Hot Fix 21WRS01 – SAS© Web Report Studio 2.1

BEFORE DOWNLOADING:

The hot fix 21WRS01 addresses the issue(s) in 2.1 of Web Report Studio software on Windows as documented in the "Issue(s) Addressed" section of the hot fix download page:

http://ftp.sas.com/techsup/download/hotfix/wrs21.html#21wrs01

NOTE:

1. You must have SAS 9.1.3, Service Pack 3 installed on your machine before applying this hotfix.

2. This hotfix ONLY applies to Web Report Studio 2.1 for NEW installations, or existing 1.1 installations which have applied the "upgrade to 2.1" which is available ~ June, 2005.

3. Manual steps are necessary to complete the fix deployment and therefore it is very important that you read the this file entirely before executing the hotfix 21WRS01wn.exe.

AFTER DOWNLOADING:

The hot fix package downloaded is a self extracting executable named 21WRS01wn.exe. Launching the executable will initiate a Java installation application which will deliver the following
files to the Web Report Studio installation path:

* sas.reportstudio.web.jar
  Java installation file containing replacement module for SAS Web Report Studio

MANUAL POST-INSTALLATION STEPS:

Once the install(s) have completed you must run the following manual steps:
* sas.wrs.config.bat for WRS
* Redeploy the .war file

Refer to Install and Deploy documentation (default locations below) for information on the above steps:
C:\Program Files\SAS\SASWebReportStudio\2.1\deployment.html

This completes the installation of hotfix 21WRS01.

ADDITIONAL USAGE INFORMATION:

In addition to the security features of the WebDAV repository, SAS Web Report Studio uses the metadata repository to manage and secure web reports. Web reports are represented as metadata objects and a folder structure is used in the repository to organize reports and to secure access. Metadata access permissions are applied to the folders to provide a secure framework for users to create and edit reports. The ReadMetadata permission is required to view a report. The WriteMetadata permission is required to create or edit or copy a report.

The default installation settings create this folder path for the application:

/BIP Tree/ReportStudio/

Reports that users want to share can be stored in this location:

/BIP Tree/ReportStudio/Shared/Reports

In addition, each user has a personal folder to store reports. The first time a user logs in to Web Report Studio, the application creates a user folder in the repository. The user folder path is created as

/BIP Tree/ReportStudio/Users/<userid>,

with a subfolder for reports,

/BIP Tree/ReportStudio/Users/<userid>/Reports

For the 2.1 release, the user's Reports folder was secured at creation with access permissions that granted ReadMetadata and WriteMetadata to the owner, and denied ReadMetadata and WriteMetadata to the PUBLIC implicit group. The PUBLIC group (or the SASUSERS group, depending on the Default ACT) still had Read Metadata and Write Metadata permissions for the <userid> folder. Additionally, the <userid> folder was created with each user's credentials. This required that the parent folder,

/BIP Tree/ReportStudio/Users,

be maintained with WriteMetadata access for all WRS users (defined as PUBLIC or SASUSERS, depending on the Default ACT).

Hot fix 21WRS01 changes the folder location where these access controls are applied, and the account credential used to apply them. First, owner access controls are now applied to both the <userid> folder and the Reports subfolder. The result is that only the owner can view the <userid> folder and any content below this location.

Second, the privileged administrative account (typically the SAS Web Administrator account, saswbadm) is used to create all user folders. With this change, access to the

Users folder is now secured to only allow WriteMetadata permission to the privileged administrative account.

All new <userid> folders that are created after the hot fix is applied will be secured in this manner. Folders created before application of the hot fix must be secured manually by an administrator. The SAS Management Console Authorization Manager is used to apply Access Control Entries (ACEs) to folders. Refer to the Management Console Help for Authorization Manager. The administrator navigates to the user folder locations and applies ACEs to grant Read Metadata and Write Metadata to the user, and deny Read Metadata and Write Metadata to PUBLIC (or SASUSERS, depending on the Default ACT).

Example

For the 'SAS Demo User' account, sasdemo, Web Report Studio creates this user folder:

/BIP Tree/ReportStudio/Users/sasdemo/

with this subfolder,

/BIP Tree/ReportStudio/Users/sasdemo/Reports

With this hot fix, the user folder,

/BIP Tree/ReportStudio/Users/sasdemo/

will be created with ReadMetadata and WriteMetadata granted for sasdemo, and ReadMetadata and WriteMetadata denied for the PUBLIC group.

The Web Report Studio administrator can make a visual inspection of user folder permissions using the SAS Management Console Authentication Manager. Using the 'Resource Management, By Location' view, and starting at the 'BIP Service' namespace, the administrator can navigate to the Web Report Studio Users folder area and confirm that the correct ACEs, as described above, have been applied.