Technical Note
201-905-01
February 22, 2000

Using Aviva Web-to-Host Server on Microsoft Windows 2000

Introduction

The information in this technical note applies only to Aviva Web-to-Host Server when installed on a computer that is running the following:

- Microsoft Windows 2000 Server or Advanced Server
- Internet Information Server (IIS) 5.0
- the NTFS file system

Due to new security policies implemented as part of the Windows 2000 operating system, administrators may be required to change the permission settings on some Aviva-related files and folders on the server before users can access sessions through the 3270-to-HTML application.

If permissions are not set correctly, only users who log on to the 3270-to-HTML application as an administrator can run sessions.

Overview

When Aviva Web-to-Host Server is installed on a hard disk formatted with the Windows NT file system (NTFS), new folders created during the installation automatically inherit the same permissions as the parent folders. For example, if C:\PROGRAM FILES gives full control to the Everyone group, then the Everyone group will have full control over the C:\PROGRAM FILES\EICON folder created when Aviva Web-to-Host Server is installed. This is true for both Windows NT and Windows 2000.

However, there is a difference in the way IIS 4.0 and IIS 5.0 manage permissions when they start an external application such as Aviva Web-to-Host Server.

With Windows NT and IIS 4.0, IIS uses the NT AUTHORITY/SYSTEM account to start an application. By default, the application will work because most folders give full permission to the SYSTEM account.

With Windows 2000, which uses IIS 5.0, IIS typically starts an application using the Anonymous User account (the account that was authenticated between the server and the Web browser). By default, the application will not work because the Anonymous User account does not have the required permissions to access application-related files and folders. Administrators of an Aviva Web-to-Host Server installation must ensure that the Anonymous User account is granted permission to access Aviva-related files and folders on the server.

Required permission settings

To run Aviva Web-to-Host Server on Windows 2000, you must ensure that the Anonymous User account is granted the permissions listed below.

- Read & Execute permission for the following folders:
  - WINNT (Aviva requires Read & Execute permission for files such as ILINK2.DLL and some OLE files. It is recommended that you grant Read & Execute permission for the entire folder.)
  - INETPUB\WWWROOT\AVIVAASP
  - PROGRAM FILES\EICON

EICON TECHNOLOGY

- Read & Execute and Write permission for the following folders/files:
  - WINNT\TEMP (Aviva and Windows use this folder to create temporary files)
  - PROGRAM FILES\EICON\AVIVA\[USER OR *USER NAME*]
  - PROGRAM FILES\EICON\EICON SHARED\CONFIG
  - INETPUB\WWWROOT\AVIVAASP\WTHCFG.ECF (This file contains the settings for user options such as default settings, dynamic screen refresh, generate java applets, host color mapping, and keyboard mapping)

Setting permissions

To set file/folder permissions, follow these steps:

Note *In the following procedure,* **IUSR_*computername*** *is used to designate the Anonymous User account. By default, the server creates and uses IUSR_*computername *(the Internet Guest Account) as the Anonymous User account. However, you can set the server to use a different account. If you have chosen to use a different Anonymous User account, you should select that account instead of IUSR_*computername*.*

1. Open Windows Explorer and locate the file or folder for which you want to change permissions.
2. Right-click the file or folder, click **Properties**, and then click the **Security** tab.
3. Click **Add**.
4. In the **Name** list, select **IUSR_*computername*** and click **Add**.
5. Click **OK**.
6. In the **Name** list, select **IUSR_*computername*** and, in the **Permissions** list, do the following:

   To grant Read & Execute permission for a file
   In the **Allow** column, make sure that the **Read & Execute** check box is selected.

   To grant Write permission for a file
   In the **Allow** column, make sure that the **Write** check box is selected.
7. Click OK.