

## 12.0 Security Measures

Security measures for the operating system and database are discussed in the following sections.

### 12.1 Operating System Security

Security measures in FEMIS include security goals, user account management, user identification number (UID) and group identification number (GID) management, password protection of accounts and files, other encryption, no access files, and NFS connections scripts. Consideration of factors common with EMIS operation on a PC or UNIX server has been taken into account.

#### 12.1.1 FEMIS Operation System Security Goals

The goals of security measures taken for FEMIS include the following:

- Establish the unique UID number, login name, and secret password for each user in the EOC. Users will maintain their own passwords.
- Verify that there is no access from ordinary user accounts to files on the UNIX server that might contain sensitive information.
- Verify that security measures are compatible with EMIS operations. Run FEMIS and EMIS on same PC. Run FEMIS and EMIS from the same login.

#### 12.1.2 User Accounts

Each individual who uses FEMIS needs an account on the Windows workstation and UNIX server. For FEMIS, multiple accounts must be maintained on both Windows and UNIX systems for security reasons.

Every person using the EOC computing resources needs a user account. If deemed suitable, an EOC's System Administrator can create and maintain user accounts for each and every person who will be using a FEMIS workstation.

As an alternative, your System Administrator may want to set up groups of users rather than individuals. In that case, several people would use the same user name and password. Examples are setting up user accounts based on operating position in the EOC, e.g., *safe* for Public Safety or *tran* for Transportation.

#### 12.1.3 UID and GID

The UID is a number that identifies user accounts in UNIX. Each user account, individual, or position must be assigned a unique UID. These numbers must be unique so that no two user names

at the EOC will have the same UID. PNNL suggests using UIDs in the range from 100 to 60,000. The main use of UID is to establish ownership of files on the UNIX system.

The GID identifies group. Each and every user account created on the UNIX server for the purpose of running FEMIS must be included in the `femisrun` group.

During execution of FEMIS on a PC workstation, files created by that PC on the `M:\` drive will have ownership/group `userid/femisrun`, where `userid` is the UID/username of the user account.

Files created by FEMIS PCs on `M:\` are for the Evacuation model log files and result files. FEMIS can be run without mapping drives as long as the Evacuation module will not be used.

At EOCs where both FEMIS and EMIS are being installed on the same server, the choice of UID and GID numbers should be coordinated with the EMIS vendor to ensure that these unique numbers do not overlap.

## 12.1.4 Passwords

A user or System Administrator must be concerned with two types of passwords, the Windows PC password and that user's password on the FEMIS UNIX server unless using Samba with Windows authentication (See Section 14.2.2, Samba Services). The Windows and UNIX passwords must be the same for FEMIS to work. If both EMIS and FEMIS are to be run from that user's PC, then they need to be concerned about the EMIS UNIX server password also.

Upon a FEMIS user logging onto a PC, the FEMIS startup script, `FSTARTUP.EXE`, is run from the `startup` group. The result is network connections being made via NFS or Samba to the FEMIS UNIX server. A connection to drive `M:\` is typically established.

The users of FEMIS should be responsible for maintaining their own Windows login password and UNIX password(s) (if applicable). A user's UNIX account password should be identical to their Windows account password unless using Samba with Windows authentication (See Section 14.2.2, Samba Services). That way, they only need to enter a password once, at the Windows Login Information dialog box. The password entered there will be reused for NFS/SMB connections needed in `FSTARTUP.EXE`. If the NFS/SMB connection password authentication fails, `FSTARTUP.EXE` will prompt the user for his/her password(s).

Since a user's Windows and UNIX passwords should be the same, UNIX password rules (the more limiting of the two) must be used in the case of NFS only. UNIX/NFS passwords must contain 1) two to eight letters or digits, 2) first character must be a letter, 3) at least one character must be lower case, and 4) may not contain a space or a new line (`\n`). A password should differ from the user's login name or any circular shift of that name. Passwords should differ from the old password by at least three characters. Password uniqueness must be established in the first eight characters. Mismatches in characters beyond eight may or may not be detected.

Each user (or group of users) is responsible for maintaining his/her own password. If password management is done by group, one person in that group should have prime responsibility for maintaining the password and letting it be known to others in that group.

Password maintenance on the PC is performed via `Ctrl-Alt-Delete`, which runs the Windows Security dialog box. UNIX password maintenance is accomplished by running `telnet` to the UNIX server and using the `passwd` command for NFS (`/etc/passwd`) authentication and `/apps/samba/bin/smbpasswd` for Samba (`/etc/samba/private/smbpasswd`). Passwords maintained by a Primary Domain Controller (PDC) are administered either by the user using the `Ctrl-Alt-Delete` mechanism as an individual user or by running the Windows application `User Manager for Domains`. Setting both passwords to the exact same string ensures that the password only needs to be entered once at the main Windows login window.

### 12.1.5 Encryption

Windows, Samba, and UNIX account passwords are encrypted in the default methods of Windows and the Sun Solaris operating systems. No other methods are incorporated in FEMIS for encrypting authentication passwords.

Data transmitted to and from the FEMIS command server are currently encrypted using a DES-like algorithm. A future version of FEMIS may use SSL. None of the other FEMIS daemons currently use encryption.

### 12.1.6 No Access Files

Some files in FEMIS may contain passwords or other sensitive information. These files have been made inaccessible to the normal EOC user accounts. This is accomplished by setting `ownership/group` to `femis/noaccess` and protection mask to `600 (rw-----)`, which results in no read access to the world. An example is the FEMIS Command Server configuration file. Do not change the protection to something else, e.g., `644`, as the world will be able to display and read any sensitive information contained in that file.

### 12.1.7 FEMIS/EMIS Issues

It is possible to run both EMIS and FEMIS on the same PC workstation and from the same Windows login. FEMIS uses drive `M:\` for access to a UNIX server. EMIS uses network drives `N:\` and `S:\` to access files on a UNIX server (may also use drive `I:\` and `T:\`).

It is also possible to install and run both EMIS and FEMIS on the same UNIX server. Security models for UIDs, GIDs, and file ownership for the two systems are compatible.

Installations where both EMIS and FEMIS are supported on one or more UNIX servers will need user account maintenance in accordance with EMIS system administration.

**Note:** NIS+ is used in EMIS for maintaining user accounts.

## 12.2 Database Security

Most of the database access security in FEMIS was added in the previous versions. This was accomplished by creating these additional Oracle schemas for each EOC's Oracle database:

- FEMIS login schema – This initial access schema can only view part of a single table in the database. The password for this account is fixed and stored in the FEMIS initialization file, but the schema can only query parameters needed to perform the initial validation of a user's login.
- FEMIS application schema – This schema is used to access the FEMIS Oracle database from the FEMIS application after a successful login. This schema can view and edit data within the FEMIS database but does not have the ability to change the structure of the FEMIS Oracle tables or perform Oracle administrative functions.
- FEMIS management schema – This schema is used to create and manage the tables, indexes, procedures, and other objects of the database. This schema “owns” the production data and is used to complete all data administrative functions that are necessary.
- FEMIS administration schema for UNIX account – This schema is used by AutoRecovery and other UNIX processes to access the local Oracle database. The password is identified externally to Oracle and is managed by UNIX, which provides security and change capabilities for the UNIX `femis` user account.

It is a long term goal to add more database security to prevent accidental or malicious access problems from occurring. Recent security measure changes are

- Increased security for database replication
- Modifications to Manage Database Passwords tool.

### 12.2.1 Replication Schema

The Oracle schema provides the capability to manage shared database information with remote servers. This schema manages the propagation of shared data and is named `PROP`. Each server database has one `PROP` user that is responsible for pushing local changes to remote databases and handling updates from remote databases. The password for this schema can be changed from the PC based password tool.

## 12.2.2 Modifications to the Manage Database Passwords Tool

The `Manage Database Passwords` tool was implemented in FEMIS v1.4.6 to change the password for an application database schema or a management database schema. It can also be used to restore all owner schema passwords for the site to the installation defaults. The tool was updated in the current release to also change the propagator password.

In FEMIS v1.5, the tool requires the user to supply at least one password to be able to do any changes. This corrected a problem with the previous version that could restore default passwords without supplying a password. A brief description of the tool follows.

**Warning:** Before using this tool, be sure that all of the appropriate servers, databases, and networks are operating normally and that you know all of the necessary passwords to complete this operation. Also make sure the FEMIS ODBC data source names on the PC are correct and complete for all databases affected. If the environment is not complete or the passwords are not known, the process may only partially finish, requiring manual intervention from a System Administrator to appropriately restore the passwords.

In general, this tool is used as follows:

1. Select a Data Source Name (DSN). The default upon entry is the DSN for your EOC.
2. Select one of the four available password options (discussed below).
3. Enter the old and new passwords in the `Change Schema Password` fields, if prompted.
4. Click the `Execute` button.
5. Respond to input requests.

**Note:** Remember that Oracle passwords are case sensitive.

### Option 1: Change the Application Password

This option will change the password of the application database schema. This is the schema used by the FEMIS application itself. It has only the database privileges necessary for the execution of the FEMIS application and some of its utilities.

To change an application database schema password, complete the following steps:

1. Select the DSN for which you wish to change the application database schema password from the `Data Source Name` drop-down list.

2. Select the `Change This Application Password` option button.
3. Enter the current password in the `Old Password` field.
4. Enter the new password in both of the `New Password` fields. The password must be between 4 and 16 characters in length and may only contain alphanumeric characters.
5. Click the `Execute` button. The process will run, changing the application schema password for the specified EOC.

Progress messages will appear in the `Process Log` field. The last progress message will indicate whether or not the full process was successful.

6. Click the `Clear Log` button to reset the window, or the `Close` button to close the window.

### **Option 2: Change the Management Password**

This option will change the password of the management database schema. This is the schema that owns the objects in the FEMIS database. Since this is the schema that exists on all servers in a multi-server configuration, changing this password involves all site servers.

To change an owner database schema password, complete the following steps:

1. Select the DSN for which you wish to change the owner database schema password from the `Data Source Name` drop-down list.
2. Select the `Change This Owner Password` option button.
3. Enter the current password in the `Old Password` field.
4. Enter the new password in both of the `New Password` fields. The password must be between 4 and 16 characters in length and may only contain alphanumeric characters.
5. Click the `Execute` button. The process will run, changing the owner schema password for the specified EOC.

Progress messages will appear in the `Process Log` field. The last progress message will indicate whether or not the full process was successful.

6. Click the `Clear Log` button to reset the window, or the `Close` button to close the window.

### Option 3: Change the Propagator Password

This option will change the password of the propagator database schema. This is the schema that controls the FEMIS database replication. Since this is the schema exists on all servers in a multi-server configuration, changing this password involves all site servers.

To change the propagator database schema password, complete the following steps:

1. Select any DSN from the `Data Source Name` drop-down list.
2. Select the `Change Propagator Password` option button.
3. Enter the current password in the `Old Password` field.
4. Enter the new password in both of the `New Password` fields. The password must be between 4 and 16 characters in length and may only contain alphanumeric characters.
5. Click the `Execute` button. The process will run, changing the propagator password for all EOCs.

Progress messages will appear in the `Process Log` field. The last progress message will indicate whether or not the full process was successful.

6. Click the `Clear Log` button to reset the window, or the `Close` button to close the window.

### Option 4: Reset All Owner and Propagator Passwords

This option will restore all owner and propagator schema passwords for the site to the installation default. It would typically be used only as part of an installation or upgrade process.

To reset all owner and the propagator passwords, complete the following steps:

1. Make sure that a DSN has been selected from the `Data Source Name` drop-down list. While all DSNs will be affected, one needs to be specified initially as the source for the basic EOC information.
2. Select the `Reset All Passwords` option button.
3. Enter the current password for the propagator schema in the `Old Password` field.
4. Enter the new password for the propagator in both of the `New Password` fields. The password must be between 4 and 16 characters in length and may only contain alphanumeric characters.
5. Click the `Execute` button. The process will run, changing all of the owner and propagator schema passwords for the site.

If the current password for any given schema is not the default, you will get an Oracle login box for that schema. Enter the current password for that schema, and click the `OK` button. If you do not know the correct password, the process will terminate.

Progress messages will appear in the `Process Log` field. The last progress message will indicate whether or not the full process was successful.

6. Click the `Clear Log` button to reset the window, or the `Close` button to close the window.