phase of the connection attempt. This user name becomes the User-Name RADIUS attribute in the Access-Request message that is sent by the authenticating switch to its configured RADIUS server, which in this configuration is a RADIUS proxy. When the RADIUS proxy receives the Access-Request message, configured rules or policies on the RADIUS proxy determine the IAS server to which the Access-Request message is forwarded.

Figure 2 shows IAS RADIUS proxies being used to forward RADIUS messages between authenticating switches and multiple IAS servers in two different Active Directory forests.

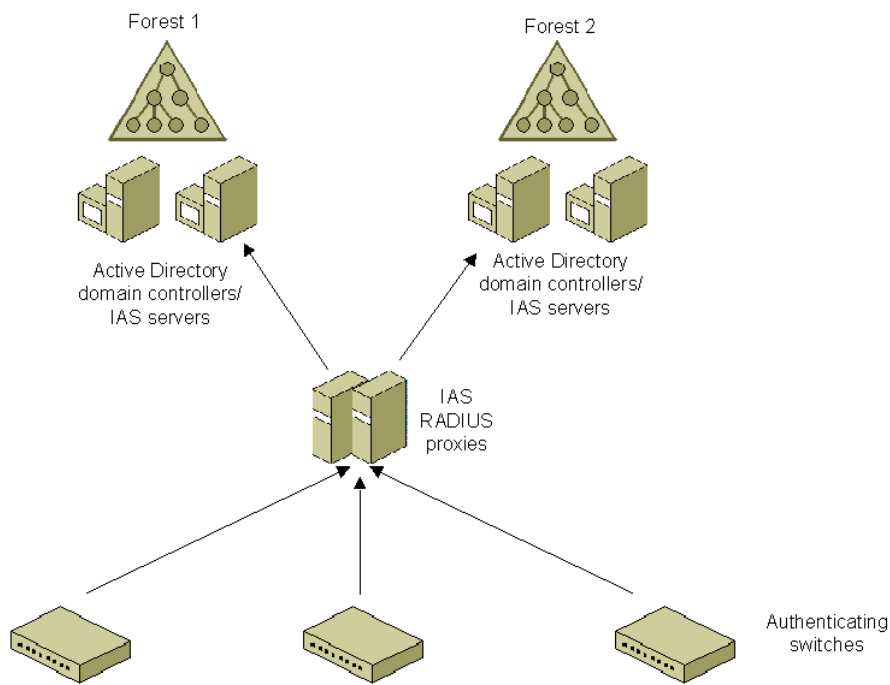


Figure 2 Using IAS RADIUS proxies for cross-forest authentication

The following configuration is for an organization that uses:

- Active Directory domains.

Active Directory domains contain the user accounts, passwords, and dial-in properties that each IAS server requires to authenticate user credentials and evaluate authorization.

- At least two IAS servers in each forest.

At least two IAS servers (one primary and one secondary) are used to provide fault tolerance for RADIUS-based authentication, authorization, and accounting in each forest. If only one RADIUS server is configured and it becomes unavailable, wired clients for that forest cannot connect. By using at two IAS servers and configuring the IAS RADIUS proxies for both primary and secondary IAS servers, the IAS RADIUS proxies can detect when the primary RADIUS server is unavailable and automatically fail over to the secondary IAS server.

- Remote access policies.

Remote access policies are configured to specify, based on group membership, the different types of connection constraints for users.

- At least two IAS RADIUS proxies.

At least two IAS RADIUS proxies are used to provide fault tolerance for RADIUS requests that are sent from the authenticating switches.

To configure IAS for this example, complete the following steps:

1. Configure the Active Directory forests for accounts and groups.
2. Configure the primary IAS server on a computer in the first forest.
3. Configure the secondary IAS server on another computer in the first forest.
4. Configure the primary IAS server on a computer in the second forest.
5. Configure the secondary IAS server on another computer in the second forest.
6. Configure the primary IAS RADIUS proxy.
7. Configure the secondary IAS RADIUS proxy.
8. Configure RADIUS authentication and accounting on authenticating switches.

IAS for Windows 2000 does not support RADIUS proxy. However, you can use IAS in Windows Server 2003 to act as a RADIUS proxy in this configuration. For more information, see the topic titled "Authentication across forests" in Windows Server 2003 Help and Support.

Configuring the Active Directory Forests for Accounts and Groups

To configure Active Directory for user accounts and groups, do the following:

1. On each Windows 2000 domain controller computer, install Windows 2000 SP4 or later.
2. Ensure that all users who are making wired connections have a corresponding user account. Ensure that all computers who are making wired connections have a corresponding computer account.
3. Set the remote access permission on user and computer accounts to the appropriate setting.
4. Organize your accounts into the appropriate groups in order to take advantage of group-based remote access policies.

Configuring the Primary IAS Server on a Computer in the First Forest

To configure the primary IAS server on a computer in the first forest, do the following:

1. If you are using Windows 2000 IAS, install IAS as an optional networking component on a computer in the first forest, and then install Windows 2000 SP4 or later. If you are using Windows Server 2003 IAS, install IAS as an optional networking component on a computer in the first forest.
2. Configure the IAS server computer to read the properties of user accounts in the domain.
3. If the IAS server is authenticating connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the IAS server computer is a member. Next, configure the IAS server computer to read the properties of user accounts in other domains.

4. If needed, enable logging for accounting and authentication events.
5. Add the IAS RADIUS proxies as RADIUS clients of the IAS server. Verify that you are configuring the correct name or IP address and shared secrets.
6. Create the appropriate remote access policy for wired clients in the first forest.

Configuring the Secondary IAS Server on Another Computer in the First Forest

To configure the secondary IAS server on another computer in the first forest, do the following:

1. If you are using Windows 2000 IAS, install IAS as an optional networking component on another computer in the first forest, and then install Windows 2000 SP4 or later. If you are using Windows Server 2003 IAS, install IAS as an optional networking component on another computer in the first forest.
2. Configure the secondary IAS server computer to read the properties of user accounts in the domain.
3. If the secondary IAS server authenticates connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the secondary IAS server computer is a member. Next, configure the secondary IAS server computer to read the properties of user accounts in other domains.
4. Copy the configuration of the primary IAS server to the secondary IAS server.

Configuring the Primary IAS Server on a Computer in the Second Forest

To configure the primary IAS server on a computer in the second forest, do the following:

1. If you are using Windows 2000 IAS, install IAS as an optional networking component on a computer in the second forest, and then install Windows 2000 SP4 or later. If you are using Windows Server 2003 IAS, install IAS as an optional networking component on a computer in the second forest.
2. Configure the primary IAS server computer to read the properties of user accounts in the appropriate domain system containers.
3. If the IAS server authenticates connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the IAS server computer is a member. Next, configure the IAS server computer to read the properties of user accounts in other domains.
4. If needed, enable logging for accounting and authentication events.
5. Add the IAS RADIUS proxies as RADIUS clients of the IAS server. Verify that you are configuring the correct name or IP address and shared secrets.
6. Create the appropriate remote access policy for wired clients in the second forest.

Configuring the Secondary IAS Server on Another Computer in the Second Forest

To configure the secondary IAS server on another computer in the second forest, do the following:

1. If you are using Windows 2000 IAS, install IAS as an optional networking component on another computer in the second forest, and then install Windows 2000 SP4 or later. If you are using Windows Server 2003 IAS, install IAS as an optional networking component on another computer in the second forest.
2. Configure the secondary IAS server computer to read the properties of user accounts in the

appropriate domain system containers.

3. If the secondary IAS server authenticates connection attempts for user accounts in other domains, verify that the other domains have a two-way trust with the domain in which the secondary IAS server computer is a member. Next, configure the secondary IAS server computer to read the properties of user accounts in other domains.
4. Copy the configuration of the primary IAS server in the second forest to the secondary IAS server.

Configuring the Primary IAS RADIUS Proxy

To configure the primary IAS RADIUS proxy, do the following:

1. On a computer running Windows Server 2003, install IAS as an optional networking component. The computer on which IAS is installed is not required to be dedicated to forwarding RADIUS messages.
2. If needed, configure additional UDP ports for RADIUS messages that are sent by the authenticating switches. By default, IAS uses UDP ports 1812 and 1645 for authentication and ports 1813 and 1646 for accounting.
3. Add the authenticating switches as RADIUS clients of the IAS RADIUS proxy. Verify that you are configuring the correct name or IP address and shared secrets.
4. Create a connection request policy that forwards RADIUS request messages (that are based on the realm name of accounts in the first forest) to the IAS servers in the first forest. Use the New Connection Request Policy Wizard to create a connection request policy that forwards connection requests to a remote RADIUS server group and where the realm name matches the realm name of the user accounts in the first forest. Clear the check box that removes the realm name for authentication. In the New Connection Request Policy Wizard, use the New Remote RADIUS Server Group Wizard to create a remote RADIUS server group with members that include the two IAS servers in the first forest.
5. Create a connection request policy that forwards RADIUS request messages (that are based on the realm name of accounts in the second forest) to the IAS servers in the second forest. Use the New Connection Request Policy Wizard to create a connection request policy that forwards connection requests to a remote RADIUS server group and where the realm name matches the realm name of the user accounts in the second forest. Clear the check box that removes the realm name for authentication. In the New Connection Request Policy Wizard, use the New Remote RADIUS Server Group Wizard to create a remote RADIUS server group with members that include the two IAS servers in the second forest.
6. Delete the default connection request policy named **Use Windows authentication for all users**.

Configuring the Secondary IAS RADIUS Proxy

To configure the secondary IAS RADIUS proxy on another computer, do the following:

1. On another computer running Windows Server 2003, install IAS as an optional networking component.
2. Copy the configuration of the primary IAS RADIUS proxy to the secondary IAS RADIUS proxy.

Configuring RADIUS Authentication and Accounting on the Authenticating Switches

Configure RADIUS settings on your third-party authenticating switches with the following:

1. The IP address or name of the primary RADIUS server, the common shared secret, UDP ports for authentication and accounting, and failure detection settings.
2. The IP address or name of the secondary RADIUS server, the common shared secret, UDP ports for authentication and accounting, and failure detection settings.

To balance the load of RADIUS traffic between the two IAS RADIUS proxies, configure half of the authenticating switches with the primary IAS RADIUS proxy as the primary RADIUS server and the secondary IAS RADIUS proxy as the secondary RADIUS server and the other half of the authenticating switches with the secondary IAS RADIUS proxy as the primary RADIUS server and the primary IAS RADIUS proxy as the secondary RADIUS server.

For more information, see the documentation for the authenticating switch.

Using RADIUS Proxies to Scale Authentications

When performing authentication for a large number of wired clients using EAP-TLS and certificates, the volume of authentication traffic needed to keep wired clients connected can be substantial. In a large deployment, it would be best to attempt to spread the load of authentication traffic among multiple IAS server computers. Because you cannot rely on the authenticating switches to consistently or adequately spread their authentication traffic among multiple IAS servers, intermediate IAS RADIUS proxies can provide this service.

Without RADIUS proxies, each authenticating switch sends its RADIUS requests to one or multiple RADIUS servers and detects unavailable RADIUS servers. The authenticating switch might or might not be balancing the load of RADIUS traffic across multiple RADIUS servers. By using IAS RADIUS proxies, consistent load balancing is used to spread the load of authentication, authorization, and accounting traffic across all the IAS servers in the organization. Additionally, there is a consistent scheme for failure detection and RADIUS server fail over and fail back.

The following configuration is for an organization that uses:

- Active Directory domains.
Active Directory domains contain the user accounts, passwords, and dial-in properties that each IAS server requires to authenticate user credentials and evaluate authorization.
- Multiple IAS servers.
To balance the load of RADIUS authentication, authorization, and accounting traffic, there are multiple IAS servers.
- Remote access policies.
Remote access policies are configured to specify, based on group membership, the different types of connection constraints for users.
- Two IAS RADIUS proxies.
Two IAS RADIUS proxies are used to provide fault tolerance for RADIUS requests that are sent from the authenticating switches.

Figure 3 shows the use of IAS RADIUS proxies to balance the load of RADIUS traffic from authenticating switches across multiple IAS servers.

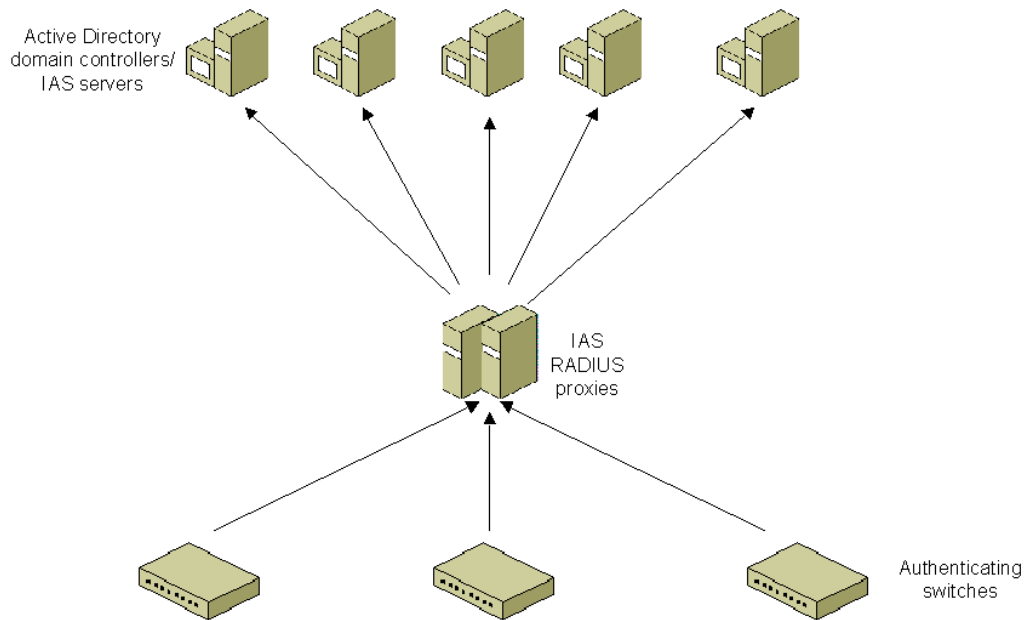


Figure 3 Using IAS RADIUS proxies for load balancing of authentication traffic

To configure IAS for this example, complete the following steps:

1. Configure the Active Directory forests for user accounts and groups.
2. Configure IAS as a RADIUS server on multiple computers.
3. Configure the primary IAS RADIUS proxy.
4. Configure the secondary IAS RADIUS proxy.
5. Configure RADIUS authentication and accounting on authenticating switches.

IAS for Windows 2000 does not support RADIUS proxy. However, you can use IAS in Windows Server 2003 to act as a RADIUS proxy in this configuration. For more information, see the topic titled "Using IAS proxy for load balancing" in Windows Server 2003 Help and Support.

Configuring Active Directory for User Accounts and Groups

To configure Active Directory for user accounts and groups, do the following:

1. On each Windows 2000 domain controller computer, install Windows 2000 SP4 or later.
2. Ensure that all users who are making wired connections have a corresponding user account. Ensure that all computers who are making wired connections have a corresponding computer account.
3. Set the remote access permission on user and computer accounts to the appropriate setting.
4. Organize your accounts into the appropriate groups in order to take advantage of group-based remote access policies.

Configuring IAS as a RADIUS Server on Multiple Computers

To configure IAS as a RADIUS server on each computer, do the following:

1. If you are using Windows 2000 IAS, install IAS as an optional networking component, and then install Windows 2000 SP4 or later. If you are using Windows Server 2003 IAS, install IAS as an optional

networking component.

2. Configure each IAS server computer to read the properties of user accounts in the appropriate domain system containers.
3. If needed, enable logging for accounting and authentication events.
4. Add the IAS RADIUS proxies as RADIUS clients. Verify that you are configuring the correct name or IP address and shared secrets.
5. Create the appropriate remote access policy for wired network access.

Configuring the Primary IAS RADIUS Proxy

To configure the primary IAS RADIUS proxy, do the following:

1. On a computer running Windows Server 2003, install IAS as an optional networking component. The computer on which IAS is installed is not required to be dedicated to forwarding RADIUS messages.
2. If needed, configure additional UDP ports for RADIUS messages that are sent by the authenticating switches. By default, IAS uses UDP ports 1812 and 1645 for authentication and ports 1813 and 1646 for accounting.
3. Add the authenticating switches as RADIUS clients of the IAS server. Verify that you are configuring the correct name or IP address and shared secrets.
4. Use the New Remote RADIUS Server Group Wizard to create a custom remote RADIUS server group. Add each IAS RADIUS server as a member of the remote RADIUS server group and configure each group member with the priority of 1 and a weight of 50 (the default settings).
5. Create a connection request policy that forwards RADIUS request messages to the IAS servers where the realm name matches the accounts in the domain. Use the New Connection Request Policy Wizard to create a connection request policy that forwards connection requests to a remote RADIUS server and where the realm name matches the realm name for the user accounts in the forest. Clear the check box that removes the realm name for authentication. Select the previously created remote RADIUS server group as the group to forward connection requests.
6. Delete the default connection request policy named **Use Windows authentication for all users**.

Configuring the Secondary IAS RADIUS Proxy

To configure the secondary IAS RADIUS proxy on another computer, do the following:

1. On another computer running Windows Server 2003, install IAS as an optional networking component.
2. Copy the configuration of the primary IAS RADIUS proxy to the secondary IAS RADIUS proxy.

Configuring RADIUS Authentication and Accounting on the Authenticating Switches

Configure RADIUS settings on your third-party authenticating switches with the following:

1. The IP address or name of the primary RADIUS server, the common shared secret, UDP ports for authentication and accounting, and failure detection settings.
2. The IP address or name of the secondary RADIUS server, the common shared secret, UDP ports for authentication and accounting, and failure detection settings.

To balance the load of RADIUS traffic between the two IAS RADIUS proxies, configure half of the authenticating switches with the primary IAS RADIUS proxy as the primary RADIUS server and the secondary IAS RADIUS proxy as the secondary RADIUS server and the other half of the authenticating switches with the secondary IAS RADIUS proxy as the primary RADIUS server and the primary IAS RADIUS proxy as the secondary RADIUS server.

For more information, see the documentation for the authenticating switch.

Using Computer-only Authentication

Some network administrators want to use only computer authentication. By using only computer authentication, a client computer must perform computer-level 802.1X authentication with an authenticating switch using either a computer certificate (when using EAP-TLS authentication) or the computer's account name and password (when using PEAP-MS-CHAP v2 authentication) before it can access the organization network. With computer-only authentication, only valid computers can connect to the wired network. Computers that do not have a computer account in the organization's domain cannot connect. This prevents users from bringing computers from home and connecting to the organization's wired LAN. Home computers represent a threat to the organization network because they are not managed in the same way as member computers and can introduce viruses or other malicious programs into the organization network.

For more information about computer authentication and user authentication, see the "[Windows XP Wireless Deployment Technology and Component Overview](http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.mspx)" article at <http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.mspx>.

To configure computer-only authentication for wired clients, all the Windows-based wired clients must have the following registry value set:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\EAPOL\Parameters\General\Global\AuthMode=2
```

With the AuthMode setting set to 2, only computer authentication is attempted. User authentication is never attempted.

To add this registry setting on all of your wired clients computers running Windows, you can use the following tools:

- Regini.exe from the [Windows 2000 Server Resource Kit Tools](#)
- Reg.exe from the [Windows Server 2003 Resource Kit Tools](#)

In both cases, you create a script file that is read by the tool to add a registry setting. The tool has to be run in the security context of a local administrator account.

Alternately, you can use network management software to change registry settings on managed computers.

Summary

You can perform IEEE 802.1X authentication for wired connections with PEAP-MS-CHAP v2, EAP-TLS, or EAP-MD5 CHAP. For EAP-TLS, you must deploy a certificate infrastructure capable of issuing computer certificates to your IAS servers and both computer and user certificates to your wired client computers and users. For PEAP-MS-CHAP v2, you only need to install computer certificates on the IAS servers, provided that the appropriate root CA certificates are already installed on the wired clients. Regardless of the authentication method, you must manage your Active Directory users and groups for wired access, configure your IAS servers as RADIUS servers to the authenticating switches, and configure your authenticating switches as RADIUS clients to the IAS servers. You can also configure Internet access for business partners, use third-party CAs, and use IAS RADIUS proxies for cross-forest authentication or load balancing.

Related Links

See the following resources for further information:

- [Windows 2000 Service Pack 4 \(SP4\)](http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp) at <http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/default.asp>
- [Internet Authentication Service Web site](http://www.microsoft.com/windowsserver2003/technologies/ias/default.mspx) at <http://www.microsoft.com/windowsserver2003/technologies/ias/default.mspx>
- [Security Services Web site](http://www.microsoft.com/windowsserver2003/technologies/security/default.mspx) at <http://www.microsoft.com/windowsserver2003/technologies/security/default.mspx>.
- [Windows XP Wireless Deployment Technology and Component Overview](http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.mspx) at <http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wificomp.mspx>.
- [Troubleshooting Windows XP IEEE 802.11 Wireless Access](http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wifitrbl.mspx) at <http://www.microsoft.com/technet/prodtechnol/winxpro/maintain/wifitrbl.mspx>.

For the latest information about Windows XP, see the [Windows XP Web site](http://www.microsoft.com/windowsxp) at <http://www.microsoft.com/windowsxp>.