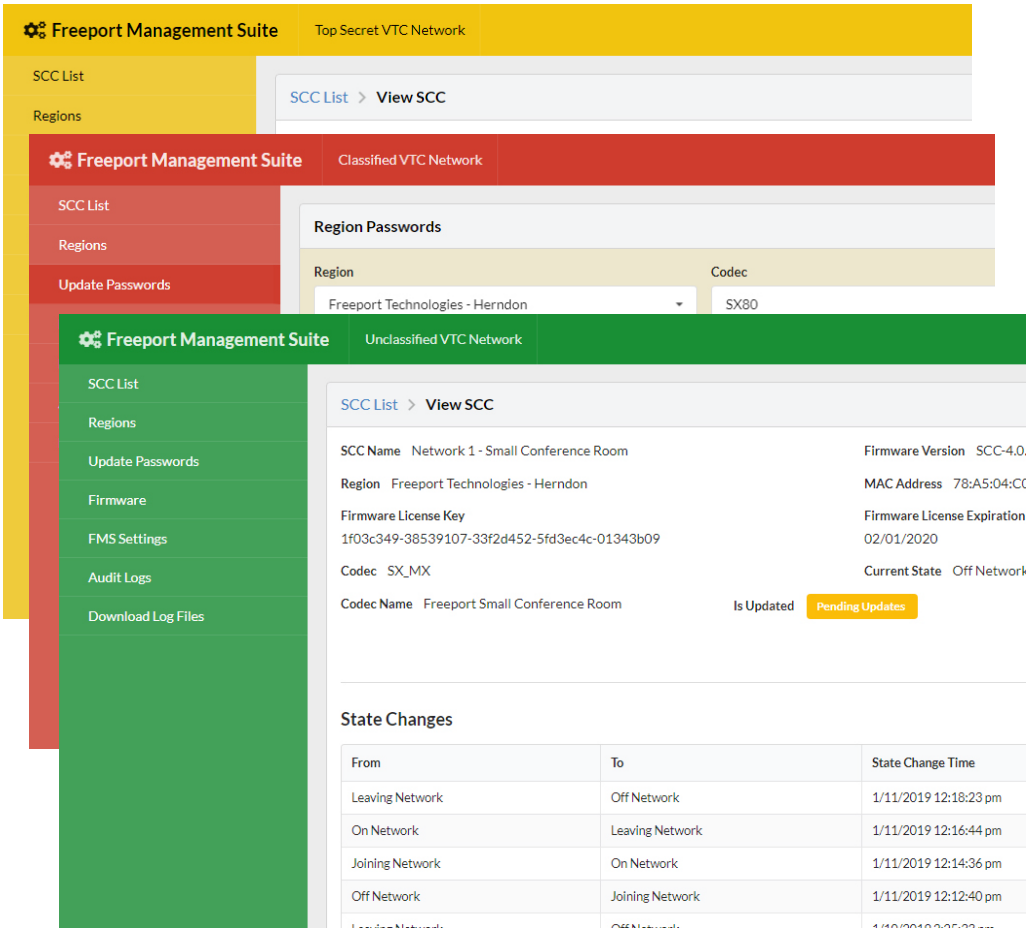
FREEPORT MANAGEMENT SUITE

INSTALLATION GUIDE

(June 2023)



Point of Contact:
Freeport Technologies Help Desk
571-262-0422
TechSupport@freeporttech.com

1 Introduction

This document will guide you through the process of setting up a Windows server to host the Freeport Management Suite (FMS) v4 application.

2 Operating System

2.1 Windows Server

The recommended operating system is Microsoft Windows Server 2019, Microsoft Windows Server 2016 or Microsoft Windows 2012 Server R2. Windows 2008 Server R2 is also supported but may require installation of additional prerequisite software. Recommend minimum 2 GB RAM, 60 GB disk space.

2.2 Web Server Role

On a new Windows Server installation, IIS must be enabled. The machine should be registered on the domain with the correct name before this is done. Use the "Add Roles and Features" wizard via the "Manage" menu or the link in "Server Manager." On the 'Server Roles" step, check the box for "Web Server (IIS)." Check the box to add management tools. On the "Role Services" step, accept the default role services and add "Windows Authentication."

2.3 .NET 3.5 Feature

SQL Server Management Studio 2012 will require the .NET 3.5 Feature. Install this with the "Add Roles and Features" wizard. SQL Server Management Studio 2016 or later does not require the .NET 3.5 Feature.

2.4 Windows Update

Make sure all important updates from Windows Update are installed before proceeding.

2.5 Internet Explorer Enhanced Security Configuration

The FMS web server requires write access to a directory on the server, for logging as well as for writing temporary files to push firmware to SCC's. If IE Enhanced Security is enabled, it may be necessary to grant additional permissions to the IIS application pool account or run the application pools under another account.

3 SQL Server

FMS uses an SQL Server database. The minimum version is SQL Server 2012; later versions are supported. SQL Server Express Edition can be used. The database may be hosted on the server where FMS is installed or on a different machine, e.g. a database server. If the database is hosted on a separate machine, Microsoft SQL Server Management Studio is required to be installed on the FMS host. Windows Authentication or SQL Server Authentication are supported. If you want to use SQL Server Authentication, then Mixed Mode Authentication is

required at the time of installation. If the database is installed locally, use the default instance if possible.

4 Prerequisites

The FMS installer includes the Microsoft .Net Windows Server Hosting redistributable and the Microsoft Windows Desktop installer. This feature may be deselected if it is already installed (e.g. upgrades).

FMS prior to version 4.2 also depended on Microsoft .NET Framework 4.6.1 or later. This is not included in the installation executable. It can be found on the installation media (NDP461-KB3102436-x86-x64-AllOS-ENU.exe) if it is not already installed. This may also be installed as a Windows Feature using Server Manager.

Windows 2008 Server R2 may require additional prerequisites.

5 Installation

5.1 Database Deployment

Use SQL Server Management Studio to install the database package (DACPAC). From the object explorer, right-click on "Databases" and select "Deploy Data-Tier Application." Navigate to the SCC.dacpac file included in the installation media. Finish the wizard.

5.2 Install FMS

Run the FmsSetup.exe to install the FMS web site files and the Freeport.SCCManager.DbConfig.exe program. It is recommended to change the installation directory to a secondary partition.

5.3 Configure Database Connection

After FMS finishes installing then start the Database Configuration tool (Freeport.SCCManager.DbConfig.exe). On the Connection tab enter the SQL Server IP address or server name along with the database name (e.g. SCC). Select Windows Authentication or SQL Server Authentication. Remember to click Save after making any changes.

If you are using Windows Authentication, then select the IIS tab and enter the Windows User account information that will be used. Remember to click Save after making any changes.

On the Connection tab click the Test Connection button to verify your database connection information is correct and the database is accessible from the FMS server.

The database connection information is stored in the Windows Registry, under the following key: HKEY_LOCAL_MACHINE\Software\Freeport Technologies\SCC Manager\Database

The database name, server, username, and password may be edited. The password is entered as plain text and will be encrypted after first use.

5.4 Configure IIS

5.4.1 Default Website

FMS is installed as a new web application at the top level. It will be bound to the same ports as the default web site in IIS. Stop the default web site and start FMS. Alternatively, specify alternate ports for either the default web site or FMS.

5.4.2 Secure Sockets

A valid server certificate should be configured for FMS. Prior to FMS version 4.2, it is necessary to manually create the HTTPS binding. In IIS Manager, select the FMS web site and click ”Bindings”. Add the HTTPS binding on port 443 if necessary. Select a valid certificate to sign the web server. The HTTP binding is still required if the server will manage generation 1 or 2 SCC’s.

5.5 Restart IIS

A restart of IIS is required after initial installation of the Microsoft .Net Core Windows Server Hosting bundle included in the FMS installer. If the installation does not require a reboot, restart IIS after the FMS installation is completed.

6 Upgrades

6.1 Upgrade the Database

From SQL Server Management Studio object explorer, right click on the SCC database and select Tasks -> Upgrade Data-tier Application. Navigate to the Scc.dacpac file and complete the wizard.

6.2 Upgrade FMS

6.2.1 Updating From Version 4.1.x.x

From Control Panel -> Programs and Features, right-click on FMS and select Uninstall. This will remove most of the files in the installation directory (c:\Freeport Technologies by default).

These files may remain:

- RegKeyFile.txt
- appsettings.json in the Api and Web directories
- Logs directories under Api and Web directories

Any other files should be removed. The web site in IIS will not be removed. The uninstaller may request a reboot. Afterwards, run the new FmsSetup.exe.

6.2.2 Upgrading From Version 4.0.x.x

From Control Panel -> Programs and Features, right click on FMS and select Uninstall. From IIS Manager, remove the SCCManager web site and the SCCManager and SCCAPI application pools. Run the new FmsSetup.exe. Follow the steps above to configure IIS again.

6.2.3 Remove FMS

To completely remove FMS, first run the uninstaller. Use IIS Manager to remove the FMS web site and FMS and SccAPI application pools. Remove the installation directory (C:\Freeport Technologies by default.) Delete the registry entries under HKEY_LOCAL_MACHINE\Software\Freeport Technologies\SCC Manager. The Microsoft .NET Core Windows Server Hosting bundle may be uninstalled through Control Panel – Programs and Features if no other web sites are using it. The Microsoft Windows Desktop Runtime 7.x may be uninstalled if it is not being used by other desktop applications.

7 Troubleshooting

7.1 Compatibility Mode

In Internet Explorer, FMS will not run in compatibility mode. It may be necessary to go to Compatibility View Settings and disable “Display intranet sites in Compatibility View.”

7.2 IIS

7.2.1 Failed Upgrade

On older operating systems or earlier IIS versions, the installer may fail when upgrading FMS. In this case, manually remove the web site from IIS Manager after uninstalling the old version and prior to running setup. It will then be necessary to recreate the HTTPS binding and select the certificate after setup completes.

7.2.2 Bindings

Prior to version 4.2, the installation requires an HTTP binding (port 80). If the FMS web site is already installed, but the HTTP binding has been removed, the upgrade might fail. Temporarily bind to port 80, install, and remove the binding. IIS can be stopped so that the HTTP binding can never be used. This issue should not occur for FMS version 4.2 and later.

7.2.3 Authentication

Authentication settings should be verified after installing FMS. Navigate to IIS Manager and select the “FMS” web site. Open the “Authentication” item. Anonymous Authentication should be disabled, and Windows Authentication should be enabled. Then select the “SCCManager” application under FMS, Anonymous Authentication should be enabled, and Windows Authentication should be disabled.

7.2.4 Web site logging

IIS will log accesses to the user interface web site and the SCC API website in the following default location:
C:\inetpub\logs\LogFiles\W3SVC
More detailed logs will be created in the Logs subdirectories of the API and Web folders under the installation directory.

8 Initial Configuration of FMS

8.1 Default account

FMS uses Windows authentication, but it is necessary to bootstrap which users or groups may access the application. At the login screen, choose authentication type "FMS Credentials." Enter the default credentials:
Username: sysop
Password: freeporttech

It is recommended to change the password for this account. Navigate to "FMS Settings" and enter the new Admin Password.

8.2 Windows Authentication

To configure Windows users to be able to access FMS without knowing the FMS credentials, navigate to FMS Settings. Enter the name of existing Windows domain user groups or users that can be mapped to the user, admin, and super admin roles. For example, under Admin Groups, enter "Administrator." All domain administrators will be granted the admin role in FMS.

The super admin role includes the ability to modify FMS Settings. The admin role includes the ability to modify regions, passwords, and firmware. The user role includes the ability to manage SCC's.

8.3 Approve SCC's

When an SCC first contacts the manager, it will be added to the SCC list as "Pending Approval." Until a user approves the SCC, FMS will not trust it and will not send any passwords. The SCC will be identified by its IP Address and MAC address in the SCC List. Assign the SCC to a region before approval.