Applying SAS Security Updates and Hot Fixes

This document contains information about the SAS security updates and product-specific hot fixes that you must apply and the required order in which they must be applied. Applying SAS security updates and hot fixes updates both the SASHOME and SAS Configuration directories.

Some product-specific hot fixes might require you to reapply SAS security updates. If so, follow the instructions in this document to reapply the appropriate SAS security updates, and then rebuild and redeploy web applications.

Before you apply security updates and hot fixes, it is strongly recommended that you back up your SAS deployment. This is the only way that you can restore the SASHOME and SAS Configuration directories to their previous state. Refer to SAS 9.4 Upgrade in Place: System-Level Backup and Recovery Best Practice for instructions.

Important: The following steps must be performed in the order in which they appear, and you must perform all steps that apply to you.

1. Perform **Step 1 — Apply Product-Specific Hot Fixes**.
2. Perform **Step 2 — Apply Java Deserialization Update**. If you are using SAS 9.4M8, **skip this step.**
3. Perform one of the following steps:

    (1) If you are using SAS 9.4M5, perform **Step 3 — Apply SAS Security Update 2018-09**.
    (2) If you are using SAS 9.4M6, perform **Step 4 — Apply SAS Security Update 2022-03-M6**.
    (3) If you are using SAS 9.4M7, perform **Step 5 — Apply SAS Security Update 2023-06-M7**.
    (4) If you are using SAS 9.4M8, perform **Step 6 — Apply SAS Security Update 2023-06-M8.**

4. Perform **Step 7 — Apply Hot Fix Y09009 – Supplemental Hot Fix for SAS Security Updates**
5. Perform **Step 8 — Rebuild and Redeploy Web Applications.**
6. Perform **Step 9 — Apply the SAS Security Update to a Horizontal Middle-Tier Cluster Node**.

Step 1 — Apply Product-Specific Hot Fixes

All deployments should perform this step.

Apply product-specific hot fixes using the following steps:

1. Run the SASHFADD tool to generate a report of other hot fixes that you might want to apply to your deployment.

    Note: When you use the SASHFADD tool, Hot Fix Y09009 and the SAS security updates are not included in the results. Hot Fix Y09009 and the SAS security updates must always be applied as directed in this document.

2. When you have determined which hot fixes to apply to your deployment, use the SASHFADD instructions to download your hot fixes.

3. Perform any pre-installation tasks for each hot fix.

4. Apply the hot fixes.

5. Perform any post-installation tasks for each hot fix. If the post-installation tasks include rebuilding and redeploying web applications, delay these tasks until you reach Step 8 — Rebuild and Redeploy Web Applications.

Step 2 — Apply Java Deserialization Update

Determine Whether Java Deserialization Update Is Needed

Follow these steps for all maintenance levels of SAS 9.4 except for SAS 9.4M8, even if other security updates have been applied.

If you are using SAS 9.4M8, then proceed no further with this step. Skip ahead to perform **Step 6 — Apply SAS Security Update 2023-06-M8**.

To determine whether you have applied the most recent Java Deserialization Update, review the contents of this file:

```
SASHome\InstallMisc\utilities\installqual\9.4\serialization_hotfix.properties
```

If this file does not exist, or if, in the file, the version of the SAS security update is less than 4.0, then you do not have the latest version of the Java Deserialization Update. Continue with these steps to apply the Java Deserialization Update.

If the correct version is listed and you have applied a hot fix, you might be directed to reapply the Java Deserialization Update. If so, please re-apply it to ensure continued system security.

Apply the Java Deserialization Update

Use the following steps to apply the update. These steps should be performed for every machine in your deployment by applying the update on each installed and configured machine.

1. Before beginning, ensure that all active SAS sessions, daemons, spawners, servers, and agents are terminated. In addition, SAS strongly recommends that you back up your system before applying the update.

2. Download the Java Deserialization Update.

3. Unzip `sas-security-update-2020-08.zip` into a directory of your choice. On UNIX, using the `unzip` command is the best option. If you use WinZip or the `jar xvf` command, you must also use the following command to preserve the appropriate permissions:

```
chmod a+x install.sh
```

If the installer ID differs from the update directory owner, make the directory writable by all IDs in the same group with the following command:

```
chmod -R g+w /security directory/sas-security-update-2020-08
```

4. From the directory into which you unzipped, go to the `sas-security-update-2020-08` directory.

5. In that directory, run the appropriate script using the same user ID that was used to install (installer ID). The script requires one argument— the full path to the SASHOME directory where the update is going to be applied.

Windows `install.bat "`*SASHOME*`"`Windows

Example `install.bat "C:\Program`

`Files\SASHome"`

Note: Depending on your settings, you might have to use the **Run as administrator** *option.*

UNIX

`./install.sh "`*SASHOME*`"` **UNIX**

Example

`./install.sh "/usr/lpp/SAS"`

6. The script applies the update to all files in the SASHOME and SAS Configuration directories that need to be updated. When the script finishes, a message states that the update is complete and the script exits.

7. If you plan to deploy other hot fixes or updates from the location where you placed this ZIP file, you need to remove it from this location. The SAS Deployment Manager, which is used for deploying other hot fixes, does not recognize this file and will issue an error.

8. Continue to the next step.

Step 3 — Apply SAS Security Update 2018-09

Determine Whether SAS Security Update 2018-09 Is Needed

If you are not using SAS 9.4M5, skip to **Step 4 — Apply SAS Security Update 2022-03-M6**.

To determine whether you have applied SAS Security Update 2018-09, review the contents of this file:
`SASHome\InstallMisc\utilities\installqual\9.4\security_hotfix.properties`

If this file does not exist, or it does not list the version as 1.0, then you do not have the latest version of the update. Continue with these steps to apply SAS Security Update 2018-09.

If the correct version is listed and you have applied a hot fix, you might be directed to re-apply the update. If so, please re-apply it to ensure continued system security.

Apply SAS Security Update 2018-09

Use the following steps to apply the update. These steps should be performed for every machine in your deployment by applying the update on each installed and configured machine.

1. Before beginning, ensure that all active SAS sessions, daemons, spawners, servers, and agents are terminated. In addition, SAS strongly recommends that you back up your system before applying the update.

2. Download SAS Security Update 2018-09.

3. Unzip `sas-security-update-2018-09.zip` into a directory of your choice. On UNIX, using the `unzip` command is the best option. If you use WinZip or the `jar xvf` command, you must also use the following command to preserve the appropriate permissions:
    `chmod a+x install.sh`

    If the installer ID differs from the update directory owner, make the directory writable by all IDs in the same group with the following command:

```
              chmod -R g+w /security directory/sas-security-update-2018-09
```

4. From the directory into which you unzipped, go to the `sas-security-update-2018-09` directory.

5. In that directory, run the appropriate script using the same user ID that was used to install (installer ID). The script requires one argument— the full path to the SASHOME directory where the update is going to be applied.

   Windows
   ```
   install.bat "SASHOME"
   ```

   Windows Example `install.bat "C:\Program`
   ```
   Files\SASHome"
   ```

   Note: Depending on your settings, you might have to use the **Run as administrator** *option.*

   UNIX
   ```
   ./install.sh "SASHOME"  UNIX
   ```
   Example
   ```
   ./install.sh "/usr/lpp/SAS"
   ```

6. The script applies the update to all files in the SASHOME and SAS Configuration directories that need to be updated. When the script finishes, a message states that the update is complete and the script exits.

7. If you plan to deploy other hot fixes or updates from the location where you placed this ZIP file, you need to remove it from this location. The SAS Deployment Manager, which is used for deploying other hot fixes, does not recognize this file and will issue an error.

8. Continue to the next step.

Step 4 — Apply SAS Security Update 2022-03-M6

Determine Whether SAS Security Update 2022-03-M6 Is Needed

If you are not using SAS 9.4M6, skip to **Step 5** — **Apply SAS Security Update 2023-06-M7.**

To determine whether you have applied SAS Security Update 2022-03-M6, review the contents of this file:
```
SASHome\InstallMisc\utilities\installqual\9.4\security_hotfix.properties
```
If this file does not exist, or it does not list the version as 5.2, then you do not have the latest version of the update. Continue with these steps to apply SAS Security Update 2022-03-M6.

If the correct version is listed and you have applied a hot fix, then you might be directed to reapply the update. If so, please re-apply it to ensure continued system security.

Apply SAS Security Update 2022-03-M6

Use the following steps to apply the update. These steps should be performed for every machine in your deployment by applying the update on each installed and configured machine.

1. Before beginning, ensure that all active SAS sessions, daemons, spawners, servers, and agents are terminated. In addition, SAS strongly recommends that you back up your system before applying the update.

2. Download [SAS Security Update 2022-03-M6](#).

3. Unzip `sas-security-update-2022-03-M6.zip` into a directory of your choice. On UNIX, using the `unzip` command is the best option. If you use WinZip or the `jar xvf` command, you must also use the following command to preserve the appropriate permissions:

   ```
   chmod a+x install.sh
   ```

   If the installer ID differs from the update directory owner, make the directory writable by all IDs in the same group with the following command:

   ```
   chmod -R g+w /security directory/sas-security-update-2022-03-M6
   ```

4. From the directory into which you unzipped, go to the `sas-security-update-2022-03- M6` directory.

5. In that directory, run the appropriate script using the same user ID that was used to install (installer ID). The script requires one argument— the full path to the SASHOME directory where the update is going to be applied.

   Windows
   ```
   install.bat "SASHOME"
   ```

   Windows Example `install.bat "C:\Program`
   ```
   Files\SASHome"
   ```

   *Note: Depending on your settings, you might have to use the **Run as administrator** option.*

   UNIX
   ```
   ./install.sh "SASHOME" UNIX
   ```
   Example
   ```
   ./install.sh "/usr/lpp/SAS"
   ```

6. The script applies the update to all files in the SASHOME and SAS Configuration directories that need to be updated. When the script finishes, a message states that the update is complete and the script exits.

7. If you plan to deploy other hot fixes or updates from the location where you placed this ZIP file, you need to remove it from this location. The SAS Deployment Manager, which is used for deploying other hot fixes, does not recognize this file and will issue an error.

8. Continue to the next step.

Step 5 — Apply SAS Security Update 2023-06-M7

Determine Whether SAS Security Update 2023-06-M7 Is Needed

If you are not using SAS 9.4M7, skip to **Step 6 — Apply SAS Security Update 2023-06-M8**.

To determine whether you have applied SAS Security Update 2023-06-M7, review the contents of this file:

```
SASHome\InstallMisc\utilities\installqual\9.4\security_hotfix.properties
```

If the file does not exist, or it does not list the version as 12.2, then you do not have the latest version of the update. Continue with these steps to apply SAS Security Update 2023-06-M7.

If the correct version is listed and you have applied a hot fix, you might be directed to re-apply the update. If so, please re-apply it to ensure continued system security.

Apply SAS Security Update 2023-06-M7

Use the following steps to apply the update. These steps should be performed for every machine in your deployment by applying the update on each installed and configured machine.

1. Before beginning, ensure that all active SAS sessions, daemons, spawners, servers, and agents are terminated. In addition, SAS strongly recommends that you back up your system before applying the update.

2. Download SAS Security Update 2023-06-M7.

3. Unzip `sas-security-update-2023-06-M7.zip` into a directory of your choice. On UNIX, using the `unzip` command is the best option. If you use WinZip or the `jar xvf` command, you must also use the following command to preserve the appropriate permissions:
   ```
   chmod a+x install.sh
   ```

   If the installer ID differs from the update directory owner, make the directory writable by all IDs in the same group with the following command:
   ```
   chmod -R g+w /security directory/sas-security-update-2023-06-M7
   ```

4. From the directory into which you unzipped, go to the `sas-security-update-2023-06-M7` directory.

5. In that directory, run the appropriate script using the same user ID that was used to install (installer ID). The script requires one argument— the full path to the SASHOME directory where the update is going to be applied.

   Windows
   ```
   install.bat "SASHOME"
   ```

   Windows Example `install.bat "C:\Program`
   ```
   Files\SASHome"
   ```

   Note: Depending on your settings, you might have to use the **Run as administrator** *option.*

   UNIX
   ```
   ./install.sh "SASHOME" UNIX
   ```
   Example
   ```
   ./install.sh "/usr/lpp/SAS"
   ```

6. The script applies the update to all files in the SASHOME and SAS Configuration directories that need to be updated. When the script finishes, a message states that the update is complete, and the script exits.

7. If you plan to deploy other hot fixes or updates from the location where you placed this ZIP file, you need to remove it from this location. The SAS Deployment Manager, which is used for deploying other hot fixes, does not recognize this file and will issue an error.

8. Continue to the next step.

Step 6 — Apply SAS Security Update 2023-06-M8

Determine Whether SAS Security Update 2023-06-M8 Is Needed

If you are not using SAS 9.4M8, skip to **Step 7 — Apply Hot Fix Y09009 – Supplemental Hot Fix for SAS Security Updates.**

To determine whether you have applied SAS Security Update 2023-06-M8, review the contents of this file:

    SASHome\InstallMisc\utilities\installqual\9.4\security_hotfix.properties

If the file does not exist, or it does not list the version as 13.0, then you do not have the latest version of the update. Continue with these steps to apply SAS Security Update 2023-06-M8.

If the correct version is listed and you have applied a hot fix, you might be directed to re-apply the update. If so, please re-apply it to ensure system security.

Apply SAS Security Update 2023-06-M8

Use the following steps to apply the update. These steps should be performed for every machine in your deployment by applying the update on each installed and configured machine.

1. Before beginning, ensure that all active SAS sessions, daemons, spawners, servers, and agents are terminated. In addition, SAS strongly recommends that you back up your system before applying the update.

2. Download SAS Security Update 2023-06-M8.

3. Unzip `sas-security-update-2023-06-M8.zip` into a directory of your choice. On UNIX, using the `unzip` command is the best option. If you use WinZip or the `jar xvf` command, you must also use the following command to preserve the appropriate permissions:

        chmod a+x install.sh

    If the installer ID differs from the update directory owner, make the directory writable by all IDs in the same group with the following command:

        chmod -R g+w /security directory/sas-security-update-2023-06-M8

4. From the directory into which you unzipped, go to the `sas-security-update-2023-06-M8` directory.

5. In that directory, run the appropriate script using the same user ID that was used to install (installer ID). The script requires one argument— the full path to the SASHOME directory where the update is going to be applied.

Windows
```
install.bat "SASHOME"
```

Windows Example `install.bat "C:\Program`
```
Files\SASHome"
```

*Note: Depending on your settings, you might have to use the **Run as administrator** option.*

UNIX
```
./install.sh "SASHOME"
```
UNIX Example
```
./install.sh "/usr/lpp/SAS"
```

6. The script applies the update to all files in the SASHOME and SAS Configuration directories that need to be updated. When the script finishes, a message states that the update is complete, and the script exits.

7. If you plan to deploy other hot fixes or updates from the location where you placed this ZIP file, you need to remove it from this location. The SAS Deployment Manager, which is used for deploying other hot fixes, does not recognize this file and will issue an error.

8. Continue to the next step.

Step 7 — Apply Hot Fix Y09009 – Supplemental Hot Fix for SAS Security Updates

Hot fix Y09009 is a container hot fix that includes hot fixes for several products. Your deployment might not include any product or all products affected by this hot fix container. If so, hot fixes are skipped and not applied to your deployment. These hot fixes are packaged together to make it simpler.

1. Review Y09009pt.pdf to see the list of SAS products that will be updated by Y09009. See SAS Note 35968 for information about how to determine whether you have any of the products installed on your SAS deployment. If you have one or more of the products, you must install Hot Fix Y09009. If you do not have any of the products, skip to **Step 8 — Rebuild** and Redeploy Web Applications.

2. Download Hot Fix Y09009.

3. Use the instructions in Y09009pt.pdf to apply Hot Fix Y09009 to every machine in your deployment. You might receive an informational message if hot fix Y09009 is applied but does not update any product on a machine.

4. Continue to the next step.

Step 8 — Rebuild and Redeploy Web Applications

Perform this step on all primary middle-tier machines.

After all updates and hot fixes have been applied, you must rebuild and redeploy every web application on each middle-tier machine to ensure that the updates and hot fixes take effect. The instructions for rebuilding and redeploying can be found in the following locations:

Rebuilding

See "Rebuild the SAS Web Applications" in SAS 9.4 Administration: Middle-Tier Administration Guide

Redeploying

See "Redeploy the SAS Web Applications" in SAS 9.4 Administration: Middle-Tier Administration Guide

When web applications are rebuilt, each web application's content is backed up in a backup directory. This backup is explained in the section **"Backups of Previous Web Application Versions"** in the SAS 9.4 Administration: Middle-Tier Administration Guide**.**

Note: JAR files with security vulnerabilities might be placed in the backup directory when rebuilding a web application. You should delete the backup directory once the web application has been successfully rebuilt, redeployed, and tested.

Step 9 — Apply the SAS Security Update to a Horizontal Middle-Tier Cluster Node

Perform this step on all horizontal cluster node middle-tier machines.

Product-specific hot fixes might require additional manual steps for configuration on horizontal middle-tier cluster nodes. If you have clustered any of the products horizontally, see "Steps to Perform on Each Horizontal Cluster Node" in "Maintain a Horizontal Cluster Member" in SAS 9.4 Administration: Middle-Tier Administration Guide.

Contacting SAS Technical Support

If you need assistance with the software or with the instructions in this guide, contact SAS Technical Support.