

# Updating Account Passwords in SAS® Fraud Management 6.1

## Contents

|                                                      |    |
|------------------------------------------------------|----|
| Overview .....                                       | 1  |
| Account Requirements .....                           | 1  |
| SAS® Management Console .....                        | 4  |
| SAS® Deployment Manager .....                        | 7  |
| SAS® Fraud Management Web Application Accounts ..... | 11 |
| Final Steps .....                                    | 13 |

## Overview

Service accounts are created for use by specific components of SAS® Fraud Management. This document details the steps for changing the passwords that were assigned to accounts in SAS Fraud Management version 6.1. These steps were fully verified running on SAS 9.4 M6. Any issues encountered in other SAS versions should be reported to the SAS Fraud Management Production Support team

The password for each account might need to be changed in several locations, including any specified databases, the server’s operating system, and SAS. The steps for changing a password in a database and the operating system depend on the installed environment, and steps for these changes are beyond the scope of this document. Steps for changing passwords in SAS® using SAS® Deployment Manager and SAS® Management Console are included in this document.

## Account Requirements

Table 1 contains an overview of the accounts and a list of their components. The actual account names in a particular SAS Fraud Management implementation might be different from those that are shown in the table.

**Table 1: User Accounts and Descriptions**

| User             | Short Description                                                                                                       | BATCH<br>HOST | RULES<br>HOST | ODE<br>HOST | MID-<br>TIER<br>HOST | TAS<br>HOST | MEH<br>HOST | SOR<br>HOST | TDR<br>HOST | METADATA<br>HOST |
|------------------|-------------------------------------------------------------------------------------------------------------------------|---------------|---------------|-------------|----------------------|-------------|-------------|-------------|-------------|------------------|
| <b>sascfg</b>    | The user account to install and configure SAS software. Also used for SAS® Metadata Repository backups.                 | ✓             | ✓             | ✓           | ✓                    | ✓           |             |             |             | ✓                |
| <b>sasomr</b>    | System of Record (SOR) database access credentials for the SAS Metadata Repository administrator process.               | ✓             |               |             |                      |             |             | ✓           |             | ✓                |
| <b>sassrv</b>    | The external account for the SAS® Object Spawner and for running the pooled workspace server and stored process server. | ✓             | ✓             |             |                      |             |             |             |             |                  |
| <b>sharedsvc</b> | Database credentials for the SAS® Web Infrastructure Platform database.                                                 |               |               |             | ✓                    |             |             |             |             |                  |
| <b>sassorspl</b> | Database credentials for SOR database special batch jobs.                                                               | ✓             |               |             |                      |             |             | ✓           |             |                  |
| <b>sassorbch</b> | Database credentials for SOR database batch jobs.                                                                       | ✓             |               |             |                      |             |             | ✓           |             |                  |
| <b>sassorapp</b> | SOR database access credentials for the SAS Fraud Management middle tier.                                               |               |               |             | ✓                    |             |             | ✓           |             |                  |
| <b>sastdrspl</b> | Database credentials for TDR database special                                                                           | ✓             |               |             |                      |             |             |             | ✓           |                  |

| User             | Short Description                                                                        | BATCH<br>HOST | RULES<br>HOST | ODE<br>HOST | MID-<br>TIER<br>HOST | TAS<br>HOST | MEH<br>HOST | SOR<br>HOST | TDR<br>HOST | METADATA<br>HOST |
|------------------|------------------------------------------------------------------------------------------|---------------|---------------|-------------|----------------------|-------------|-------------|-------------|-------------|------------------|
|                  | batch jobs.                                                                              |               |               |             |                      |             |             |             |             |                  |
| <b>sastdrgrp</b> | Database credentials for TDR database batch jobs.                                        | ✓             |               |             |                      |             |             |             | ✓           |                  |
| <b>sastdrapp</b> | TDR database access credentials for the SAS Fraud Management middle tier.                |               |               |             | ✓                    |             |             |             | ✓           |                  |
| <b>sasmehspl</b> | Database credentials for MEH database special batch jobs.                                | ✓             |               | ✓           |                      |             | ✓           |             |             |                  |
| <b>sasmehbch</b> | Database credentials for MEH database batch jobs.                                        | ✓             |               | ✓           |                      |             | ✓           |             |             |                  |
| <b>sasmehose</b> | User credentials for the OnDemand Scoring Engine.                                        |               |               | ✓           |                      |             | ✓           |             |             |                  |
| <b>sasosesor</b> | SOR database credentials for the OnDemand Decision Engine.                               |               |               | ✓           |                      |             |             | ✓           |             |                  |
| <b>sasosetdr</b> | TDR database credentials for the OnDemand Decision Engine.                               |               |               | ✓           |                      |             |             |             | ✓           |                  |
| <b>sastastdr</b> | SAS Fraud Management transaction analysis engine: sampling process database credentials. |               |               |             |                      | ✓           |             |             | ✓           |                  |
| <b>sastassor</b> | SAS Fraud transaction analysis engine system of record database credentials.             |               |               |             |                      | ✓           |             | ✓           |             |                  |

## SAS® Management Console

Use the following steps to change the SAS Fraud Management account passwords in the SAS Management Console. These changes should be completed before changing the database and server operating system passwords and need to be completed only once per environment.

1. Log on to the SAS Metadata Server as the SAS configuration user (**sascfg**, from Table 1).
2. Navigate to the SAS Management Console directory in the *SASHOME* directory, as shown below:

***SASHOME/SASManagementConsole/9.4***

3. If necessary, assign and export the DISPLAY environment variable for X windows:

**Example:** `export DISPLAY=working-PC-IP-address:0.0`

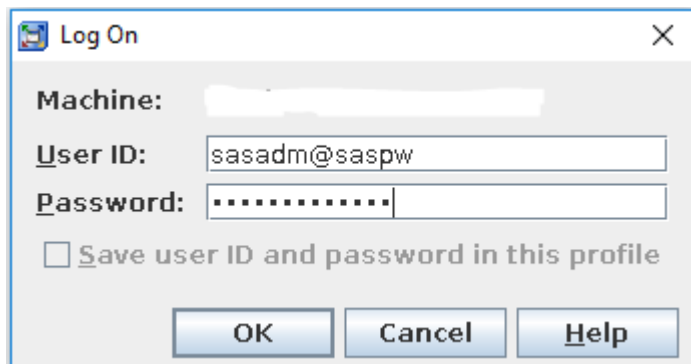
4. Execute the following command from the current directory to start the SAS Management Console:

```
./sasmc
```

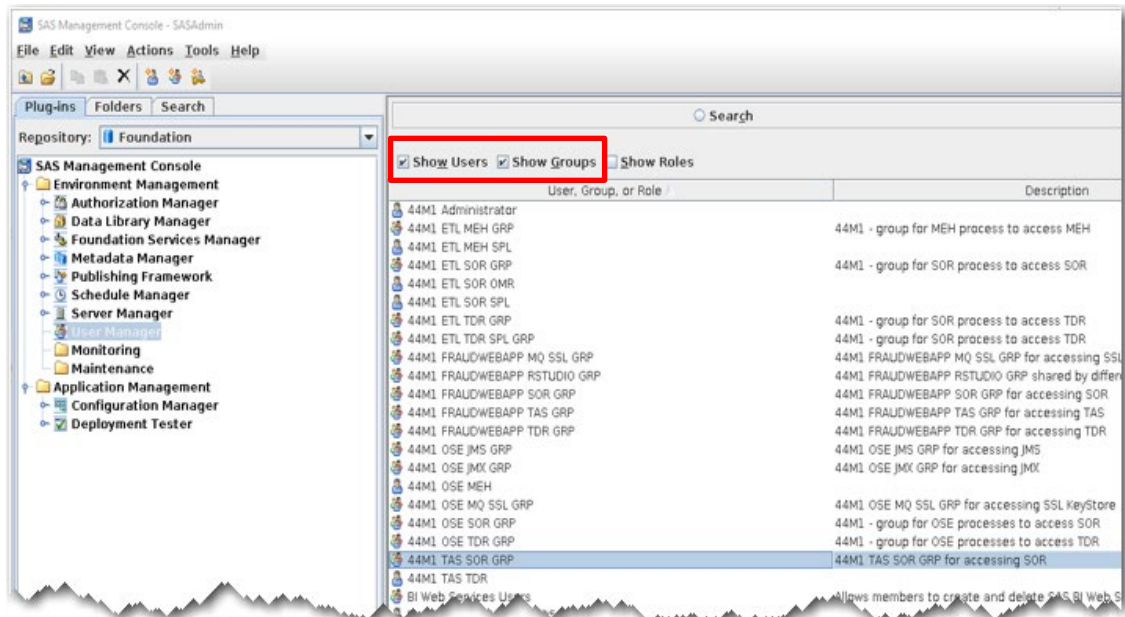
5. Select the correct connection profile to connect to the Metadata server or create a new profile with the appropriate details.



6. Enter the user credentials of the SAS Admin user (**sasadm@saspw** by default).



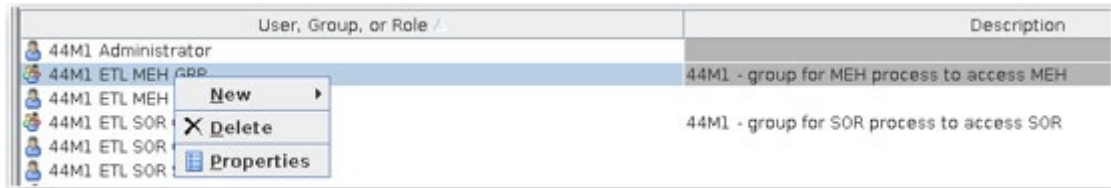
7. Navigate to User Manager in the left pane and make sure that the **Show Users** and **Show Groups** check boxes are selected, as shown below:



The listing contains a set of users with names like *implementation-name* ETL, *implementation-name* FRAUDWEBAPP, *implementation-name* OSE, and *implementation-name* TAS. In this example, *implementation-name* is replaced with 44M1, but this is different in other environments.

- *implementation-name* ETL MEH GRP
- *implementation-name* ETL MEH SPL
- *implementation-name* ETL SOR GRP
- *implementation-name* ETL SOR OMR
- *implementation-name* ETL SOR SPL
- *implementation-name* ETL TDR GRP
- *implementation-name* ETL TDR SPL GRP
- *implementation-name* FRAUDWEBAPP SOR GRP
- *implementation-name* FRAUDWEBAPP TDR GRP
- *implementation-name* OSE MEH
- *implementation-name* OSE SOR GRP
- *implementation-name* OSE TDR GRP
- *implementation-name* TAS SOR GRP
- *implementation-name* TAS TDR

8. Right-click the first name in the list and select **Properties**.

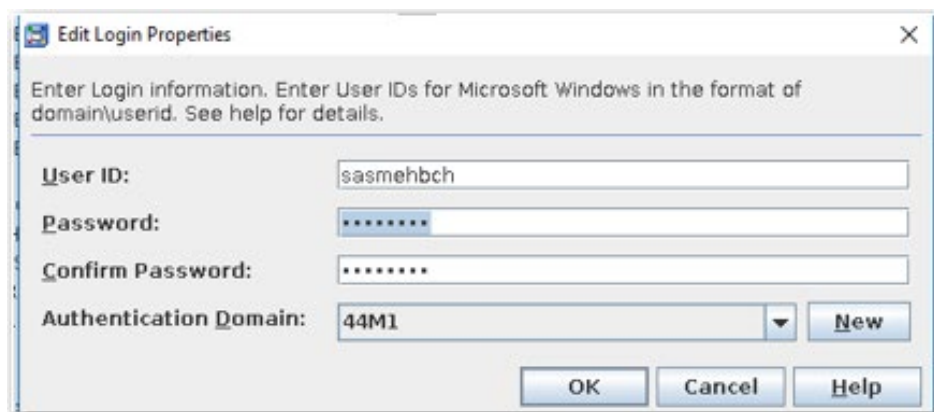


9. Navigate to the **Accounts** tab in the new window that is displayed. Then, select the user ID and click the **Edit** button.



This action opens the Edit Login Properties window.

10. Enter the new password value in the **Password** and **Confirm Password** fields in the Edit Login Properties window. Then click **OK**.



11. Click **OK** in the *Name* Properties window (from step 9) to return to the User Manager.
12. Repeat steps 8-11 for the remaining users in the list.
13. Exit out of SAS Management Console.

## SAS® Deployment Manager

Use SAS Deployment Manager to update the password of the **sharedsvc** user. Execute the following steps on each middle-tier server in the environment.

**Note:** Substitute the full path to the SASHOME directory for **SASHOME** and the full path to the SAS configuration directory for **SAS-configuration-directory** in the commands.

1. Log on to the SAS middle-tier server as the SAS configuration user (**sascfg**, from [Table 1](#)).
2. Execute the following command to stop the web application servers that run on this server:

```
SAS-configuration-directory/Levl/sas.servers.mid stop
```

3. Navigate to the SAS Deployment Manager directory in the **SASHOME** directory as shown below:

**SASHOME/SASDeploymentManager/9.4**

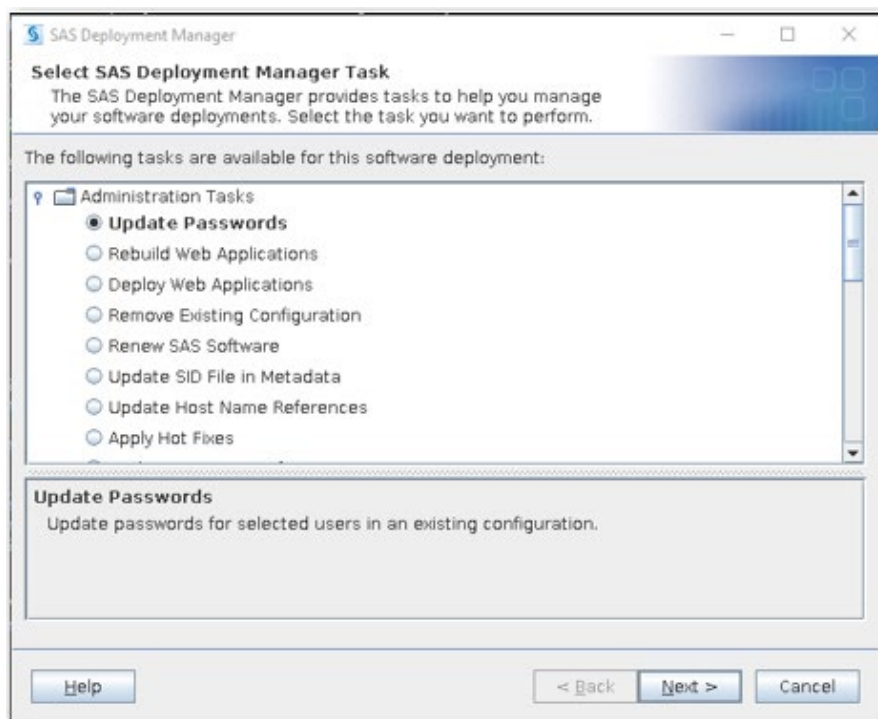
4. If necessary, assign and export the DISPLAY environment variable for X windows:

**Example:** `export DISPLAY=working-PC-IP-address:0.0`

5. Launch SAS Deployment Manager by executing the following command:

```
./sasdm.sh
```

6. On the **Select SAS Deployment Manager Task** page select **Update Passwords** and click **Next**.



7. Select the configuration directory of the middle tier (if there are multiple selections). Then click **Next**.

The screenshot shows the 'Select Configuration Directory/Level' dialog box in the SAS Deployment Manager. The title bar reads 'SAS Deployment Manager'. The main heading is 'Select Configuration Directory/Level' with a subtitle 'Select the configuration directory and the level within the configuration directory to manage.' There are two radio buttons: 'Select Configuration Directory' (selected) and 'Enter Configuration Directory and Level'. Under the selected radio button, there is a table with two columns: 'Configuration Directory' and 'Configuration Level'. The table lists several directories, all with 'Lev1' as the configuration level. The last entry, '/sso/config/SASFraudMidtier', is highlighted. Below the table, the 'Enter Configuration Directory and Level' section has a text box for 'Configuration Directory' with a 'Browse...' button, and a dropdown for 'Configuration Level' set to 'Lev1'. At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

| Configuration Directory     | Configuration Level |
|-----------------------------|---------------------|
| /sso/config/SASFraudOMR     | Lev1                |
| /sso/config/SASFraudWIP     | Lev1                |
| /sso/config/SASFraudBatch   | Lev1                |
| /sso/config/SASFraudRules   | Lev1                |
| /sso/config/SASFraudODE     | Lev1                |
| /sso/config/SASFraudTas     | Lev1                |
| /sso/config/SASFraudMidtier | Lev1                |

8. Enter the SAS administrator user credentials. Then click **Next**.

The screenshot shows the 'Specify Connection Information' dialog box in the SAS Deployment Manager. The title bar reads 'SAS Deployment Manager'. The main heading is 'Specify Connection Information' with a subtitle 'Specify connection information to the SAS Metadata Server.' There are five text boxes: 'Host Name:', 'Port:' (with '8561' entered), 'User ID:' (with 'sasadm@saspw' entered), and 'Password:' (with masked characters '\*\*\*\*\*'). At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

9. Enter the current credentials for the SAS Shared Services database user (**sharedsvc**, from Table 1). Then click **Next**.

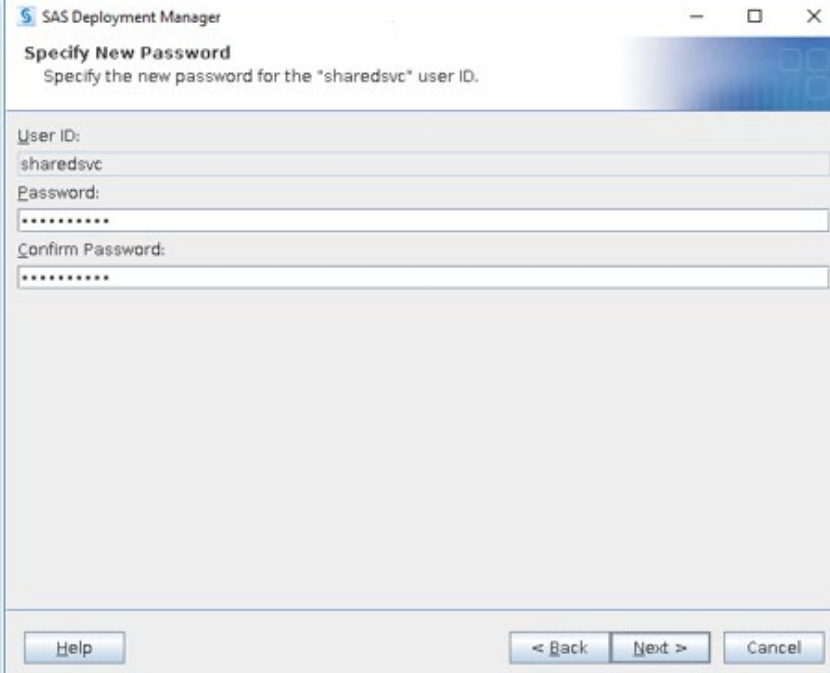
The screenshot shows the 'SAS Deployment Manager' window with the title 'SAS Web Infrastructure Database JDBC Properties'. The subtitle reads 'Specify the connection information for the SAS Web Infrastructure Database JDBC connection.' The form contains three input fields: 'Host Name' with the value 'dbc', 'User ID' with the value 'sharedsvc', and 'Password' with a masked value '\*\*\*\*\*'. At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

10. Select the **sharedsvc** user ID from the list. Then click **Next**.

The screenshot shows the 'SAS Deployment Manager' window with the title 'Select User IDs'. The subtitle reads 'Select the user IDs for which the passwords should be updated.' Below the subtitle is a table with two columns: 'User ID' and 'Authentication Domain'. The table lists several user IDs, with 'sharedsvc' selected (indicated by a checkmark in the checkbox column). At the bottom of the table are two buttons: 'Select All' and 'Clear All'. Below the table, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button.

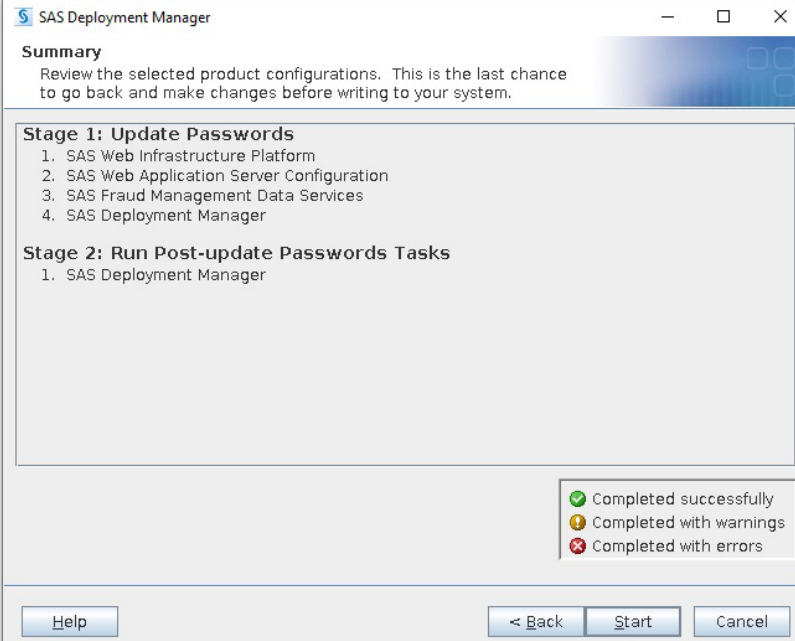
| User ID                                       | Authentication Domain |
|-----------------------------------------------|-----------------------|
| <input type="checkbox"/> sastrust@saspw       | Not Applicable        |
| <input type="checkbox"/> sasadm@saspw         | Not Applicable        |
| <input checked="" type="checkbox"/> sharedsvc | Not Applicable        |
| <input type="checkbox"/> sassorapp            | Not Applicable        |
| <input type="checkbox"/> sastdrapp            | Not Applicable        |
| <input type="checkbox"/> midssl_44M1          | Not Applicable        |
| <input type="checkbox"/> midexplr_44M1        | Not Applicable        |
| <input type="checkbox"/> tasdds_44M1          | Not Applicable        |

11. Enter the new password value into the **Password** and **Confirm Password** fields. Then click **Next**.



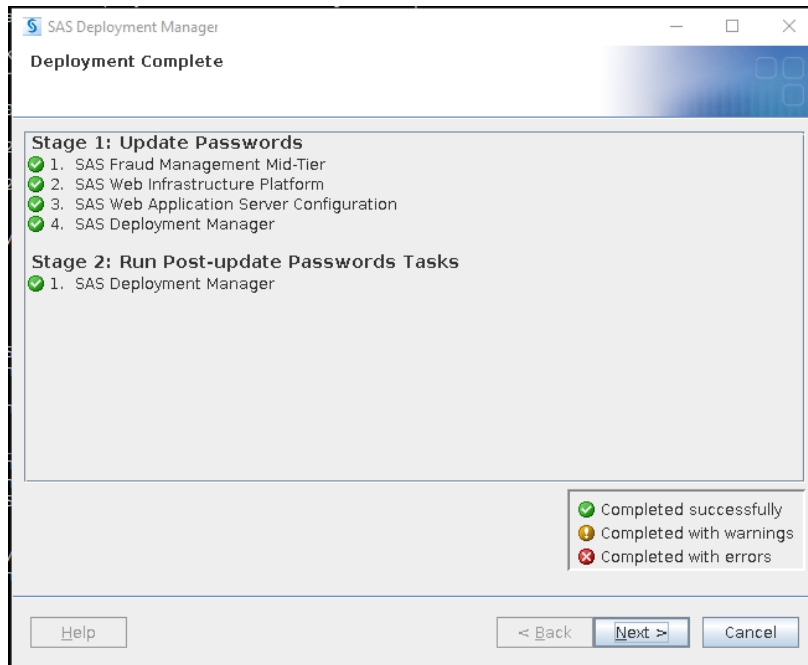
The image shows a Windows-style dialog box titled "SAS Deployment Manager" with a subtitle "Specify New Password". Below the subtitle is the instruction "Specify the new password for the 'sharedsvc' user ID." The dialog contains three input fields: "User ID:" with the text "sharedsvc", "Password:" with masked characters "\*\*\*\*\*", and "Confirm Password:" with masked characters "\*\*\*\*\*". At the bottom, there are four buttons: "Help", "< Back", "Next >", and "Cancel".

12. Click the **Start** button to start the password change process.



The image shows a Windows-style dialog box titled "SAS Deployment Manager" with a subtitle "Summary". Below the subtitle is the instruction "Review the selected product configurations. This is the last chance to go back and make changes before writing to your system." The dialog contains two sections: "Stage 1: Update Passwords" with a list of four items (SAS Web Infrastructure Platform, SAS Web Application Server Configuration, SAS Fraud Management Data Services, SAS Deployment Manager) and "Stage 2: Run Post-update Passwords Tasks" with a list of one item (SAS Deployment Manager). At the bottom right, there is a legend with three items: a green checkmark for "Completed successfully", a yellow warning icon for "Completed with warnings", and a red X icon for "Completed with errors". At the bottom, there are four buttons: "Help", "< Back", "Start", and "Cancel".

13. The process should complete with all green check marks each stage, as shown below.



14. Click **Next** to advance the page. Then, click **Finish** to close SAS Deployment Manager.

## SAS® Fraud Management Web Application Accounts

The encrypted passwords for the SAS Fraud Management web application accounts (**sassorapp** and **sastdrapp**) are generated from the operating-system command line and are updated manually in the `catalina.properties` file. Execute the following steps on each middle-tier server in the environment.

**Note:** In the commands below, substitute the full path to the SASHOME directory for **SASHOME** and the full path to the SAS configuration directory for **SAS-configuration-directory** in the commands.

1. Log on to the SAS middle-tier server as the SAS configuration user (**sascfg**, from [Table 1](#)).
2. If the web application servers are not shut down, execute the following command to stop the web application servers that run on this server:

```
SAS-configuration-directory/Lev1/sas.servers.mid stop
```

3. Navigate to the SAS Fraud Management web application's configuration directory, as shown below:

```
SAS-configuration-directory/Lev1/Web/WebAppServer/SASServer8_1/conf
```

**Note:** Some SAS Fraud Management environments do not use **SASServer8\_1** for the web application directory. If this directory does not exist, use **SASServer1\_1** instead.

4. View the `catalina.properties` file and review the lines for the user accounts **pw.sastdrds** and **pw.sascfds**. The lines look similar to those listed below:

```
pw.sastdrds.4.444M1=tcEnc://97SuFmBubCAX72u5AE2us4OQvhXYi7x4EKWyJ7D77s8=
```

```
pw.sascfds.4.444M1=tcEnc://cseKGjLgWeWH+ootES+H5+QYKcj4TAFQulhy4m6jw4U=
```

The line starting with **pw.sastdrds** is the **sastdrapp** account and the line starting with **pw.sascfds** is the **sassorapp** account.

5. The type of encoding used to encrypt the password for each account is shown between the equal sign and the colon. The steps used to generate a new encrypted password will differ based on the type of encoding used.

### tcEnc Encoding

Execute the following command once for each account. The command generates the encoded password as its output:

```
SASHOME/SASWebApplicationServer/9.4/tcruntime-admin.sh encode plain-text-password '!St@tS!'
```

### pbkdf2 Encoding

Navigate to the SAS Web Application Server directory in SASHOME, as shown below:

***SASHOME/SASWebApplicationServer/9.4***

Execute the following command once for each account. The command generates the encoded password as its output:

```
SASHOME/SASPrivateJavaRuntimeEnvironment/9.4/jre/bin/java -cp  
":lib/*"  
-  
Dcom.springsource.tcserver.security.PropertyDecoder.decoder_prefix=pb  
kdf2:// com.springsource.tcserver.security.PropertyDecoder -encode  
'!St@tS!' plain-text-password
```

### sasmtr01 Encoding

Navigate to the SAS Fraud Management web application directory, as shown below:

***SAS-configuration-directory/Lev1/Web/WebAppServer/SASServer8\_1***

Execute the following command to set environment variables:

```
export `grep ^CATALINA_HOME bin/setenv.sh`  
  
export `grep ^JAVA_HOME bin/setenv.sh`
```

Execute the following command once for each account. The command generates the encoded password as its output:

```
bin/decoder.sh -e -c sasmt01 -pwf conf/secure.file -v plain-text-  
password
```

Execute the following command to unset the environment variables:

```
unset CATALINA_HOME JAVA_HOME
```

6. Edit the `catalina.properties` file and replace the current encoded passwords with the newly generated encoded passwords. For **tcEnc** and **pbkdf2** encoding, replace the string after the double forward slashes (`//`). For **sasmt01** encoding, replace the string after the colon.

## Final Steps

Completing the previous steps changes the application's passwords so that they are detected upon start-up. As mentioned earlier, the passwords must be changed for each of the accounts for the host operating systems and corresponding databases that are listed in [Table 1](#).

After the passwords for each host and database are changed, you can start (or restart) the applications to load the latest credentials and create new database connections.