



Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2 Wireless Authentication

Microsoft Corporation

Published: October 2003

Updated: January 2005

Abstract

Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2) provides secure wireless authentication using passwords. To use PEAP-MS-CHAP v2, the Internet Authentication Service (IAS) Remote Authentication Dial-In User Service (RADIUS) servers performing wireless authentication need a computer certificate and wireless clients need to trust the computer certificate of the IAS server. VeriSign, Inc. has partnered with Microsoft® to allow mutual customers to easily obtain and install a VeriSign WLAN Server Certificate, a computer certificate for IAS servers performing PEAP-MS-CHAP v2 authentication.

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.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, Windows, and Windows Server 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
PEAP Overview.....	1
MS-CHAP v2 Overview	1
PEAP Support in Windows.....	2
Installing a VeriSign Certificate	3
Step 1: Completing the VeriSign Enrollment Form.....	3
Step 2: Checking Your Email for a Message From VeriSign.....	4
Step 3: Retrieving Your WLAN Server Certificate	4
Step 4: Installing the WLAN Server Certificate	4
Summary	7
Related Links	8

Introduction

In Microsoft® Windows® XP with no service packs installed, secure wireless authentication used the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication method. Although EAP-TLS provides a secure authentication method, it requires the deployment of a public key infrastructure (PKI) to issue user certificates to wireless clients and computer certificates to wireless clients and Remote Authentication Dial-In User Service (RADIUS) servers, such as the Microsoft Windows Server™ 2003 or Windows 2000 Server Internet Authentication Service (IAS).

With Windows XP Service Pack 1 (SP1), Windows XP Service Pack 2 (SP2), Windows Server 2003, and Windows 2000 Service Pack 4 (SP4), secure wireless authentication can also be achieved using Protected EAP (PEAP) and Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2).

PEAP Overview

Although EAP provides authentication flexibility through the use of EAP types, the entire EAP conversation might be sent as plaintext (unencrypted). A malicious user with access to the media can inject packets into the conversation or capture the EAP messages from a successful authentication for analysis. This is especially problematic for wireless connections, in which the malicious user can be located outside of your business. EAP occurs during the IEEE 802.1X authentication process, before wireless frames are encrypted with Wired Equivalent Privacy (WEP).

PEAP is an EAP type that addresses this security issue by first creating a secure channel that is both encrypted and integrity-protected with TLS. Then, a new EAP negotiation with another EAP type occurs, authenticating the network access attempt of the client. Because the TLS channel protects EAP negotiation and authentication for the network access attempt, password-based authentication protocols that are normally susceptible to an offline dictionary attack can be used for authentication in wireless environments.

MS-CHAP v2 Overview

MS-CHAP v2 is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS-CHAP v2 was originally designed by Microsoft as a Point-to-Point Protocol (PPP) authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections.

Although MS-CHAP v2 provides better protection than previous PPP-based challenge-response authentication protocols, it is still susceptible to an offline dictionary attack. A malicious user can capture a successful MS-CHAP v2 exchange and methodically guess passwords until the correct one is determined. Using the combination of PEAP with MS-CHAP v2, the MS-CHAP v2 exchange is protected with the strong security of the TLS channel.

For detailed information about PEAP-MS-CHAP v2 authentication process, see [IEEE 802.11 Wireless LAN Security with Microsoft Windows XP](#).

PEAP Support in Windows

Windows XP with SP1, Windows XP with SP2, Windows Server 2003, and Windows 2000 SP4 wireless clients support PEAP-MS-CHAP v2. For authentication servers, IAS for Windows Server 2003 and Windows 2000 Server SP4 supports PEAP-MS-CHAP v2.

PEAP with MS-CHAP v2 requires certificates on the IAS servers but not on the wireless clients. IAS servers must have a certificate installed in their Local Computer certificate store. Instead of deploying a PKI, you can purchase individual certificates from a third-party CA to install on your IAS servers. To ensure that wireless clients can validate the IAS server certificate chain, the root CA certificate of the CA that issued the IAS server certificates must be installed on each wireless client.

Windows wireless clients include the root CA certificates of many third-party CAs. If you purchase your IAS server certificates from a third-party CA that corresponds to an included root CA certificate, no additional wireless client configuration is required. If you purchase your IAS server certificates from a third-party CA for which your Windows wireless clients do not include a corresponding root CA certificate, you must install the root CA certificate on each wireless client.

Installing a VeriSign Certificate

VeriSign, Inc., working with the Microsoft Corporation, has created a Web site and process to purchase and obtain computer certificates to be installed on IAS servers for PEAP-MS-CHAP v2 authentication of wireless connections. The VeriSign computer certificates are known as VeriSign WLAN Server Certificates. The root CA certificate of the issuing CA of the VeriSign WLAN Server Certificate is already installed on computers running Windows XP, Windows Server 2003, and Windows 2000 SP4. The root CA certificate for VeriSign WLAN Server Certificate can be viewed in the Trusted Root Certificate Authorities\Certificates folder of the Certificates snap-in. It has the friendly name of **VeriSign Class 3 Primary CA** (as listed in the **Friendly Name** column) and the expiration date of **8/1/2028**.

To obtain a VeriSign WLAN Server Certificate for each of your IAS servers that are providing authentication and authorization for PEAP-MS-CHAP v2-based wireless connections, do the following:

- Step 1: Complete the VeriSign enrollment form
- Step 2: Check your email for a message containing instructions about how to retrieve your WLAN Server Certificate.
- Step 3: Retrieve your WLAN Server Certificate.
- Step 4: Install the WLAN Server Certificate on the IAS server computer.

The recommended method of installing a VeriSign WLAN Server Certificate is to perform these steps from the IAS server computer. If this is not possible or desired, then you can perform these steps from an administrator computer and then export the WLAN Server Certificate from the administrator computer and import it on the IAS server computer. The additional procedures to perform the certificate export and import are included in the "Step 4: Installing the WLAN Server Certificate" section of this article.

Step 1: Completing the VeriSign Enrollment Form

To complete the VeriSign enrollment form, do the following:

1. Go to the IAS server computer on which you want to install a WLAN Server Certificate and login.
2. Run Microsoft Internet Explorer or any other Internet browser that is installed.
3. Use the Internet browser to access the [Wireless LAN Server Certificates Web page](http://www.verisign.com/products-services/security-services/ssl/wireless-lan-security/index.html) at <http://www.verisign.com/products-services/security-services/ssl/wireless-lan-security/index.html>.
4. From the Wireless LAN Server Certificates page, click **Buy Now** to begin the enrollment and payment process. The categories of information needed by VeriSign for the WLAN Server Certificate might include the following:
 - WLAN Server Certificate information
 - A challenge phrase
 - Technical contact information
 - Organizational contact information
 - Billing contact information

- Payment information
5. Complete the VeriSign enrollment process.

Step 2: Checking Your Email for a Message From VeriSign

You will receive a message from VeriSign sent to the email address given during the VeriSign enrollment process. The email message will contain a Uniform Resource Locator (URL) to a Web page and a Personal Identification Number (PIN) that you will use to retrieve your WLAN Server Certificate.

Step 3: Retrieving Your WLAN Server Certificate

To retrieve your WLAN Server Certificate, do the following:

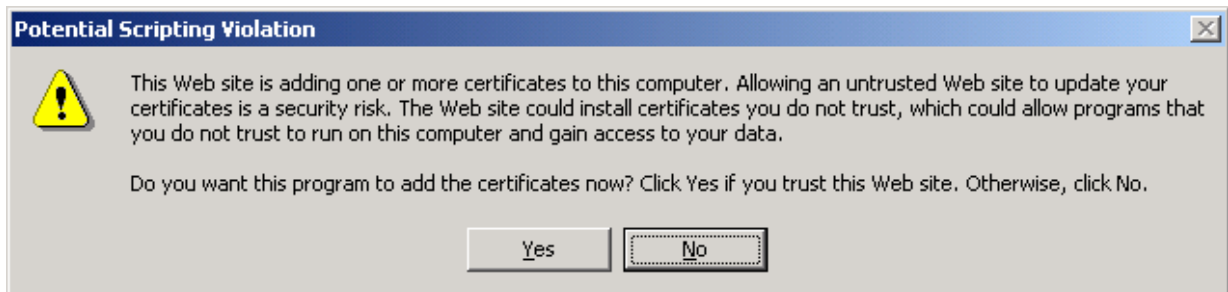
1. Print a copy of the email message from VeriSign that contains the URL and PIN number needed to retrieve your certificate.
2. Go to the IAS server computer that you used to complete the VeriSign enrollment and login using an account that has local administrator permissions. Step 4 of the VeriSign WLAN Server Certificate installation process automatically installs the WLAN Server Certificate in the Local Computer certificate store. To allow this, you must be using a Local Administrator account.
3. Run the same Internet browser that you used in the "Step 1: Completing the VeriSign Enrollment Form" section.
4. Use the Internet browser to access the Web location specified in the email message.
5. When prompted, type and submit the PIN from the contents of the email message.

Step 4: Installing the WLAN Server Certificate

To install the WLAN Server Certificate, do the following:

1. When prompted, click the appropriate button to install the certificate.

You should see a message similar to the following:



2. Click **Yes**. You now have a WLAN Server Certificate installed in your Certificates (Local Computer)\Personal\Certificates folder.

To use the Certificates snap-in to verify that the WLAN Server Certificate is installed, do the following:

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 **Certificates**, click **Computer Account**, and then click **Next**.

4. Click **Local Computer** and then click **Finish**.
5. Click **Close**.

Certificates (Local Computer) appears on the list of selected snap-ins for the new console.

6. In the console tree, open **Certificates (Local Computer)**, open **Personal**, and then click **Certificates**.

In the details pane, you should see a certificate with the **Issued To** name set to the name specified during the enrollment process.

7. To view the details of the certificate, double click it in the details pane.

If you performed the VeriSign WLAN Server Certificate enrollment and installation process on an administrator computer, you must perform the following to install the WLAN Server Certificate on the IAS server:

1. On the administrator computer, create a Certificates (Local Computer) console using steps 1-5 in the previous procedure (if needed).

2. Open **Certificates (Local Computer)** and then **Personal**, and then click **Certificates**.

In the details pane, you should see a certificate with the **Issued To** name set to the name specified during the enrollment process.

3. In the details pane, click the WLAN Server Certificate.

4. On the **Action** menu, point to **All Tasks**, and then click **Export**.

5. On the **Welcome to the Certificate Export Wizard** page of the Certificate Export Wizard, click **Next**.

6. On the **Export Private Key** page, click **Yes, export the private key**, and then click **Next**.

7. On the **Export File Format** page, click **Include all certificates in the certification path if possible** and then click **Next**.

8. On the **Password** page, type the password that will be used to import the certificate on the IAS server computer in **Password** and **Confirm password**, and then click **Next**.

9. On the **File to Export** page, type the name of the file to contain the exported WLAN Server Certificate in **File name**.

10. On the **Completing the Certificate Export Wizard** page, click **Finish**.

11. Copy the file specified in step 9 to the IAS server computer.

12. Log on to the IAS server computer using an account that has local administrator privileges.

13. Use steps 1-5 in the previous procedure to create a Certificates (Local Computer) console containing the Certificates (Local Computer) snap-in.

14. Open **Certificates (Local Computer)** and then click **Personal**.

15. On the **Action** menu, point to **All Tasks** and then click **Import**.

16. On the **Welcome to the Certificate Import Wizard** page of the Certificate Import Wizard, click **Next**.

17. On the **File to Import** page, type the name of the pfx file copied to the IAS server computer in step 11 or click **Browse** to specify the file type of **Personal Information Exchange (*.pfx, *.p12)** and the

location of the pfx file.

18. On the **Password** page, type the password specified in step 8, and then click **Next**.
19. On the **Certificate Store** page, by default **Place all certificates in the following store** is selected with the **Personal** certificate store. If not, click **Browse** to specify the Personal store. Click **Next**.
20. On the **Completing the Certificate Export Wizard** page, click **Finish**.

To configure your IAS server for additional settings to allow PEAP-MS-CHAP v2-based authenticated wireless connections, see [Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows](#).

Summary

VeriSign, Inc. has partnered with Microsoft to provide a quick and easy method to obtain computer certificates for IAS servers that are providing PEAP-MS-CHAP v2-based wireless access authentication. Obtaining a WLAN Server Certificate from VeriSign is a four-step process consisting of filling out a Web enrollment form, checking your email for instructions about how to obtain your certificate, following the instructions in the email to access a Web page that verifies a PIN number, and then installing the WLAN Server Certificate in the Local Computer certificate store on the IAS server computer.

Related Links

See the following resources for further information:

- [Wi-Fi](http://www.microsoft.com/wifi) at <http://www.microsoft.com/wifi>
- [Internet Authentication Service](http://www.microsoft.com/ias) at <http://www.microsoft.com/ias>
- [Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows](http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/) at <http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/>
- [PEAP with MS-CHAP Version 2 for Secure Password-based Wireless Access](http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0702.asp) at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0702.asp>

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003) at <http://www.microsoft.com/windowsserver2003>.