

11.0 Security Measures

Security measures for the UNIX server and database are discussed in the following sections.

11.1 UNIX Server Security

11.1.1 Software Patches

The FEMIS installation should have included the latest OS patches and server software available during development and installation. Vendors periodically release patches or fixes to software installed when FEMIS is installed (i.e., Perl, Oracle, and Java). Before upgrading or installing patches to software installed, you should contact PNNL to determine if the change will affect the functionality of FEMIS. Applying the latest patches to NFS, Samba, and the Solaris operating system are however recommended to have the latest security and bug fixes. If installing a patch disrupts FEMIS functionality, remove the patch and contact PNNL.

11.1.2 Shared Directories

The FEMIS PCs will need to be able to run the FEMIS installation program located on the FEMIS server and periodically receive software updates. This requires directories being shared either through nfs (UNIX native file share) or smb (PC native file share). The two directories required are:

```
/home/femis  
/home/femis/user
```

These shares should be read-only (except for the femis user on `/home/femis`) for security purposes and to protect the integrity of the FEMIS configuration.

11.2 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.

11.2.1 Replication Schema

The Oracle `prop` schema provides the capability to manage shared database information with remote servers. This schema manages the propagation of shared data. 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.

11.2.2 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

In FEMIS v1.5.3, 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.