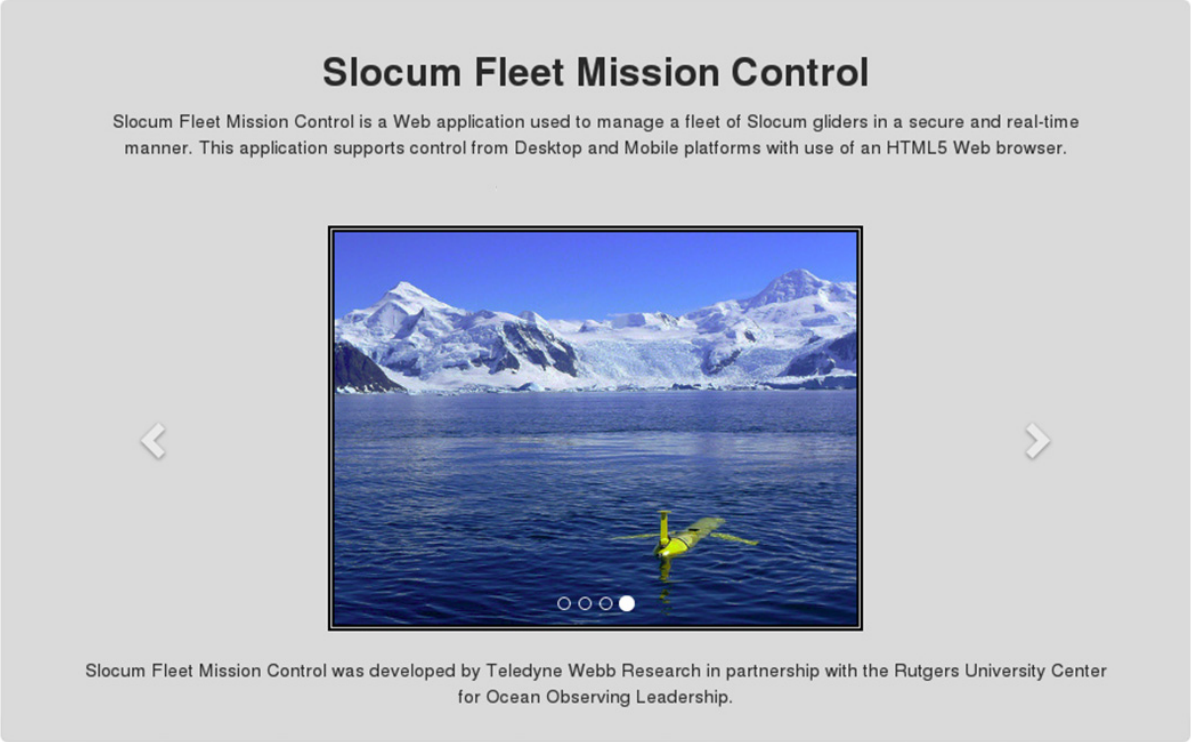
Slocum Fleet Mission Control

Software Installation & Setup Guide

P/N M313589-NFC, Rev. B
Software Version 8.7.0-1



TELEDYNE MARINE
WEBB RESEARCH
Everywhereyoulook™

Teledyne Webb Research
49 Edgerton Drive
North Falmouth, MA 02556
U.S.A.
Tel: (508) 563-1000
Fax: (508) 563-6444

www.teledynemarine.com/webb-research

NOTICES

Proprietary Information

The information contained herein is the property of Teledyne Webb Research and is considered proprietary. This information may not be used for any other purpose, copied, transferred, or disclosed to third parties, reverse engineered, modified, or improved without written consent from Teledyne Webb Research.

Terms and Conditions

Teledyne Webb Research's General Terms and Conditions of Sale are hereby incorporated by reference and are located at www.teledynemarine.com/webb-research under *Terms & Conditions*.

Changes

Teledyne Webb Research reserves the right to make changes to the design or specifications at any time without incurring any obligation to modify previously installed units. In addition, while considerable effort has been made to ensure that the information in this manual is accurate and complete, Teledyne Webb Research assumes no liability for any errors or omissions.

Refer to the applicable parts of this user manual before installing, setting up, connecting to, and using the SFMC web application.

CONTENTS

LIST OF TABLES

Preface

Teledyne Webb Research Slocum Fleet Mission Control (SFMC) is a collection of software services that enables tracking of Teledyne Webb Research Slocum gliders, displaying their reported data, and creating mission plans for them using a standard HTML5-supported Web browser.

Conventions Used in This Publication

Safety Symbols

Where applicable, safety information is presented as follows:

Note

Identifies information of particular interest that the reader must be aware of, a referral to another part of this manual, or a referral to another manual.

CAUTION

Identifies a potential hazard that could result in damage to equipment or loss of data.

WARNING

Identifies a potential hazard that could result in injury or death to the operator or to other personnel.

Other symbols include:

A referral to: another part of this manual, an external reference, or general information applicable to Slocum Fleet Mission Control.

Menu Options and Paths

Menu options are in bold type. Rather than writing out "From the **Admin** menu, select **User Administration**, then select **Users**," angle brackets are used to show the next menu level down:

Select **Admin > User Administration > Users**.

File Types and Extensions

File names are written as `file.typ`, where **`file`** is the descriptor and **`typ`** is the extension.

- When the text mentions a specific file name, it is written as `sfmc.xml` or something similar.
- When the text mentions file types in general, it is written using the extension in all caps without the period before it; for example, `INI` files or `XML` files.

Typographical Conventions

Font	Description
Bold	The name of a folder, node, path, menu option, or icon.
Italic	The name of a window, page, tab, dialog box, panel, area, field, button, or drop-down list within the software interface.
[blue square brackets]	The label of a physical key on the computer's keyboard or device's keypad.
`Monospace`	A system value or text displayed by the screen or computer.
`Monospace Bold`	A user value or text the user enters.

Customer Service

We welcome your comments and suggestions for improving our products and documentation as well as developing better ways of serving you. Should you require service or support for SFMC, contact Teledyne Webb Research customer service using any of the following means:

TELEDYNE WEBB RESEARCH
Attention: Customer Service
49 Edgerton Drive
North Falmouth, MA 02556
U.S.A.
Telephone: (508) 548-2077
Fax: (508) 540-1686

E-mail: webbresearch@teledyne.com
Email support: glidersupport@teledyne.com

www.teledynemarine.com/webb-research/support

RMA Request Form

To request an RMA for repair of any Webb Research products:

1. Please follow the link below.

   RMA Request Form Link

2. Complete all information in the form and select SUBMIT.
3. You will receive an automated confirmation that your form has been received.
4. We will respond within 24–48 hours to provide your RMA number and shipping instructions.

   Please do not ship any goods until you have received the RMA number.
5. Please mark the shipment clearly with the provided RMA number.

1 Introduction

New

If installing the software for the first time, please follow steps in Chapter 2, "New SFMC Installation."

Upgrade

If upgrading an existing installation, please follow steps in Chapter 3, "Upgrade SFMC Installation."

Noteworthy Changes in Latest Release

The following are noteworthy for this latest release:

- SFMC Postgresql Upgrade from 10 to 13
- Support for NavyLinux 8
- Support for Ubuntu 22
- Support for Benthos acoustic modem post processing
- Support for newer science sensors
- Altered local firewall settings for fresh install to only open ports 80, 443, and 6565
- Password expiration changed from 180 days to 365
- The default admin user **`sfmcadmin`** initial login will require password change
- Administrative changes result in emails with change info being sent to all SFMC administrators
- Fix for archived deployments sometimes having NULL archive file name
- Fix to ensure **`localuser`** Desktop icons are updated during an SFMC upgrade
- Additional `sfmc-webserver` logs added to `logrotate` to save space
- REST API – support for directory listing options
- Improvement on the glider identification regex
- Improved handling on duplicate key violation errors associated with sensor data processing
- Tweak on glider terminal background color when glider port disconnected

2 New SFMC Installation

Host System Installation Requirements

This section specifies the installation platform requirements to install and run the SFMC software.

The recommended resources for SFMC are:

- One or more CPUs that allow for 8 cores operating at 2.7GHz
- 16 GB RAM
- 500 GB hard disk

The allowed resources for SFMC are:

- One or more CPUs that allow for 4 cores operating at 2.7GHz
- 8 GB RAM
- 300 GB hard disk

Installation Dependencies

- The SFMC software requires usage of one of the following operating system distributions:
  - CentOS 7
  - RockyLinux 8
  - NavyLinux 8
  - Red Hat Enterprise Linux (RHEL) 8
  - Ubuntu 18.04
  - Ubuntu 20.04
  - Ubuntu 22.04
- To ensure maximum disk space in the **/var** folder, following the recommendations for disk partition sizing in Table 2.1:

Note

Partitioning guidance is not applicable to Ubuntu. It is only applicable for CentOS, RockyLinux, NavyLinux, and RHEL.

Table 2.1: Recommended Partition Sizes

Partition Name	Partition Capacity
/boot	1 GB
swap	5 GB
/home	20 GB
/tmp	10 GB
/opt	50 GB
/	20 GB
/var	Remaining

- An SSL Web certificate is required to complete the install.

  You can use a self-signed certificate if you wish. However, if connected to the Internet, the recommendation is to use an SSL Web certificate provided by a well-known and trusted Certificate Authority.

Note

Both the SSL certificate and private key files are required to complete the installation.

- SFMC Installation files, where <*version*> represents the SFMC version:
  - CentOS 7, RHEL 8, RockyLinux 8, or NavyLinux 8:

    rpm-install-sfmc-<*version*>.bsx

  - Ubuntu 18.04/20.04/22.04:

    deb-install-sfmc-<*version*>.bsx

SFMC Software Installation

Perform the following steps:

1. Log in as the root user or a user with "sudo all" permissions.
2. In a terminal window, ensure the Linux system time is set to UTC:

   timedatectl set-timezone UTC
3. Install SSL Web server certificate and private key files to:
   - **/etc/pki/tls/certs/localhost.crt**
   - **/etc/pki/tls/private/localhost.key**

4. In a terminal window, change directory to the location of one of the appropriate files:
   - CentOS 7, RHEL 8, RockyLinux 8, or NavyLinux 8:

     rpm-install-sfmc-<*version*>.bsx

   - Ubuntu 18.04/20.04/22.04:

     deb-install-sfmc-<*version*>.bsx

5. In the terminal window, enter the appropriate command depending on the operating system platform:
   - CentOS 7, RHEL 8, RockyLinux 8, or NavyLinux 8:

     sudo sh ./rpm-install-sfmc-*

   - Ubuntu 18.04/20.04/22.04:

     sudo bash ./deb-install-sfmc-*

   The system displays:

   ```
   Will this installation utilize a static IP? Answer y or n >
   ```

6. Enter one of the following answers:
   - **y** — for a Dock Server system that utilizes a static IP
   - **n** — for a mobile Dock Server system that connects to various Wireless Access Points

   The system displays:

   ```
   Please press any key to review the license agreement >
   ```

7. Press the **[Enter]** key and review the license agreement.
8. After reviewing the license agreement, press the **[q]** key to quit out of the license agreement view.

   The system displays:

   ```
   Please enter y if you accept the terms of the license agreement >
   ```

9. Press the **[Enter]** key to accept the license agreement terms and begin the installation process.
10. Update the system firewall settings to allow external access to the specified ports, then press **[Enter]**.

    The system displays:

    ```
    The system requires a reboot. Please press any key to initiate the reboot >
    ```

11. Press the **[Enter]** key.

    The system restarts.

12. Log in to the system using:
    - Account — **localuser**
    - Default password — **WideOpen**
13. Use the **/opt/sfmc-dockserver/localuser/bin/port-dockserver** program to configure the Dock Server to include your desired ports.

3 Upgrade SFMC Installation

Upgrade Dependencies

CAUTION

Ensure there are no gliders expected to call into the SFMC being upgraded.

- The individual completing the upgrade has the ability to use the root account or has access to an account with sudo all permissions.
- The SFMC upgrade expects that an existing version of the SFMC software was already installed.
- The administrator completing the upgrade has access to the appropriate file, where <*version*> represents the SFMC version for the new version being installed:
  - CentOS 7, RHEL 8, RockyLinux 8, or NavyLinux 8:

    rpm-upgrade-sfmc-<*version*>.bsx
  - Ubuntu 18.04/20.04/22.04:

    deb-upgrade-sfmc-<*version*>.bsx
- The upgrade will take about 15 minutes to complete.

CentOS/RHEL Upgrade Steps

1. Log in to the SFMC machine as the root user or a user account with "sudo all" permissions.
2. Attach the media holding the **rpm-upgrade-sfmc-<*version*>.bsx** file.
3. In a terminal window, change directory to the location of the `rpm-upgrade-sfmc-<version>.bsx` file; for example, `cd /var/run/media/root/KINGSTON`.
4. In the terminal window, run the following command, replacing <*version*> with the actual version details (for example, `8.5.0-1`):

   sh ./rpm-upgrade-sfmc-<*version*>.bsx
5. Wait for the upgrade to complete.
6. Log out of the root user session.

Ubuntu Upgrade Steps

1. Log in to the SFMC machine as the user account with "sudo all" permissions.
2. Attach the media holding the **deb-upgrade-sfmc-<*version*>.bsx** file.

3. In a terminal window, change directory to the location of the `deb-upgrade-sfmc-<version>.bsx` file; for example, `cd /var/run/media/root/KINGSTON`.
4. In the terminal window, run the following command, replacing `<version>` with the actual version details (for example, `8.5.0-1`):

   `sudo bash ./deb-upgrade-sfmc-<version>.bsx`
5. Wait for the upgrade to complete.
6. Log out of the user session.

A Abbreviations and Acronyms

This appendix includes the abbreviations and acronyms pertaining to Slocum gliders.

Abbreviation or Acronym	Description
AC or ac	Alternating Current
ASSY	Assembly
BAM	Beam Attenuation Meter
CTD	Conductivity/Temperature/Depth
COTS	Commercial Off-the-Shelf
DC or dc	Direct Current
DDM	Degrees Decimal Minutes Latitude/Longitude format displayed as: -70° 34.50' W (entered as **-7034.50**)
DG	Dangerous Goods
DMS	Degrees Minutes Seconds Latitude/Longitude format displayed as: -70° 34' 29.9776" W
GLMPC	Glider Mission Planning and Control
GMC	Glider Mission Control
GPS	Global Positioning System
IR	Infrared
ISO	International Organization for Standardization
ISU	Iridium Subscriber Unit
LNA	Low Noise Amplifier
MS Plug	Military Standard Plug
MSDS	Material Safety Data Sheet
OC	Operations Center
OEM	Original Equipment Manufacturer
QCP	Quality Control Process
PPE	Personal Protective Equipment
RHEL	Red Hat Enterprise Linux
RHN	Red Hat Network
RUDICS	Router-based Unrestricted Digital Internetworking Connectivity System
SE	Systems Engineering
SHCS	Socket Head Cap Screw
SN	Serial Number
SOP	Standard Operating Procedure

Abbreviation or Acronym	Description
SSL	Secure Sockets Layer A security protocol that creates an encrypted link between a web server and a web browser.
STE	Secure Telephone Equipment
TWR	Teledyne Webb Research
U.S.	United States
USB	Universal Serial Bus
UUV	Unmanned Undersea Vehicle
VAC	Volts Alternating Current

B SFMC Dock Server Folders

The /var/opt/gmc/ Folder

The **/var/opt/gmc** folder represents the **/var/opt/sfmc-dockserver/stations/default** folder.

The **/var/opt/sfmc-dockserver/stations** folder includes all of the group-specific <*groupName*> folders, including the **default** group folder:

- /var/opt/sfmc-dockserver/stations/default
- /var/opt/sfmc-dockserver/stations/group1, group2, and so on

In each group folder are the following:

- <*groupName*>.xml — An XML file that must ***not*** be modified.
- **scripts** — A folder that can contain Dock Server scripts for the group.
- **maps** — A folder that can contain maps for the group.
- **gliders** — A folder that contains a list of folders for each glider registered in the group.
- **backups** — A folder that contains archives of specific glider folders that have been backed up by users.

The /var/opt/sfmc-dockserver/stations/<*groupName*>/gliders Folder

The folder **/var/opt/sfmc-dockserver/stations/<*groupName*>/gliders** contains one or more glider folders, each named **<*gliderName*>** and each representing the glider as in the following examples:

- /var/opt/sfmc-dockserver/stations/default/gliders/hostglider1
- /var/opt/sfmc-dockserver/stations/group1/gliders/hostglider4
- /var/opt/sfmc-dockserver/stations/group2/gliders/hostglider5

In each glider folder are the following:

- **archive** — A folder that stores archived files associated with **dockzr** command executions for the glider.
- **configuration** — A folder that contains mission planner files to be transferred to the glider.
- **from-glider** — A folder that contains files transferred from the glider.

- **logs** — A folder that contains Dock Server created log files capturing glider dialog for each communication session with the glider.
- **to-glider** — A folder that contains flight files to be sent to the glider.
- **to-science** — A folder that contains science files to be sent to the glider.

C Creating a Self-Signed SSL Certificate

This appendix is only applicable for users who plan to use a self-signed Web server certificate instead of a valid Certificate Authority-signed Web server certificate.

Secure Sockets Layer (SSL) is a security protocol that creates an encrypted link between a web server and a web browser.

An SSL Certificate is a digital certificate that authenticates your website's identity and enables an encrypted connection.

Perform the following steps:

1. Generate the **server.key** file. Type the following in a command line:

   openssl genrsa -des3 -out server.key 4096

   The system displays:

   ```
   Enter pass phrase for server.key:
   ```

2. Enter the pass phrase.

   The system displays:

   ```
   Verifying – Enter pass phrase for server.key:
   ```

3. Re-enter the pass phrase.
4. Generate the Certificate Request. Type the following in a command line:

   openssl req -new -key server.key -out server.csr

   The system displays:

   ```
   Enter pass phrase for server.key:
   ```

5. Enter the **server.key** file pass phrase.

   The system requests certificate request parameters.

6. Enter the following required parameters:
   - Country Name
   - State or Province Name
   - Locality Name (for example, city)
   - Organization Name
7. For all other parameters, press the **[Enter]** key.
8. Copy the **server.key** file to `server.key.org`. Type the following in a command line:

   cp server.key server.key.org

9. Re-create the **server.key** file so that a pass phrase is not required. Type the following in a command line:

   openssl rsa -in server.key.org -out server.key

   The system displays:

   ```
   Enter pass phrase for server.key:
   ```

10. Enter the **server.key** file pass phrase.
11. Generate the Web server certificate. Type the following in a command line:

    openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt