

Date: January, 2003
Tech Tip #: CTI000013
Product Line: Corporate Call
Revision: All Revisions

Topic Outlook 2000 E-mail Security Update Issues

Information

Overview

Microsoft's Outlook E-mail Security Update is intended to prevent the spread of malicious attachments and custom code. (See reference 1) Initially when it is installed on a client PC, Outlook is locked down in its most secure mode. While this accomplishes the intended goal, it presents Corporate Call users with numerous warning dialog boxes that must be acted upon before continuing:



This prompting dialog box pops whenever Corporate Call interacts with Outlook. There are two ways to keep these dialogs from popping. One is to permit access; the other is to restrict access.

Permitting access requires downloading and installing an administration tool that allows specific security functions to be controlled. A network administrator must perform this; the user cannot install it.

WARNING: Lowering any default security setting may increase your risk of virus execution or propagation. Use caution and read the documentation before you modify these settings.

Alternatively, access can be restricted by not allowing Corporate Call to store calls or interact with Outlook's Calendar. Using Corporate Call's Configuration Options dialog a user can restrict interaction with Outlook to a point where warning dialogs no longer appear. While this limits the feature set, it can be done without the

Security Update Administration tool. With this method the user will still have to acknowledge a warning dialog on startup. This document outlines the basic steps to installing the security update administration tool. If you choose to restrict Corporate Call's interaction with Outlook, proceed to the section *Administering the Security Update* and follow the *Alternative* instructions for the two sections.

Installing the Security Update

Because of the wide variety of installation options this document provides only basic guidelines. Decisions need to be made by the network administrator concerning how the administration update is to be deployed and who will be granted rights. Additionally the way the policies are deployed on the network and the operating systems of the client PCs will affect how the installation is performed.

First, an administration tool that controls which security parameters are applied to the user needs to be downloaded from Microsoft's website. It consists of two components, an Outlook Security Form Template "OutlookSecurity.oft", and a policy file "Outlk9.adm".

The administration tool "Admpack.exe" is found at:

<http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm#secupd>

After downloading the application "Admpack.exe" and running it, the three files are extracted: Readme.txt, OutlookSecurity.oft, and Outlk9.adm.

"Readme.txt" along with Microsoft's Q263297 (*Reference 2*) contain the most important information for installing and administering the security update. These two documents will guide you through the installation specific to your site's configuration.

"OutlookSecurity.oft" is an Outlook Security Form Template. Controlled by the administrator, it holds the security setting policies. Refer to the readme file and Q263297 for installation details.

"Outlk9.adm" applies the policies set by the Outlook Security Form Template. Refer to the readme file and Q263297 for installation details.

Administering the Security Update

Once the Outlook Security Form Template is installed and policies are added to recognize it, the Security Update settings can be administered. The default state of the items under the Programmatic Settings tab of the Outlook Security Form Template are set to "Prompt User". Any interactions by a third party program (in our case Corporate Call) and Outlook will result in a warning prompt dialog box. Two of these programmatic settings need to be adjusted to allow Corporate Call to function without triggering warning dialog boxes:

1) To disable warning prompt on initial startup and call history logging:

Change: "When accessing address information via Outlook object model"

To: "Automatically Approve"

Alternative: This security policy modification can be avoided if the user is willing to accept a warning dialog prompt on startup and call logging is not required. In Corporate Call's Configuration Option dialog, click on the *Call History* tab and then select the *Do not keep any calls in history* button. The user will still see one warning dialog on start up and must click on *Yes* to proceed.

2) To permit calendar interaction functions to proceed without prompting:

Change "When accessing the address book via Outlook object model"

To: "Automatically Approve"

Alternative: This security policy modification can be avoided if the user disables calendar interactions. In Corporate Call's Configuration Option dialog, click on the *Options* tab and uncheck the *When calling internally, check the called party's calendar to see if they are available* box. Additionally, they will not be able to use the email notification feature for calendar events.

After the changes are made to the Outlook Security Form Template click the "Close" button at the bottom of the form and then exit the form dialog by clicking the "X" box. You will be prompted to save the changes, click "Yes". Outlook must be restarted for these changes to take effect.