

DigitalPersona® Privacy Manager Pro

DigitalPersona Privacy Manager Pro is a centrally-managed secure communication solution for businesses. It allows sensitive documents and communications to remain private, secure and unaltered wherever they are transmitted or stored.

With Privacy Manager Pro, you can digitally sign and encrypt Microsoft® Outlook email, Office documents and Windows® Live Messenger instant messages with the touch of a finger or a password. Your business now gets per-person accountability and fine-grained control over access to electronic documents and communication, without sacrificing productivity or ease of use. This makes it easier for organizations to comply with the growing demands of regulatory compliance and corporate loss prevention mandates.

Privacy Manager Pro can be layered on top of DigitalPersona Pro's fingerprint identity solution to provide a higher level of convenience and security than lengthy passwords. In addition, businesses have increased assurance that the signature truly represents the indicated person.

This Guide and the DigitalPersona Privacy Manager Pro software it describes are furnished under license as set forth in the applicable End User License Agreement (the "EULA"), which is located in the product package. The contents of this Guide are furnished for informational use only and are subject to change without notice.

Contents

The purpose of this guide is to give you information that you need in order to begin using DigitalPersona Privacy Manager Pro. It covers the basics of installing the program, and introduces the major features of the program. There are many more exciting features available in the software than we can cover in this guide and still keep the Quick Start Guide "quick." Make sure to read the online Help after the software is installed. If you will be administering multiple installations of the software, you will want to read the DigitalPersona Pro Administration Guide as well, included in the product package.

Additional Resources

Use the following resources for additional information about this product:

- The Readme.txt file containing last minute information is included in the product package.
- AskPersona.com (<http://askpersona.com>) is a Pro Knowledge Portal providing answers to many frequently asked questions about Pro Server, Workstation and Kiosk and Privacy Manager Pro.
- DigitalPersona Maintenance and Support customers will find additional information about technical support resources in their Maintenance and Support confirmation email.
- Online Help is accessible from the client after it is installed.

Table of Contents

<i>Installing the DigitalPersona Privacy Manager Pro client</i>	2
<i>Opening Privacy Manager</i>	3
<i>Installing a Privacy Manager certificate</i>	3
<i>Managing your Trusted Contacts</i>	5
<i>Using Privacy Manager Pro In Microsoft Outlook</i>	7
<i>Using Privacy Manager in a Microsoft Office document</i>	9
<i>Using Privacy Manager in Windows Live Messenger</i>	12

System Requirements

Privacy Manager requires the following:

- Microsoft Windows Vista® or Windows® XP operating system
- Microsoft Outlook 2003 or 2007
- Microsoft Office 2007 for Office-related features
- Windows Live Messenger 8.1 or above for Secure Chat features
- Valid e-mail account

A Privacy Manager Certificate (a digital certificate) must be installed in Privacy Manager Pro before you can access the security features. For information on installing a Privacy Manager Certificate, refer to *Installing a Privacy Manager certificate* on page 3.

You can add fingerprint authentication to Privacy Manager by installing one of the following products:

- DigitalPersona Pro Workstation 4.2 and later
- DigitalPersona Personal 3.0 and later
- Without one of the above-listed products, you can still use all of the Privacy Manager Pro features, but instead of authenticating with your fingerprints, you will authenticate using your Windows password.

Installing the DigitalPersona Privacy Manager Pro client

The DigitalPersona Privacy Manager Pro client can be installed and used as a standalone product, or in an enterprise deployment that is managed through the use of an Active Directory administrative template.

The ability to verify your identity with your fingerprint requires the additional installation of either DigitalPersona Pro Workstation or DigitalPersona Personal. This guide assumes that you have already installed one of these programs.

Refer to the DigitalPersona Privacy Manager Pro Administrator Guide located in the product package for information on system configuration and deployment options.

Opening Privacy Manager

To open Privacy Manager:

- In Microsoft Outlook 2003, you can access Privacy Manager features by clicking the Privacy icon on the Outlook toolbar.
- In Microsoft Outlook 2007, you can access Privacy Manager features by clicking Send Securely in the Privacy Group on the Message tab or by clicking the Privacy icon on the Outlook toolbar.
- In Microsoft Office 2007 documents, you can access Privacy Manager by clicking on Sign and Encrypt in the Privacy group on the Home tab.
- To Start a Secure Chat, click Start, All Programs, Privacy Manager, Start Chat.
- To display the Privacy Manager Properties dialog, click Start, All Programs, Privacy Manager, Privacy Manager Properties.
- To open the Live Messenger History Viewer, click Start, All Programs, Privacy Manager, Live Messenger History Viewer.

Installing a Privacy Manager certificate

Before you can use any Privacy Manager features, you must install a Privacy Manager Certificate (from within Privacy Manager).

If requesting a digital certificate from within Privacy Manager, you will need a valid e-mail address, set up as an account within Microsoft Outlook, on the same computer from which you are requesting the Privacy Manager Certificate.

The exact steps in the installation process will depend on how your administrator has configured the software in your organization.

There are three scenarios for installing a Privacy Manager certificate.

Obtaining a preassigned Privacy Manager Corporate Certificate

Your IT administrator may have obtained a corporate certificate from a partnered certificate authority, Comodo, which is then distributed to you through an email.

1. In Outlook, open the email that you received indicating that a Corporate Certificate has been preassigned to you.
2. Click **Obtain**.
3. You will receive an additional email in Microsoft Outlook with your Privacy Manager Certificate attached.
4. To install the certificate, refer to the topic *Setting up a Privacy Manager Certificate* on page 4.

Requesting a Privacy Manager Certificate

If your IT administrator has not prohibited it, you may request a Privacy Manager certificate from a partnered certificate authority, Comodo. The certificate is offered with a free trial period and may be easily renewed through Comodo.

1. Open Privacy Manager, and click the **Certificate** tab.
2. Click **Request a Privacy Manager Certificate**.
3. Follow the on-screen instructions.
4. On the “Certificate Request Accepted” page, click **Finish**.
5. Click **OK** to close the dialog.

You will receive an e-mail in Microsoft Outlook with your Privacy Manager certificate attached.

Installing Other certificates

Your IT administrator may have installed a non-Comodo (Other) certificate on your computer in the Windows Personal Certificate Store, which you can view in the Control Panel by clicking Internet Options, selecting the Content tab and clicking the Certificates button. The certificate may also be sent to you in a PFX (Personal Information Exchange) file.

1. Open Privacy Manager, and click the **Certificate** tab.
2. Click **Import certificates**.
3. Select **Installed certificates** or **Personal Information Exchange file - PKCS #12(.PFX)**.
4. Follow the on-screen instructions.

Setting up a Privacy Manager Certificate

1. When you receive the e-mail with your Privacy Manager Certificate attached, open the e-mail and click the **Setup** button, in the lower-right corner of the message in Outlook 2007, or in the upper-left corner in Outlook 2003.
2. Follow the on-screen instructions.
3. If you choose to begin the Trusted Contact invitation process, follow the instructions beginning with step 2 of the topic Adding Trusted Contacts using your Microsoft Outlook address book.

– or –

If you click Cancel, refer to Managing Trusted Contacts for information on adding a Trusted Contact at a later time.

Managing your Trusted Contacts

There are three ways to create a Trusted Contact, as described in the next three topics.

Adding Trusted Contacts using Microsoft Outlook Contacts

1. On the Microsoft Outlook toolbar, click the **Privacy** button and then click **Invite My Outlook Contacts**.
2. When the “Trusted Contact Invitation” page opens, select the email addresses of the recipients you want to add as Trusted Contacts and then click **Next**.
3. When the “Sending Invitation” page opens, click **Finish**.

An e-mail listing the selected Microsoft Outlook e-mail addresses is automatically generated.
4. Edit the text and add your name (optional).
5. Click **Send**. If you have not obtained a Privacy Manager Certificate, a message informs you that you must have a Privacy Manager Certificate in order to send a Trusted Contact request. Click **OK** to launch the Certificate Request Wizard. Refer to the help topic, “Requesting and installing a Privacy Manager Certificate” for more information.
6. Authenticate using your chosen security login method. This will also add your digital signature to the email invitation.

When the e-mail is received by the Trusted Contact recipient, the recipient must open the e-mail and click **Accept**, and then click **OK** when the confirmation dialog box opens.
7. When you receive an e-mail response from a recipient accepting the invitation to become a Trusted Contact, click the **Accept** button. A dialog box opens, confirming that the recipient has been successfully added to your Trusted Contacts list.
8. Click **OK**.

Adding a Trusted Contact through e-mail exchange

Adding a Trusted Contact through e-mail exchange is a simple 3-step process:

1. You send an e-mail invitation to a Trusted Contact recipient.
2. The Trusted Contact recipient responds to the e-mail.
3. You receive the e-mail response from the Trusted Contact recipient, and click **Accept**.

In order to respond to your invitation to become a Trusted Contact, a recipient must have DigitalPersona Privacy Manager Pro or Privacy Manager for HP Protect Tools installed on their computer. Information on obtaining and installing DigitalPersona Privacy Manager Pro can be found at: <http://www.digitalpersona.com/privacymanager/download>.

More detailed instructions for adding a Trusted Contact by inviting someone to exchange Privacy Manager certificates with you are shown below:

1. Open Privacy Manager, click Trusted Contacts Manager, and then click Invite Contacts.

– or –
On the Microsoft Outlook toolbar, click the Privacy button, and then click Invite Contacts.
2. If the Select Certificate dialog box opens, click the Privacy Manager Certificate you want to use, and then click OK.
3. When the Trusted Contact Invitation dialog box opens, read the text, and then click **OK**. An e-mail is automatically generated.
4. Enter one or more e-mail addresses of the recipients you want to add as Trusted Contacts. Separate multiple addresses with semicolons (;).
5. Edit the text and add your name (optional).
6. Click **Send**.

If you have not obtained a Privacy Manager Certificate, a message informs you that you must have a Privacy Manager Certificate in order to send a Trusted Contact request. Click **OK** to launch the Certificate Request Wizard. Refer to “Requesting and installing a Privacy Manager Certificate” in the online help for more information.

7. Authenticate using your chosen security login method. This will also add your digital signature to the email invitation.

When the e-mail is received by the Trusted Contact recipient, the recipient must open the e-mail and click Accept in the lower-right corner of the e-mail, and then click OK when the confirmation dialog box opens.

8. When you receive an e-mail response from a recipient accepting the invitation to become a Trusted Contact, click Accept in the lower-right corner of the e-mail.

A dialog box opens, confirming that the recipient has been successfully added to your Trusted Contacts list.

9. Click **OK**.

Adding a Trusted Contact using certificates published to Active Directory

Your IT administrator may have set a GPO policy to have digital certificates automatically published to Active Directory. If so, you do not have to exchange certificates through email, but can simply add people as your Trusted Contacts using their Outlook email address or Active Directory domain username.

You can also manually publish digital certificates, if your IT administrator has set the GPO policy to allow it, by clicking **Advanced** on the **Certificate** tab.

Using Privacy Manager Pro In Microsoft Outlook

When Privacy Manager Pro is installed, a Privacy *button* is displayed on the Microsoft Outlook toolbar, and a Privacy *group* is added to the Ribbon of each Microsoft Outlook e-mail message. When you click the down arrow next to the Privacy button, or the down arrow next to Send Securely in the Privacy group, you can choose from the following options:

- Sign and Send (for messages only)—This option adds a digital signature to the e-mail and sends it after you authenticate using your chosen security login method.
- Seal for Trusted Contacts and Send (for messages only)—This option adds a digital signature, encrypts the e-mail, and sends it after you authenticate using your chosen security login method.
- Invite Contacts—This option allows you to send a single Trusted Contact invitation to one or more e-mail addresses.
- Invite My Outlook Contacts—This option allows you to send individual Trusted Contact invitations to selected contacts from your Microsoft Outlook address book. Refer to Adding Trusted Contacts using your Microsoft Outlook address book for more information.
- Certificate Manager—This option allows you to manage your Privacy Manager certificates, including requesting a certificate, importing a certificate, view see certificate details and set various certificate defaults. Refer to the topic “Managing Privacy Manager Certificates” in the online help for more information.
- Trusted Contacts Manager—This option provides a means for you to manage your Trusted Contacts, including inviting others to be your Trusted Contacts, viewing Trusted Contact details and deleting Trusted Contacts. Refer to the topic “Managing Trusted Contacts” in the online help for more information.
- Settings—This option allows you to change the default behavior of the Send Securely button and other settings. Refer to the topic “Configuring Privacy Manager for Microsoft Outlook” in the online help for more information.

Signing and sending an e-mail message

1. In Microsoft Outlook, click **New** or **Reply**.
2. Type your e-mail message.
3. Click the down arrow next to Send Securely (Privacy in Outlook 2003), and then click **Sign and Send**.
4. Authenticate using your chosen security login method.

Sealing and sending an e-mail message

Sealed e-mail messages that are digitally signed and sealed (encrypted) can only be viewed by people you choose from your Trusted Contacts list.

To seal and send an e-mail message to a Trusted Contact:

1. In Microsoft Outlook, click New or Reply.
2. Type your e-mail message.
3. Click the down arrow next to Send Securely (Privacy in Outlook 2003), and then click **Seal for Trusted Contacts and Send**.
4. Authenticate using your chosen security login method.

Using Privacy Manager in a Microsoft Office document

After you install your Privacy Manager Certificate, a Sign and Encrypt button is displayed on the right side of the toolbar of all Microsoft Word, Microsoft Excel, and Microsoft PowerPoint documents. When you click the down arrow next to Sign and Encrypt, you can choose from the following options:

- Sign Document—This option adds your digital signature to the document.
- Add Signature Line Before Signing (Microsoft Word and Microsoft Excel only)—By default, a signature line is added when a Microsoft Word or Microsoft Excel document is signed or encrypted. To turn this option off, click Add Signature Line to remove the check mark. This behavior can also be changed on the Settings tab in the Privacy Manager Properties dialog.

If *Add Signature Line* is unchecked, the only way to see the signature is to click the Digital Signature icon on the bottom toolbar.

- Encrypt Document—This option adds your digital signature and encrypts the document.
- Remove Encryption—This option removes encryption from the document.
- Certificate Manager—This option allows you to manage your Privacy Manager certificates. Refer to the online help topic “Managing Privacy Manager Certificates” for more information.
- Trusted Contacts Manager—This option provides a means for you to manage your Trusted Contacts. Refer to the online help topic “Managing Trusted Contacts” for more information.
- Settings—This option allows you to change the default behavior of the Send Securely button and other settings. Refer to the online help topic “Configuring Privacy Manager for Microsoft Office” for more information.

Signing a Microsoft Office document

1. In Microsoft Word, Microsoft Excel, or Microsoft PowerPoint, create and save a document.
2. Click the down arrow next to **Sign and Encrypt**, and then click **Sign Document**.
3. Authenticate using your chosen security login method.
4. When the confirmation dialog box opens, read the text, and then click **OK**.

To add multiple signatures to a Microsoft Office document:

1. From the menu, select **Insert**.
2. In the Text group, click the down arrow next to **Signature Line**.
3. Select **Privacy Manager Signature Provider**.

4. Type the name of the suggested signer and any instructions to the signer that you want to appear below the signature line. Optionally, select additional options available in the dialog.
5. Repeat the above steps for additional signature lines.

If you later decide to edit the document, follow these steps:

1. Click the Office button in the upper-left corner of the screen. Click **Prepare**, and then click **Mark as Final**.
2. When the confirmation dialog box opens, click **Yes**, and continue working.
3. When you have completed your editing, sign the document again.

Note: After the document is signed, neither the sender or receiver can make further changes to the document without invalidating the signatures, including saving the file to a different format.

Warning: Saving a signed document as a PDF will save the *image* of the signature as shown on the screen in the Office document. It may appear as though the PDF is signed, but it is *not*. The signature can no longer be considered as valid and cannot be authenticated.

Encrypting a Microsoft Office document

You can encrypt a Microsoft Office document for you and for your Trusted Contacts. When you encrypt a document and close it, you and the Trusted Contact(s) you select from the list must both authenticate before opening it.

To encrypt a Microsoft Office document:

1. In Microsoft Word, Microsoft Excel, or Microsoft PowerPoint, create and save a document.
2. Click the Home menu.
3. Click the down arrow next to Sign and Encrypt and then click **Encrypt** Document. The Select Trusted Contacts dialog box opens.
4. Click the name of a Trusted Contact who will be able to open the document and view its contents. To select multiple Trusted Contact names, hold down the **ctrl** key and click the individual names.
5. Click **OK**.

Viewing an encrypted Microsoft Office document

To view an Office document that has been encrypted using Privacy Manager, on the same computer that it was encrypted on:

1. Open the document.
2. Authenticate using your chosen security login method.

To view an Office document that has been encrypted using Privacy Manager, on the same different computer than the one that it was encrypted on:

1. Privacy Manager must be installed on that computer.
2. Import the Privacy Manager certificate that was used to encrypt the file.

To view an Office document encrypted by someone else, using Privacy Manager:

1. Privacy Manager must be installed on your computer.
1. You must have a Privacy Manager certificate set up and installed through Privacy manager.
2. You must have been selected, during the encryption process, as one of the Trusted Contacts intended to receive the document.

Viewing a signed Microsoft Office document

When a signed Microsoft Office document is opened, a Digital Signatures icon displays in the status bar at the bottom of the document window.

- Click the Digital Signatures icon to toggle display of the Signatures dialog, which displays the name of all users who signed the document and the date each user signed it.
- To view additional details about each signature, right-click a name in the Signatures dialog and select Signature Details.

You do not need to have Privacy Manager or a Privacy Manager Certificate in order to view a signed Microsoft Office document.

Using Privacy Manager in Windows Live Messenger

Privacy Manager adds the following secure communications features to Windows Live Messenger:

- **Secure chat**—Messages are transmitted using the SSL/TLS (Secure Sockets Layer/Transport Layer Security) over XML protocol, the same technology that is used to encrypt and improve the security of e-commerce transactions.
- **Recipient identification**—You can verify the presence and identity of a person before sending a message.
- **Signed messages**—You can electronically sign your messages. Then, if the message is tampered with, it will be marked as invalid when the recipient receives it.
- **Hide/show feature**—You can hide any or all messages in the Privacy Manager Chat window. You can also send a message where the content is hidden. Authentication is required before the message is displayed.
- **Secure chat history**—Logs of your chat sessions are encrypted before they are saved and require authentication in order to be viewed.
- **Automatic locking/unlocking**—You can lock and unlock the Privacy Manager Chat window or set it to lock automatically after a specified period of inactivity.

Starting Privacy Manager Chat

In order to use Privacy Manager Chat, both parties must have Privacy Manager and a Privacy Manager certificate installed. For details about installing a Privacy Manager certificate, see "Requesting and installing a Privacy Manager certificate" in the online help.

1. To start Privacy Manager Chat in Windows Live Messenger, click **Start, All Programs, Privacy Manager, Start Chat**.
2. Privacy Manager sends an invitation to the contact to start Privacy Manager Chat.
3. When the invited contact accepts, the Privacy Manager Chat window opens. If the invited contact does not have Privacy Manager, they will be prompted to download it.

An alternative method of starting a Privacy Manager chat session is:

1. Within Windows Live Messenger, double click an available contact.
2. From the menu of the resulting window, select **Activites** and then **Privacy Manager Chat**.
3. Follow the onscreen instructions.

Chatting in the Privacy Manager Chat window

After starting Privacy Manager Chat, a Privacy Manager Chat window opens in Windows Live Messenger.

Using Privacy Manager Chat is similar to using basic Windows Live Messenger, except that the following additional features are available in the Privacy Manager Chat window:

- **Save** - Click this button to save your chat session to the folder specified in your configuration settings. You can also configure Privacy Manager Chat to automatically save each session when it is closed.
- **Hide all and Show all** - Click the appropriate button to expand or collapse the messages shown in the Secure Communications window. You can also hide or show individual messages by clicking the message header.
- **Are you there?** - Click this button to request authentication from your contact.
- **Lock** - Click this button to close the Privacy Manager Chat window and return to the Chat Entry window. To display the Secure Communications window again, click **Resume the session**, and then authenticate using your chosen security login method.
- **Send** - Click this button to send an encrypted message to your contact.
- **Send signed** - Select this check box to electronically sign and encrypt your messages. Then, if the message is tampered with, it will be marked as invalid when the recipient receives it. You must authenticate each time you send a signed message.
- **Send hidden** - Select this check box to encrypt and send a message showing only the message heading. Your contact must authenticate to read the content of the message.

Viewing chat history

The Privacy Manager Chat History Viewer displays encrypted Privacy Manager Chat session files. Sessions may be saved by clicking **Save** in the Privacy Manager Chat window, or by configuring automatic saving on the **Chat** tab in Privacy Manager.

In the viewer, each session shows the (encrypted) Contact Screen Name, and the date and time the session began and ended. By default, sessions are shown for all e-mail accounts that you have set up. You can use the **Display history for** menu to select only specific accounts to view.

The viewer allows you to perform the following tasks:

- Reveal all sessions
- Reveal sessions for a specific account
- View a session ID
- View a session
- Search sessions for specific text
- Delete a session
- Add or remove columns
- Filter displayed sessions

For more information on each of these functions, see the online help.

To start the Chat History Viewer:

1. Click **Start, All Programs, DigitalPersona Privacy Manager Pro**.
2. Click **Chat History Viewer**.

This Quick Start Guide is simply a brief introduction to the powerful features available in Privacy Manager Pro. For complete details, read the DigitalPersona Privacy Manager Pro Administrator Guide, and the online help that is available on most windows and dialogs throughout the user interface.

Published 09/15/2009



© 2009 DigitalPersona, Inc. All Rights Reserved. DigitalPersona, the DigitalPersona logo and U.are.U are trademarks of DigitalPersona, Inc. registered in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.