Xerox Multifunction Devices

Customer Tips

... for the user

dc02cc0303
July 2, 2003

CentreWare Distribution Server and the Microsoft Outlook Email Security Update

Purpose

This document describes the Microsoft Outlook Email Security Update and how it affects the CentreWare Distribution Server's automated scan to email functionality. It also provides instructions for system administrators that show how to change the email security settings in Microsoft Outlook to allow the Distribution Server to run on a machine without user intervention.

Overview

Information about the Microsoft Outlook Email Security Update was taken from articles at the following sites:

http://www.slipstick.com/outlook/esecup.htm

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q262631

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q263297

http://www.microsoft.com/Office/ORK/2000/journ/outsecupdate.htm

The Microsoft Outlook Email Security Update changes the way Outlook handles attachments, provides additional levels of protection against malicious email messages, and changes the way other applications communicate with Outlook.

Office 2000 Service Pack 2 and Outlook 2002 include the security update. To find out whether your copy of Outlook includes the security update, open Outlook and select **Help>About Microsoft Outlook**. If the title has the words "Security Update," the patch is installed. If it does not, compare the number with this chart, which lists the versions that contain the security update.

Outlook 97	Not applicable. The security update is not available for Outlook 97
Outlook 98	Version 8.5.7806 and later
Outlook 2000	Version 9.0.0.4201 and later
Outlook 2002	All versions (10.x.x)

This document applies to these Xerox products:

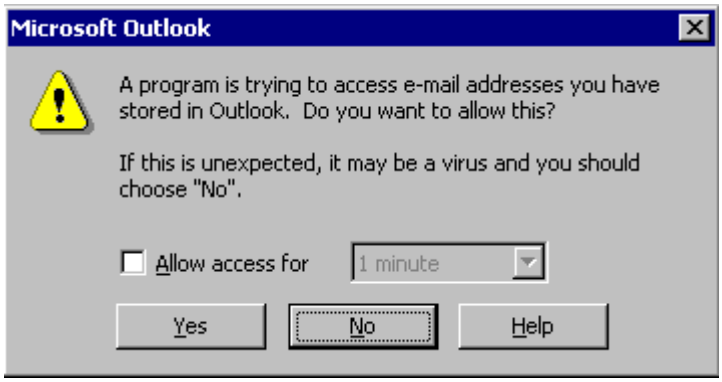
x	WC Pro 32/40 Color
x	WC Pro 65/75/90
x	WC Pro 35/45/55
	WC M35/M45/M55
x	DC 555/545/535
x	DC 490/480/470/460
x	DC 440/432/425/420
x	DC 340/332
x	DC 265/255/240
x	DC 230/220
	DCCS 50

Security Update Pop-up Messages

When the CentreWare Distribution Server runs on a PC that has the Microsoft Outlook Email Security Patch installed, two pop-up messages result when:

- you create a CentreWare email template
- the Distribution Server attempts to send a scanned email job

The first pop-up message occurs when you run the Distribution Template utility and create a scan to email template. In the process of resolving the recipient's email address, the Outlook client returns a pop-up message.



When you click a button, the following occurs:

– If you click [**Yes**], the address is resolved and you can continue to create the scan to email template.

– If you click [**No**] this error message appears, **One or more recipients of the message were invalid or could not be identified**, and you cannot finish the scan to email template.

The second pop-up message occurs when the CentreWare Distribution Server detects a scan to email job and it attempts to send the email note.

The CentreWare Distribution Server is designed to function without user intervention. The second pop-up message poses a problem, especially in environments where the distribution server is in a locked room or is not "manned." Without disabling this security feature, the only recourse is to manually clear the pop-up message by clicking [**Yes**] to allow the CentreWare software to send the email note. After clearing the message, the Distribution Server processes the next email or OCR scan job.

NOTE: Since the first pop-up occurs when you create a template using the PC (and you can easily click [**Yes**] when the pop-up appears), we do not recommend editing the security setting to remove the occurrence of this pop-up. This setting may have other security implications that impact the email client.

Modifying the Default Security Settings

To individualize user restrictions, publish a custom form in an Exchange Server public folder and edit the published form's security settings to allow the CentreWare Distribution Server to send emails without user intervention.

Outlook 2002 Security Feature's Administrative Package

Install the Outlook Security Feature's administrative package (Admpack.exe) on the CentreWare Distribution Server from one of the following places. Use this kit to administer the security update for Outlook 2002 clients.

- The Windows XP Office Resource Kit CD from the \Files\Pfiles\ORK10\Tools\Admpack\ folder
- The Windows XP Office Enterprise Edition CD from the \ORK\Files\Pfiles\ORK10\Tools\Admpack\ folder
- From the Microsoft website at http://www.microsoft.com/office/ork/xp/appndx/appa11.htm

The Admpack.exe file contains the following files:

OutlookSecurity.oft – an Outlook template that enables you to customize the security settings on the Microsoft Exchange Server

Readme.doc –documentation for administrators

Hashctl.dll – a file for the Trusted Code control, a tool used by the template to specify trusted COM add-ins

Comdlg32.ocx – a file for the Trusted Code control, provides a user interface for selecting the trusted COM add-in

Note: This document describes editing Outlook security settings using the Outlook template form only. It does not discuss using Hashctl.dll or Comdlg.ocx to specify Trusted Code control.

Outlook 2000 / 98 Security Feature's Administrative Package

Download Admpack.exe from the Microsoft website and unpack it to a folder on the CentreWare Distribution Server PC. Use this kit to administer the security update for Outlook 2000 and 98 clients. To obtain the Admpack.exe, access the site: http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#secupd and download **Outlook 2000 SR-1a Security Update Administrative Tools — updated August 16, 2001**.

The Admpack.exe file contains the following files:

Readme.txt –documentation for administrators

OutlookSecurity.oft – an Outlook template that enables customized security settings on the Microsoft Exchange Server

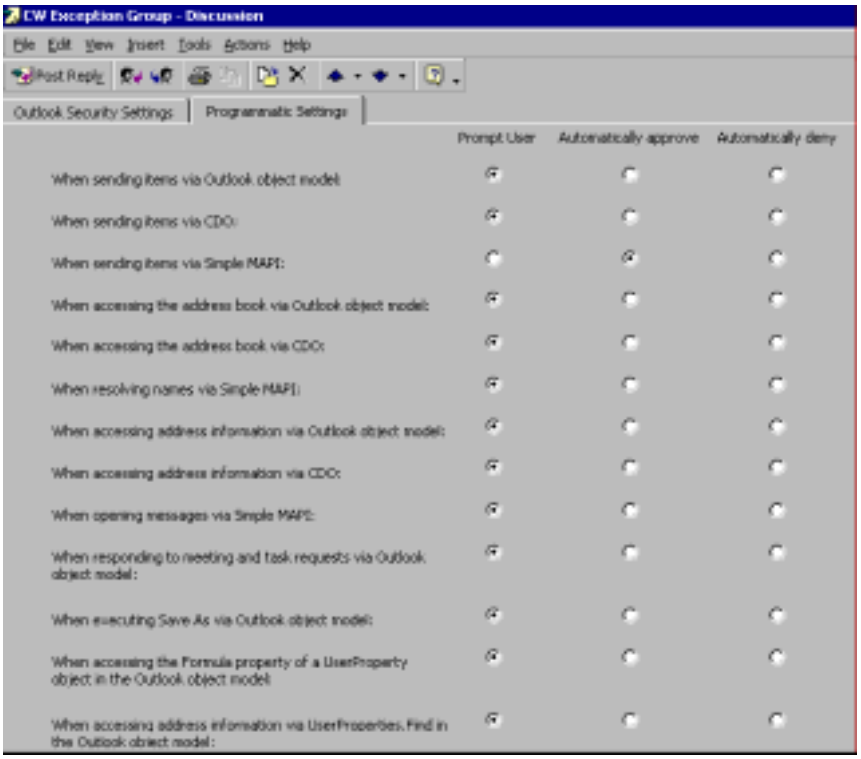
Outlk9.adm – a policy file for computers that are set up with system policies

Modifying Outlook Security Settings

After you run Admpack.exe and unpack the files listed above, use the following steps to create a public folder and install the form.

1. On the Microsoft Exchange Server, create a public folder in the root folder of the Public Folder tree called **Outlook Security Settings** (use that exact folder name). Set the folder Access Control Lists (ACL) so all users can read all items in the folder. Next, set the folder ACL so the CentreWare Distribution Server user has permission to create, edit, or delete items in the folder.
2. On the CentreWare Distribution Server, in the folder where you extracted the Admpack.exe files, double-click OutlookSecurity.oft to open the template.

3. When asked to select a folder, select the **Outlook Security Settings** public folder you created on the Exchange server. The template opens in Compose mode.
4. Select **Tools>Forms>Publish Form**. Type the name **Outlook Security Form** and click [**Publish**]. Close the form and click [**No**] when asked if you wish to save the settings.
5. Switch to the Microsoft Outlook client on the CentreWare Distribution Server.
   - For Outlook 2002 clients, click the drop-down arrow next to [**New**] on the toolbar, and select [**Choose Form**]. Navigate to the template you just created in the previous steps, select **Outlook Security Form** and click [**Open**].
   - For Outlook 2000 and 98 clients, expand **Public Folders**, **All Public Folders**, and **Outlook Security Settings**. Double-click the published form ***Default Security Settings***. Click [**Edit, Revise Contents**].
6. On the **Outlook Security Settings** tab, select the **Security Settings for Exception Group**.
7. Enter a **Security Group Name** (example: CW Exception Group).
8. In the **Members** box, enter the name of the email user that applies to this group of settings. An email user is a Microsoft Outlook user on the CentreWare Distribution Server. The form doesn't provide a button to let you pick names from the Global Address List (GAL); you must enter the names yourself. (TIP: You can use the **To** button on a regular Outlook message item to help you select the names, then copy and paste into the security form item.)
9. Press Ctrl+K to resolve the name. If the name remains without an underline, Outlook couldn't match the name against a valid address book entry. Check your spelling, and then press Ctrl+K to try to resolve again.
10. On the **Programmatic Settings** tab, change the **When sending items via Simple MAPI** option to **Automatically approve**. This setting allows the CentreWare Distribution Server to send emails without any user intervention.



NOTE: If **When resolving names via Simple MAPI** is set to **Automatically approve** you can create email templates without the pop-up message. Since this pop-up occurs when you are at the PC creating templates (and you can easily click

[**Yes**] at the pop-up), we do not recommend using the **Automatically approve** setting. It may have other security implications for email users.

11. Click [**Close**], and [**Yes**] to save changes. Your Scan to E-mail jobs sent by the CentreWare Distribution Server no longer requires user intervention.

IMPORTANT: If a user's name is entered as a member of more than one security group, the settings of the most recently created group apply. Make sure the email user on the CentreWare Distribution Server is a member of only one Outlook security group.

Making a Change to the Windows Registry (Outlook 2000 and 98 clients only)

Make a change to a registry key as the last step to implement custom. You only perform this procedure in Outlook 2000 and 98 client environments. Use the Outlk9.adm file extracted when you ran the Admpack.exe download file to make this change.

NOTE: Users cannot use the exception settings in the Outlook Security Settings folder unless you make the change to their Windows Registry in the following procedure. The Registry setting is a new DWORD value named CheckAdminSettings, which you must create in the HKEY_CURRENT_USER\Software\Policies\Microsoft\Security key.

If you deployed Outlook with system policies, you must change the policies on Exchange Server. This involves removing the current .adm file and replacing it with Outlk9.adm. This file automatically passes your customized security settings to client computers each time they log on to the system.

If Outlook was deployed without system policies, you must modify a registry key directly on the client computers. Outlook respects this new registry key, even if you are not using policies.

See section 2.4 of the readme.txt file included with admpack.exe for more details about rolling out the Registry change to Outlook 2000 using the Outlk9.adm policy file(also part of Admpack.exe). Microsoft has not provided a new policy file for Outlook 98.

Updating the Outlook Policy Template File for Windows 2000

1. On the Start menu, click [**Run**], and then type "gpedit.msc" to start the Group Policy Editor.
2. Expand the following series of folders:

   User Configuration \ Administrative Templates
3. Right-click **Administrative Templates** and select **Add/Remove Templates** on the shortcut menu.
4. If you see **Outlk9** in the **Current Policy Templates** list, select it, and click [**Remove**].
5. Click [**Add**].
6. Use the **Look in** box and locate the folder where you saved the updated Outlk9.adm template. Select **Outlk9.adm**, then click [**Open**].
7. Click [**Close**] to return to the Group Policy Editor.
8. Expand the following series of folders:

   User Configuration \ Administrative Templates\Microsoft Outlook 2000 \ Tools|Options\Security
9. Double-click the Outlook virus security settings policy name.
10. Click [**Enabled**], and then select the **Apply individual settings for Outlook virus security** check box.
11. Click [**Apply**] then [**OK**].

12. Close the **Group Policy** window.

Updating the Outlook Policy Template File for Windows 9.x and Windows NT 4.x

NOTE: The System Policy Editor is included with the Office Resource Kit core tool set, available on the Office Resource Kit Web site at: http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#orktools.

1. On the **Start** menu, select [**Run**] then type **poledit.exe** to start the System Policy editor.
2. On the **Options** menu, select [**Policy Template**].
3. In the **Policy Template Options** list, select **Outlk9.adm**, and click [**Remove**].
4. In the same dialog box, click [**Add**], then browse to the folder where you installed the updated Outlk9.adm template. Select **Outlk9.adm**, then click [**Open**].
5. Click [**OK**].
6. On the **File** menu, select [**Open Registry**], then double-click the **Local User** icon.
7. Expand the following series of folders:

   Microsoft Outlook 2000\Tools|Options\Security

8. Select the **Outlook virus security settings** check box, then select the **Apply individual settings for Outlook virus security** check box in the **Settings for Outlook virus security settings** box.
9. To apply the new policy, click [**OK**].
10. Close the System Policy Editor window and click [**Yes**] to save changes to the registry.

Additional Information

Xerox Customer Service welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA), TTY 1-800-855-2880 or at http://www.xerox.com.

Other Tips about Xerox multifunction devices are available at the following URL: http://www.xerox.com/DocumentCentreFamily/Tips.

THE DOCUMENT COMPANY
XEROX®