Ellipse Security

Ellipse EAM 9.0

Published: Tuesday, 16 October 2018

Legal Disclaimer

The product described in this documentation may be connected to, and/or communicate information and data via, a network interface, which should be connected to a secure network. It is your sole responsibility to ensure a secure connection to the network and to establish and maintain appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the product, the network, your systems, and the interface against any kind of security breach, unauthorised access, interference, intrusion, leakage, damage, or corruption or theft of data. We are not liable for damages or losses related to any such security breach, unauthorised access, interference, intrusion, leakage, damage, or corruption or theft of data.

Contents

Ellipse Security

Ellipse EAM comes with comprehensive and flexible security capability. Ellipse EAM enables you to secure applications (including programs, menus, and menu options), reports, batch programs, and reference codes.

Ellipse EAM uses two forms of security. The first is the protection of online, batch, and report programs through a process known as profile comparison. In this form, each program is allocated a protective profile, which is compared with the profile of the user attempting access to determine whether access is granted, and if so, how much access is permitted. The second form is for the granting of access to, and visibility of the elements of, the Ellipse EAM objects.

Maintaining Application Security - MSE

Security is used to ensure users have the correct level of access to the applications available in Ellipse EAM. The setting of security access is performed by the System Administrator.

All users are assigned a sign on profile. There are two types of profile available:

- **Sign On Profile** - This identifies individual users and are district specific.
- **Global Profile** - This can be used to define a standard set of access control information for users with common requirements.

Note: MSE Application Security is not related to Program Security (**MSO**). Application and Program security are maintained independently of each other, for example, the user can have access to **MSE005**, but not **MSO005**. Application and Program security only share the **Profile Name**, for example the **Global Profile** or **Sign on Name**.
For more information on program security, refer to ***Maintaining Program Security - MSO***.

MSE020 - Security allows you to secure and maintain the following:

- Applications which includes:
  - Application Classes
  - Application Methods and Attributes
- Reference Codes

By supplying security to these components, Ellipse EAM provides a greater deal of flexibility in the data that is presented to (or hidden from) users.

MSE020 uses four applications; these applications can be used to apply access levels to applications, classes, methods and attributes, review class details, review class methods and attributes and apply security to reference codes. The applications can only be accessed using ***MSE020*** and cannot be launched from the **Quick Launch** field on the **Home** screen.

Applications accessed using ***MSE020***:

- MSE02A - Class Security
- ***MSE02C*** - Security Classes
- ***MSE02D*** - Security Application
- ***MSE02R*** - Security Profile Reference Codes

Note: Before setting access levels for security profiles, it is important to read the information on ***Setting Security Access Levels for Applications, Classes, Methods and Attributes***. This information provides a full description on selecting the appropriate access level for Ellipse EAM applications.

Application

An application is a web page that consists of one or more Ellipse EAM classes and or reference codes. An example of an application is **MSE100 -** Catalogue. An application can have three levels of access:

- **0 - No Access** - The user is unable to launch the secured application from the **Quick Launch** and the application is removed from the Ellipse EAM menu structure.
- **1 - Review Access**
  - the user has the ability to search for application
  - the fields on the selected application are set to Read Only
  - the **Submit** button in the Detail screen is disabled
  - the **New** button on the Search screen is disabled
  - any button associated with the class method is also disabled

- **2 - Full Access**
  - the **Submi**t button is enabled allowing the user to save new or modified data
  - the **New** button is enabled allowing the user to create security profiles
  - depending on the class access, all fields and buttons associated with the class method is enabled

In some cases there are applications that have been defined as Review Only by Mincom, for example, **MSE010** - Tables. A Review application can have two levels:

- 0 - No Access
- 1 - Review Access

Class

A class represents an Ellipse EAM business entity, for example, a WorkOrderTask or HoldingsTask. A class provides all of the methods and fields that can be carried out in order to perform a given business process.

A class can have two levels of access:

- No Access
- Full Access

Method

A method represents an action that can be performed by a class, for example, the Workorder 'Create' method.

A method can have two levels of access:

- 0 - No Access
- 9 - Full Access

In some cases, there are methods that can have up to ten levels of access which have been defined by Mincom. An example of a method that has more than two levels of access is **MSE81H** - Employee Fetch method.

Attribute

An attribute represents a field or column that is used by a class, for example, Account Code. These attributes (fields or columns) display in the application screens.

An attribute can have three levels of access:

- **0 - No Access**
  - the attribute does not display in both the application's search or detail screens
- **1 - Read Only Access**
  - the attribute displays as read only in the Detail screen; no data can be entered in the field or column
- **2 - Read/Write Access**
  - data can be entered in the field or column

In some cases, an attribute will be defined as a key attribute (mandatory field) to a method. In this case, the attribute will only have two levels of access:

- 0 - No Access
- 1 - Read/Write Access

Reference Codes

Only reference codes associated with an Ellipse EAM application display in the Ellipse EAM security applications. For further information on reference codes, refer to Maintaining Reference Codes.

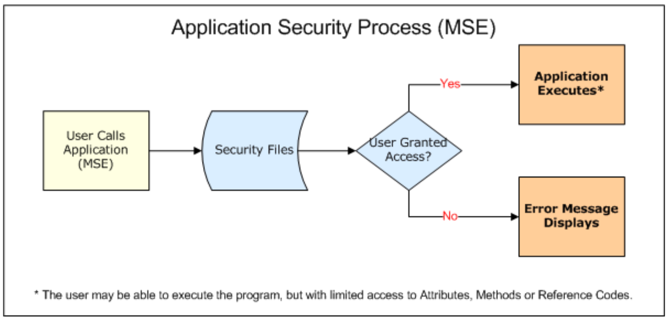
A reference code can have three levels of access:

- **0 - No Access**
    - the reference code tab does not display in the application's Search or Detail screens
- **1 - Read Only Access**
    - the reference code grid on the Detail page displays as read only; no data can be entered
- **2 - Read/Write Access**
    - data can be entered in all columns of the reference code grid in the Details screen

Diagram

The ***Maintaining Application (MSE) Security*** diagram represents the security profile process.

Maintaining Application (MSE) Security - Diagram



* The user may be able to execute the program, but with limited access to Attributes, Methods or Reference Codes.

Setting Security Access Levels for Applications, Classes, Methods, and Attributes

Use this information to apply the appropriate security access level for an Ellipse EAM application, including classes, methods, and attributes.

Note: This section gives a basic overview for applying security access levels. Not all scenarios are covered in this section.

Application Security

The profile has **No Access** to an application and **No Access** to the Application subordinate classes.

a. Set application to **Review Only**:
   1. The subordinate class is set to **Full Access**.
   2. All Read Only methods of the class are set to **Full Access**.
   3. All update methods of the class are set to **No Access**.
   4. All attributes of the class are set to **Read Write Access**.
   5. The application's subordinate reference code is set to **Review Only**.

b. Set application to **Full Access**:
   1. The subordinate class is set to **Full Access**.
   2. All methods of the class are set to **Full Access**.
   3. All attributes of the class are set to **Full Access**.
   4. The application's subordinate reference code is set to **Full Access**.

The profile has **Review Only** access to the application but **Full Access** to a subordinate class.

a. Set Application to **Full Access**:
   1. The application is set to **Full Access**.
   2. The subordinate class access remains unchanged.

      Note: Once a class security has been set, there is no longer any interaction between the application and the class, this is because a number of applications may use the same class, for example **MSE100**, **MSE171** and so on, these applications all use the Catalogue class.

      A warning is returned as a visual clue to indicate that the class has been previously defined and requires investigation into why the class has been secured and what its relationship is to the application.

The profile has **Review Only** access to the application but **Full Access** to a subordinate class.

a. Set Application to **No Access**:
   1. The application is set to **No Access**.
   2. The subordinate class access remains unchanged.

The profile has **Full Access** to an application but secured access to a class. Secured access is **Full Access** to the class, but access to one or more methods or attributes has been set to **Read Only** or **No Access**.

a. Set the application to **Review** access:
   1. The application is set to **Review Access**.
   2. The subordinate class access remains unchanged.

b. Set the application to **No Access**:
   1. The application is set to **No Access**.

2. The subordinate class access remains unchanged.

The profile has **No Access** to an application but a subordinate class has limited access.

a. Set the application to **Review** access:
    1. A warning displays for each subordinate class - '**<Class> has secured access**'.
    2. The application will now have **Review** access.
    3. The subordinate classes highlighted in the warning remain unchanged.

b. Set the application to **Full Access**:
    1. A warning displays for each subordinate class - '**<Class> class has secured access**'.
    2. The application will now have **Review** access and the subordinate classes which display in the warning remain unchanged.

The profile has **Full Access** to an application but limited access to a class.

a. Set the application to **Review** access:
    1. The application is set to **Review** access.
    2. The subordinate class access remains unchanged.

The profile has **Full Access** to an application and **Full Access** to a subordinate class.

a. Set the application to **Review Only**:
    1. The application is set to **Review**.
    2. The subordinate class access remains unchanged.

b. Set the application to **No Access**:
    1. The application is set to **No Access**.
    2. The subordinate class access remains unchanged.

c. Set an application subordinate class to **No Access**.

    If the class is a primary class of an application (primary class to application rules are defined by Mincom):

    1. A warning - '**<Class> class is a primary class for <Application>, application access will be removed**' displays for all applications where the class is primary for the application.
    2. Each application displayed in the warning is set to **No Access**.
    3. The class is set to **No Access**.

    - All methods of the class are set to **No Access**.
    - All attributes of the class are set to **No Access**.

      If the class is not a primary class:

    - Application access remains changed.
    - The class is set to **No Access**.

      All methods of the class are set to **No Access**.

      All attributes of the class are set to **No Access**.

Attribute Security

The profile has full access to an attribute.

a. Set the attribute to **Read Only** access:
    1. If the attribute is a key field for a method (key field rules are defined by Mincom):

    - A warning '**<Attribute> is key field of <Method>, method access will be removed**' displays for all methods where the attribute is a key field.
    - Each method displayed in the warning is set to **No Access**.

- The attribute is set to **Read Only** access.

  If the attribute is a standard attribute:

- The attribute is set to **Read Only** access.

b. Set the attribute to **No Access**:

   1. If the attribute is a key field for a method (key field rules are defined by Mincom):

   - A warning **'<Attribute> is key field of <Method>, method access will be removed'** displays for all methods where the attribute is a key field.
   - Each method displayed in the warning is set to **No Access**.
   - The attribute is set to **Read Only** access.

     If the attribute is a standard attribute:

   - The attribute will be set to **No Access**.

Reference Code Security

The profile has **No Access** to an application and **No Access** to the application's subordinate reference code.

a. Set the application to **Review**:

   1. The application access is in **Review**.
   2. The subordinate reference code is set to **Read Only** access.

The profile has **Review** to an application and **Review** access to the application's subordinate reference code.

a. Set the application to **Full Access**:

   1. The application access is **Full Access**.
   2. The reference code remains at **Review Access**.

The profile has **Full Access** to an application and **Full Access** to the application's subordinate reference code.

a. Set the Application to **Read Only** access:

   1. The application access is **Read Only**.
   2. The subordinate reference code access remains unchanged.

b. Set the Application to **No Access**:

   1. The application access is **No Access**.
   2. The subordinate reference code access remains unchanged.

The profile has **Review** to an application and **No Access** to the application's subordinate reference code.

a. Set the Application to **Full Access**:

   1. The application access is **Full Access**.
   2. The subordinate reference code access is **Full Access**.

The profile has **No Access** to an application and **Review** access to the application's subordinate reference code.

a. Set the Application to **Full Access**:

   1. The application access is **Full Access**.
   2. The subordinate reference code remains unchanged.

Security Procedures

The security procedure application allows for setting-up and maintaining the Ellipse EAM security facilities.

Users should have an understanding of the Ellipse EAM application architecture before using the system, in particular the differences between **MSE** (application) and **MSO** (program) applications.

The prime function of Ellipse EAM security is to provide access control over:

- Applications (**MSE**), which includes:
    - Application classes
    - Application methods and attributes
- Reference codes
- Reports and batch programs
- Programs (**MSO**)

Note: Before setting access levels for security profiles, it is important to read the information on ***Setting Security Access Levels for Applications, Classes, Methods and Attributes***. This information provides a full description on selecting the appropriate access level for Ellipse EAM applications/programs.

The following is the recommended procedure for setting up Ellipse EAM security:

Note: This procedure assumes mixed application and program security is in use. The procedure is also applicable to those clients using program security exclusively.

- Determine profile positions for program (**MSO**) applications and reports.

  Ensure that allowances are made for applications with special security match values.
- Document profile positions in the table file - Security Profile Position Descriptions.
- Create program profiles for each program using ***MSM020A*** - Maintain Security Profile. Sign-On profiles should where possible, be created using a Global profile.
    - Create entity profiles for each Reference Code entity to be secured.
- Determine common user groups (for example, Purchasing Officers, Maintenance Planners, and so on) and their access requirements.
    - Create Global Profiles for each group of users using the Security Maintenance program (**MSO020**)
    - Add Applications (**MSE**) to the Global Profile using the Security Application (***MSE020***)
- Add Global Profiles to Establishment Positions if appropriate.
- Create Sign-On Profiles using the Security Maintenance program (**MSO020**).

Security Program (MSO) Applications

Access control over programs is achieved by limiting the applications that a user can start when using the Ellipse EAM user interface. This is accomplished through a profile matching process that operates as follows:

- Each program to be secured is given a program profile. Each user is given a sign-on profile (the make up of the sign-on profile is derived from a global profile).
- The system checks each non-blank position in the sign-on profile with each corresponding position in the program profile.
- If there is a value in a corresponding position and the value in the sign-on profile is equal to, or greater than the value in the program profile, then access is granted.

For example (simple):

Profile Type	Profile Name	Profile Positions			
		01	02	03	04
Program	MSO220	9	1		
Program	MSO200	9		1	
Sign-On (derived)	Fred	0	1	1	
Sign-On (derived)	Mary	0	0	1	

In this example, Fred has access to both **MSO220** and **MSO200** while Mary only has access to **MSO200**.

Note: By default a user has access to ALL programs unless the security system removes that access.

The security system not only controls access to applications but in certain cases limits the use of specific functions within an application (for example, a user with access to the requisition program can enter a warehouse requisition, but not a purchase requisition). These applications have embedded security levels that apply in the profile matching process.

To give users the correct level of access within programs with specific security levels, the correct match value (as documented under ***Security Specifics***) must be entered in the Sign-On profile (or derived from the Global profile).

For example (simple):

Profile Type	Profile Name	Profile Positions			
		01	10	11	12
Program	MSO080	9			1
Program	Harry	0	0	0	1
Sign-On (derived)	Fred	0	0	0	2
Sign-On (derived)	Mary	0	0	0	5

In this example Harry, Fred and Mary all have access to program **MSO080** - Request Reports. Harry can only request single copies of reports, Fred can request multiple copies and Mary can request multiple copies, and submit the report for immediate processing.

Sign On Profile

To access the system an Ellipse EAM sign-on profile is required.

Recommendation:

- Because the employee is linked to the sign-on profile, it is recommended that individual Ellipse EAM sign-on profile be assigned to each person accessing the system.

The Ellipse EAM sign-on profile is used in conjunction with the login position (if Position Management is installed) to determine the access rights of the person trying to access the system. To determine access rights the system checks for profiles in the following sequence.

- Global Profile for the login Position/Employee combination
- Global Profile for the login Position
- Global Profile for the login user ID
- Sign-On Profile for the user ID

Note: If the sign-on profile is not the same as the Employee ID, the password functionality on the requisition screens cannot be used.

Access to Employee Data

Where the HR modules are installed, facilities exist to restrict access to data related to employees. In certain instances, some users may require access to all employees, however in most cases access should be restricted to a nominated set of employees (for example, within a group or within a pay group). This restriction is provided by assigning access rules to a user's position in the Establishment; this defines which category of employee the user can access.

In order to implement this level of security, the Position Management module must be installed.

User profiles must be created, including the assignment of a user ID to an employee ID (for further details, refer to ***MSM020B*** - Maintain UserID Profile).

- An employee, with access to the system, must be assigned to a position. The user profile (the profile that determines access to programs) can then be defined at the following levels:
  - When the employee is assigned to a particular position (using **MSE81S** - Update Personnel workbench). This allows different incumbents in the same position to have access to different programs.
  - When the position is defined (**MSO870**). This allows all incumbents in a position to have access to the same programs.
  - When the user profile is defined. This allows a user to access a specific set of programs. The system will search for a user profile in the order defined above. This allows maximum flexibility in the use of user profiles. For example, a user who is temporarily incumbent in a position may have access to a different set of programs while in that position, but will automatically revert to their standard profile when they leave that position.
- An access rule and value must be assigned to a position (using **MSO870**). The following access rules are available:
  - **1** allows access only to the employee assigned to the user
  - **2** allows access only to employees on the same level or one level down in the organisation hierarchy. Access to terminated employees is based on the employee's position before termination
  - **H** allows access only to employees in positions below the user's position, or to a specific position nominated in the access value. Access to terminated employees is based on the employee's position before termination
  - **A** allows access to all employees
  - **B** allows access to all employees except the user
  - **I** allows access only to those employees in the pay groups (up to 20) nominated in the access value
  - **E** allows access only to those employees not in the pay groups (up to 20) nominated in the access value
  - **L** allows access only to those employees in the pay locations (up to 35) nominated in the access value
  - **W** allows access only to those employees in the work groups (up to 10) nominated in the access value

Note: If a user profile has a match value greater than 4, these data access restrictions are ignored. This allows the user to access all employees, using the relevant program.

Access to Inventory Categories

For customers using the Category Management function of the Warehouse Management module, additional access control can be applied to inventory categories. This facility limits those users who can review holdings, enter requisitions and process transactions in respect to inventory held in specific categories. Categories for inventory items are set up on the IG - Inventory Category table file.

This access control is achieved through category match value processing, not through the Ellipse EAM security. To use this function:

- A match value (0 to 9) is assigned to each Inventory Category using associated values to the IG - Inventory Category table file.
- In the Position Management module, positions are also assigned a category match value. When a user attempts to access information about items assigned to an inventory category, Ellipse EAM checks if the category match value for their position is equal to or greater than the category match value for the category. If it is, the category and its items will be visible to the user.

Create a Security Profile

Use this activity to create a security profile.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Select **New**.

   The ***MSE020*** - Create Security screen displays.

3. Perform one of the following steps:

   a. To create a **Global** security profile:

      1. Enter data in the following fields:

         Profile Name

         Profile Type (Select **Global**)

      2. Enter data in the following field in the ***Profile Details*** tab:

         Owner Id (Optional)

> **Note:** When **Global** is selected as the profile type, all fields in the **Profile Details** tab are disabled except **Owner Id**.

   b. To create a **Sign On** security profile:

      1. Enter data in the following fields:

         Profile Name

         Profile Type (Select **Sign On**)

      2. Enter data in the following fields in the ***Profile Details*** tab:

         Employee Id

         Menu Name

4. Select **Submit**.

   The security profile is saved and the ***MSE020*** - Security detail screen displays.

   The ***Applications*** and ***Class*** tabs are populated with all applications and classes currently available in the system.

Modify a Security Profile

Use this activity to modify security profile details.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Modify data in the ***Profile Details*** tab as required.
5. Select **Submit**.

   The security profile changes are saved.

   To modify security access levels for applications, class methods and class attributes, refer to the following activities:

   Modify Security Access Levels for an Application

   Modify Security Access Levels for Application Classes

   Modify Access Levels for Class Methods

   Modify Access Levels for Class Attributes

Delete a Security Profile

Use this activity to delete a profile.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Delete**.

   The confirm deletion message displays.

5. Select **Submit**.

   The profile is deleted. The ***MSE020*** - Security detail screen displays.

Copy a Security Profile

Use this activity to copy a security profile.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Save As**.

   The Dialog Box - ***Save As*** displays.

5. Enter data in the following fields in the **Save To** section:

   Profile Type

   Profile Name

6. Select **Submit**.

   The security profile is saved.

Open a Security Profile using MSE or MSO Program Security

Use this activity to open a Security Profile using MSE or MSO Program Security.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Perform one of the following steps:

   a. To open **MSE** security details for a profile:

      1. Click the Grid Action Menu icon beside the required profile.
      2. Select **MSE Program Security.**

         The ***MSE020*** - Update Security screen for the selected profile displays.

   b. To open **MSO** security details for a profile:

      1. Click the Grid Action Menu icon beside the required profile.
      2. Select **MSO Program Security**.

         The ***MSM020A*** - Maintain Security Profile screen displays.

4. Review or modify details as required.

Modify Security Access Levels for Applications

Use this activity to modify the access levels of applications.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Class Security**.

   The MSE02A - Update Class Security screen displays the applications associated with the selected profile.

5. Perform one of the following steps:

   a. To select the required application from the tree view:

      1. Scroll through the list of applications in the tree view and select the required application.

         The ***MSE02D*** - Update Security Application screen displays.

   b. To select the required application using **Go To**:

      1. Select **Go To** from the **MSE02A** screen.

         The Dialog Box - ***Go To*** displays.

      2. Enter data in the following field:

         Application Name

      3. Select **OK**.

         The ***MSE02D*** - Update Security Application screen displays the application and its associated classes in the tree view.

6. Select the required access level from the ***Access Level*** field.

   Note: Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to an application.

7. Select **Submit**.

   The access level is modified and saved.

Review Security Classes for an Application

Use this activity to review security classes associated with an application.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Class Security**.
5. The MSE02A - Update Class Security screen displays the applications associated with the selected profile in the tree view.
6. Select the Expand icon beside the application in the tree view, this displays the security classes associated with the selected application.
7. Review data as required.

Modify Security Access Levels for Application Classes

Use this activity to modify the access level for application security classes.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Class Security**.

   The MSE02A - Update Class Security screen displays.

5. Select the Expand icon beside the application to display the security classes associated with the application.
6. Select the required class to modify.

   The ***MSE02C*** - Update Security Classes screen displays.

7. Modify the access level as required in the ***Access Level*** field.

   Note: Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a security class.

8. Select **Submit**.

   The change is saved.

Add a Security Class to a Profile

Use this activity to grant access to an existing class.

Note: This activity does not allow you to create or add a new class to an application.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Class Security**.

   The MSE02A - Update Class Security screen displays.

5. Select **Add Security Class**.

   The Dialog Box - ***Add Security Class*** displays.

6. Enter data in the following fields:

   Class Name

   Access Level

   Note: Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a class.

7. Select **OK**.

   The access level is applied to the class.

Modify Access Levels for Class Methods

Use this activity to modify the access level for class methods.

Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a method or attribute.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Class Security**.

   The MSE02A - Update Class Security screen displays the security applications associated with the selected profile.

5. Select the Expand icon beside the application, this displays the security classes associated with the application.
6. Select the required class.

   The ***MSE02C*** - Update Security Classes screen displays.

   > **Note:** If you have **No Access** to the class, the class methods are protected and cannot be modified.

7. Select the ***Methods*** tab.
8. Perform one of the following steps:
   a. To set all class methods to the same access level:
      1. Select **Set All Methods**.

         The Dialog Box - ***Set All Methods*** displays.

      2. Select the required access level.
      3. Select **OK**.

         All methods for the selected class are modified.

   b. To set individual class method access levels:
      1. Select the required class method.
      2. Modify the access level as required.
9. Select **Submit**.

   The methods for the selected class are saved.

Modify Access Levels for Class Attributes

Use this activity to modify the access level for attributes.

> Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a method or attribute.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Class Security**.

   The MSE02A - Update Class Security screen displays the security applications associated with the selected profile.

5. Select the Expand icon beside the application, this displays the security classes associated with the application.
6. Select the required class.

   The ***MSE02C*** - Update Security Classes screen displays.

7. Select the ***Attributes*** tab.

   > **Note:** If you have **No Access** to the class, the class attributes are protected and cannot be modified.

8. Perform one of the following steps:
   a. To set all class attributes to the same access level:
      1. Select **Set All Attributes**.

         The Dialog Box - ***Set All Attributes*** displays.

      2. Select the required access level.
      3. Select **OK**.

         All attributes for the selected class are modified.

   b. To set individual class attribute access levels:
      1. Select the required class attribute.
      2. Modify the access level as required.
9. Select **Submit**.

   The methods for the selected class are saved.

Apply Access Levels to Reference Codes

Use this activity to apply access levels to a reference code entity.

> **Note:** Only reference codes associated with an Ellipse EAM application display in the summary grid.

MSE02R can be accessed from the following screens by selecting the **Reference Codes Security** button:

- ***MSE020*** - Update Security
- MSE02A - Update Class Security
- ***MSE02D*** - Update Security Application
- ***MSE02C*** - Update Security Classes

The following activity uses ***MSE020*** - Update Security screen to apply access levels to application reference codes.

Activity Steps

1. Access **MSE020** - Security.

   The ***MSE020*** - Search Security screen displays.

2. Enter the relevant search criteria and select **Search**.

   Security profiles matching the search criteria entered displays in the results grid.

3. Select the required security profile.

   The ***MSE020*** - Security detail screen displays with the profile details.

4. Select **Reference Codes Security**.

   The ***MSE02R*** - Update Security Profile Reference Codes screen displays.

5. Select the appropriate access level for the reference code entity as required.
6. Select **Submit**.

   The access details are applied to the reference codes.

Managing Named User Licences

If your organisation has opted to use the named user licence model, a licence key is provided by ABB Enterprise Software that when installed contains the number of each licence type your organisation has permission to use. Each named user can be nominated to use the following licence types:

- **Full**

  The Full use license enables access to all applications in Ellipse EAM.

- **Limited Use**

  The Limited use licence includes a base set of applications, including an additional set of applications (some application are Review mode only).

- **ESS (Employee Self Service)**

  The ESS use license contains access to a base set of applications.

The Named User Licence process allows you to easily monitor your licence types so that you do not exceed your licence allocation. The monitoring of licence types is provided by the ***MSELIC*** - Licence Management application. This application allows you to:

- Upload the system licence key
- View allocated, used and available licence types
- Set the licence type for one or more users
- Review a list of applications and the minimum licence type using ***MSEALT*** - Review Application Licence Type.

Business Rules

The following business rules govern this process:

- To implement named user licensing you need to install a licence key containing the number of licences for each licence type, this key is provided by ABB Enterprise Software.
- You can opt-out of the named user licence model by requesting a new licence from ABB Enterprise Software that reverts to the original licensing model.
- The number of licences permitted for each licence type is incorporated in the licence key.
- The licence key needs to be installed using ***MSELIC*** - Licence Management.

View User Licence Types

Use this activity to view the number of allocated, used and available licence types. You can also view users and the licence type they have assigned.

Licence types are:

- No Licence
- Full Licence
- Limited Use Licence
- Employee Self Service Licence

On accessing ***MSELIC***, the number of allocated, used and available licences display in the Licence Information.

Activity Steps

To view all users and their assigned licence types:

1. From ***MSELIC*** - Search Licence Management, select **Search**.

   All users and their assigned licence types are returned in the search.

To view only users that match your search criteria:

1. From ***MSELIC*** - Search Licence Management, enter data in any of the following fields:

   Licence Type

   Global Profile

   Position

   Employee

2. Select **Search**.

   Results matching your search criteria display in the grid.

Set a Licence Type for a User

Use this activity to set a licence type for a user or multiple users.

Note: If there are insufficient licences available for the selected licence type an error message is returned.

1. From ***MSELIC*** - Search Licence Management search results, select the check box beside the user.
2. Select the ***Set User Licence Type*** action.
3. In the ***Set User Licence Type*** dialog box, enter data in the following field:

   Licence Type

4. Select **OK**.

   Licence type for the selected user is updated in the results grid.

Upload System Licence Key

Use this activity to install the system licence key. This key is provided when your organisation has opted to use the named licensing model or is moving back to a named licensing model from using a concurrent user licence model.

Note: It is recommended that licence types are set before entering the licence key.

1. From the ***MSELIC*** - Search Licence Management screen, select the ***Upload System Licence*** action.
2. In the ***Upload System Licence*** dialog box, enter the ***licence key*** provided and select **OK**.
3. Select **New Search** to refresh the licensing data.

Review Application Licence Type

Use this activity to review a list of applications and the minimum licence types required for the user to use each application.

Note: ***MSEALT*** - Review Application Licence Type can only be accessed using ***MSELIC*** - Search Licence Management.

1. From the ***MSELIC*** - Search Licence Management screen, select the ***List Application Licence Type*** action.
2. Review applications and their licence types in the ***MSEALT*** - Review Application Licence Type screen.

Maintaining MSO Security

Ellipse EAM security is used to ensure that all users have the correct level of access to all the programs they require.

There are five types of profile available when setting security for programs:

- **Entity Profile**

  This is used to secure data entries to which reference codes may be linked.

- **Function Profile**

  This is used to define the access level required for a particular function.

- **Program Profile**

  This is used to define the access level required to start and use the application. This secures an Ellipse EAM program from unauthorised user access.

  Ellipse EAM now enforces a check to ensure MSOs have a security program profile set up for all MSO programs.

  Where MSOs do not have a security program profile set, one can be set up using ***Create MSO Security Profiles***.

  MSEPRF - User Preferences can be used as an interim solution to set up a default application security property. This property allows MSOs without a security program profile to be used.

  Set up Default Application Security Property using MSEPRF

  1. From MSEPRF - User Preferences
  2. Select **New**.
  3. Enter data in the following fields:

     Property - Enter **default.application.security**

     Value - Enter **9**.

     No other fields require entry.

  4. Select **Submit**.

     Note: A security program profile can be set at a later date for MSO programs that did not have a security program profile previously set.
     Once you have created your MSO security program profiles for all MSOs, you can delete the property **default.application.security** from MSEPRF.

- **Sign On Profile**

  This identifies individual users and are district specific. This profile is allocated to all Ellipse EAM users. The match values for a sign-on profile are entered for each occurrence or are derived from a global profile. If the sign-on profile is linked to a global profile the access rights of the user are derived from the global profile.

  A single user can have different access rights in different districts. To achieve this, the system creates a separate sign-on profile for each district where the operator has access.

- **Global Profile**

  This can be used to define a standard set of access control information for users with common requirements.

Note: **MSO** program security is not related to MSE application security. Program and application security are maintained independently of each other, for example, the user can have access to **MSO005**, but not **MSE005**. Application and program security only share the **Profile Name**, for example the **Global Profile** or **Sign on Name**.
For more information on application security, refer to ***Maintaining Application Security - MSE***.

MSO020 - Security allows you to secure and maintain the following permissions:

- Applications including programs, menus and menu options
    - Reports and batch programs
- MSO reference codes

Note: Before setting access levels for security profiles, it is important to read the information on ***Setting Security Access Levels for Applications, Classes, Methods and Attributes***. This information provides a full description on selecting the appropriate access level for Ellipse EAM applications/programs.

Ellipse EAM security determines if and how a user can execute an application by a profile matching process.

This operates as follows:

- Every Ellipse EAM user is assigned a sign on profile. This can be an individual profile or a global profile. A single user can have different access rights in different districts.
- Each program requiring security is given a program profile. These profiles contain a 250-character numeric string.
- Ellipse EAM compares the user's current profile with the program profile. The first comparison is to see if the user is an administrator, which is identified by the user's profile containing a value of **9** in the first profile position. If the user is not an administrator, Ellipse EAM identifies the next point from the profiles at which a numeric-to-numeric comparison can take place.

Note: This check does not compare blanks to blanks and does not compare blanks to numeric values.

- If the user's profile contains (at the next point of comparison) a numeric that is equal or greater than the value at the same point in the program profile, the user is granted access. If the user's value is less than the value in the program profile, the user is denied access. If the user's value is equal to or greater than the value in the program profile (that is, the user is granted access), the value in the user's profile becomes that user's level of access to that program.

  For example:

  A situation occurs where Ellipse EAM needs to know if a particular user has access to an application. This can be for any number of reasons, for example, Ellipse EAM is working out what menu options to display or the user has made a direct attempt to launch an application.

  Ellipse EAM security compares the user's profile with the program profile.

  The program profile has a value at position 121. The security routine looks at the user's profile in position 121 and compares the two values. If the user has a lower value at position 121, the routine will decide that the user does not have access to the application. If the user has a value at position 121 that is greater than, or equal to, the value at position 121 in the program profile, the user will be allowed to execute that program.

  The screen used for comparing values is ***MSM020C*** – Maintain UserID Profile (Short form) and is accessed through the ***MSM020A*** – Maintain Security Profiles screen.

Creating Profiles

- Before starting to create profiles it is important that you determine how each position in the profile is to be used within your organisation.
- A system administrator should create a sign on profile with **9** in position **1**, and **9** in security access. (Position 001 should be reserved for a System Administrator).

- Once the usage of each profile position is determined, record the profile positions in the PW - Security Profile Position Descriptions Table File. The **PW** table holds the descriptions of the various positions in a security profile. Although Ellipse EAM will work without entering these descriptions, documenting the security profile positions will make administering Ellipse EAM security easier.
- A profile should be created for each program. Make sure that an allowance is made for applications with special security match values.
- An entity profile should be created for each reference code to be secured.
- Determine common user groups such as purchasing officers and maintenance planners and their access requirements and apply to a global profile.
- For each employee position a global profile can be created. A position can be given a profile for all of the incumbents to inherit. Individual incumbents can be assigned their own global profile.

  Note: The Position Management module must be installed.
- Global profiles assigned to sign on profiles are overridden by the global assigned to the user's position. The global assigned to the position is overridden by the global assigned to the incumbency, if one exists.

Other Security

The following programs are subject to their own security:

- **Reference Codes** - Reference code information is subject to its own access control. For example, a user is given access to Maintain Employee information but is restricted from updating Reference information associated with Employee (EMP) data.

  To apply access control over reference codes using program security, an entity type profile is set-up using the ***MSM020A*** - Maintain Security Profile. This is done by creating an **E** type profile for the reference code entity (for example, EMP). Refer to Maintaining Reference Codes.
- **Ellipse EAM Menus** - Refer to ***MSM025B*** - System Menu.
- **Ellipse EAM Tables** - Refer to Secure a Table Type.
- **Reports and Batch Programs** - Security over reports and batch programs operates, and is set-up in the same way as programs.

  Reports and batch programs start either directly from the main menu or from the MSO080 - Reports Request application. In the former situation, access control is achieved by removing the menu option or giving an error when the option is selected. In the latter situation, the report or batch program is removed from the list of available reports displayed by the Reports Request application.
- **Inventory Categories** - If you are using the Category Management function in the Warehouse Management module, inventory categories are subject to their own security. For more information, see Modify Position Attributes and ***Access to Inventory Categories***.

Note: Security for MSE programs is separate to that used for other applications. To maintain security for MSE applications, see ***Maintaining Application Security - MSE***.

Diagram

The ***Maintaining MSO Program Security*** diagram represents the security profile process.

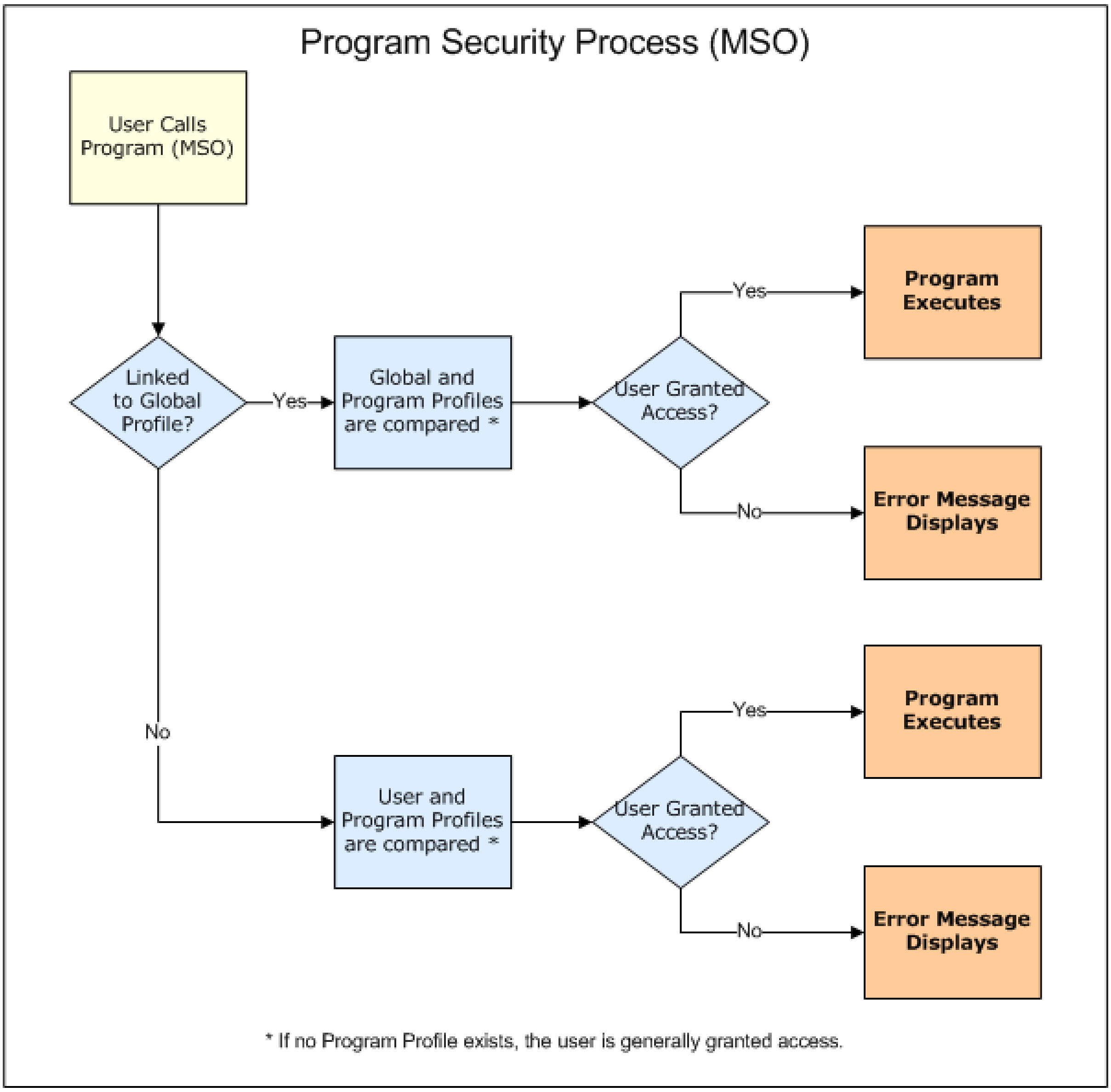
Business Rules

The following business rules govern this process:

- Each program profile should consist of a 9 in position one and a 1 or greater in another profile position. This will ensure that system administrators have access to all secured programs, and that non-administrators are not able to modify the profile.
- Position 001 of all profiles should be reserved for system administration use.
- Each non-administrator's user profile should have a value not equal to 9 in position 001.
- Programs with internal or 'split' security must have profiles, to allow Ellipse EAM to determine the user's level of access.
- Program profiles must consist of the program identity.

  For example, to secure **MSO220**, a program profile must exist with the identifier of **MSO220**. To secure batch and report processes, the profiles contain an eight-character identifier. For example, to secure **MSB900**, we need a profile called **MSB90001**. The last two characters identify the batch/report request number.
- Program profiles need only contain a value in one position other than position 001.
- Programs not required should be secured in the same way as administrator-only programs, that is, with a value of 9 in position 001 only.
- All reports and batch programs including cross-reference rebuilds, and uploads should be secured.
- Access to housekeeping programs should be given to technical and system administrators only. These programs have the following prefixes: MSH, MSI, MSL, MSX and MSV.

Maintaining MSO Program Security - Diagram



* If no Program Profile exists, the user is generally granted access.

Create MSO Security Profiles

Use this activity to create a security profile.

Activity Steps

1. Access **MSO020** Security Profile Maintenance.

   The ***MSM020A*** - Maintain Security Profile screen displays.

2. Select **Create Profile**in the **Option** field.
3. Enter data in the following fields:

   Profile type

   Profile name - The name of the new profile being created.

   Format

   District - This field only displays for multi-district systems, by leaving this field blank the new profile is applied to all districts. By entering a district, the profile will apply to one district only.

4. Select **Submit**.

   The ***MSM020B*** - Create UserID Profile (Long format) or the ***MSM020C*** - Create UserID Profile (Short format) screen displays, depending on the ***Format*** specified above.

5. Enter data into the fields as required.

   To switch between the short format and long format, click **Long Form** or **Short Form** from the tool bar in either the **MSM020B** or **MSM020C** screens.

   For details on comparing profiles, refer to ***Compare Two Profiles***.

6. Select **Submit**.

Modify MSO Security Profiles

Use this activity to modify security profile details. This may be necessary, for example, when needing to change to level of protection assigned to individual programs, or when making changes to the access provided to users.

Activity Steps

1. Access **MSO020** Security Profile Maintenance.

   The ***MSM020A*** - Maintain Security Profile screen displays.

2. Select **Modify Profile** in the **Option** field.
3. Enter data in the following fields:

   Profile type

   Profile name - when modifying a report, enter the full name of the field.

   Format

   District - this field is mandatory when modifying a sign-on profile, and is not required for other options.

4. Select **Submit**.

   The ***MSM020B*** - Create UserID Profile (Long format) or the ***MSM020C*** - Create UserID Profile (Short format) screen displays, depending on the ***Format*** specified above.

5. Modify data to reflect the changes to the profile.

   To switch between the short format and long format, click **Long Form** or **Short Form** from the tool bar in either the **MSM020B** or **MSM020C** screens.

   For details on comparing profiles, refer to ***Compare Two Profiles***.

6. Select **Submit**.

   The changes are saved.

Delete MSO Security Profiles

Use this activity to delete security profiles when they are no longer required.

Any type of profile can be deleted, including global profiles. Deleting a global profile invalidates any sign-on profiles attached to it. The system will display an error message '**Profiles using this profile must be changed**', but this does not prevent the deletion.

Depending if the Position Management module is installed, the deletion of a global profile with attached sign on profiles may result in users and positions and incumbents not having access to job-critical programs.

Activity Steps

1. Access **MSO020** Security Profile Maintenance.

   The ***MSM020A*** - Maintain Security Profile screen displays.

2. Select **Delete Profile**in the **Option** field.
3. Enter data in the following field:

   Profile type

   Profile Name

   Format

   District - When deleting sign on type profiles, if you leave the **District** field blank, the profile is deleted from all districts.

4. Select **Submit**.

   A message displays, confirming the deletion.

5. Select **Yes**.

   If the user deleting the profile is an administrator, Ellipse EAM deletes the profile. If the user is not an administrator, Ellipse EAM requests the password of the profile being deleted.

Review MSO Security Profiles

Use this activity to review security profile details for any profile type.

Activity Steps

1. Access **MSO020** Security Profile Maintenance.

   The ***MSM020A*** - Maintain Security Profile screen displays.

2. Select **Review Profile** in the **Option** field.
3. Enter data in the following fields:

   Profile type

   Profile Name

   Format

   District

4. Select **Submit**.

   Depending on the format selected either the ***MSM020C*** - Review UserID Profile (Short format) screen or the ***MSM020B*** - Review UserID Profile (Long format) screen displays.

5. Review security profile details as required.

Compare Two Profiles

Use this activity to compare two profiles. For example, compare a sign-on profile with a program profile in order to determine if the sign-on has access to the program.

Note: To compare profiles, select the **Short form** display in the ***Format*** field.

Activity Steps

1. Access **MSO020** Security Profile Maintenance.

   The ***MSM020A*** - Maintain Security Profile screen displays.

2. Select **Review Profile** in the **Option** field.
3. Enter data in the following fields:

   Profile type

   Profile Name

   Format

   District

4. Select **Submit**.

   The ***MSM020C*** - Review UserID Profile screen displays.

5. Click the ***Access*** tab.
6. Enter data in the following field:

   Type

   Name

   District

7. Select **Submit**.

   The results of the comparison display.

MSE Security Specifics

The Class Methods below use the security access level and standard security profile procedures to control the functions of the application.

Class Name	Class Method	Access Level	Level Description
Diary	Fetch	0	No Access
	Fetch	4	Current User Only
	Fetch	9	Full Access
Diary	Retrieve	0	No Access
	Retrieve	4	Current User Only
	Retrieve	9	Full Access
Document	Fetch	0	No Access
	Fetch	4	District Based
	Fetch	9	Full Access
Document	Retrieve	0	No Access
	Retrieve	4	District Based
	Retrieve	9	Full Access
Employee	Fetch	0	No Access
	Fetch	1	Self Only
	Fetch	2	Self and Access Based on Position
	Fetch	4	Access Based on Position
	Fetch	9	Full Access
Employee	Retrieve	0	No Access

	Retrieve	1	Self Only
	Retrieve	2	Self and Access Based on Position
	Retrieve	4	Access Based on Position
	Retrieve	9	Full Access
Employee	RetrieveEmpForReqmts	0	No Access
	RetrieveEmpForReqmts	1	Self Only
	RetrieveEmpForReqmts	2	Self and Access Based on Position
	RetrieveEmpForReqmts	4	Access Based on Position
	RetrieveEmpForReqmts	9	Full Access
Employee	RetrieveViaRefCodes	0	No Access
	RetrieveViaRefCodes	1	Self Only
	RetrieveViaRefCodes	2	Self and Access Based on Position
	RetrieveViaRefCodes	4	Access Based on Position
	RetrieveViaRefCodes	9	Full Access
Equipment	Create	0	No Access
	Create	1	Create Access in Own District
	Create	2	Auto Generate Equipment
	Create	9	Full Access
Equipment	Delete	0	No Access
	Delete	1	Delete in Own District
	Delete	9	Full Access
Equipment	Modify	0	No Access
	Modify	1	Modify in Own District
	Modify	9	Full Access
NotificationMsg	Fetch	0	No Access
	Fetch	4	Current User Only
	Fetch	9	Full Access
NotificationMsg	Retrieve	0	No Access
	Retrieve	4	Current User Only
	Retrieve	9	Full Access

PersonnelEmp	Fetch	0	No Access
	Fetch	1	Self Only
	Fetch	2	Self Only Based on Position
	Fetch	4	Access Based on Position
	Fetch	9	Full Access
PersonnelEmp	Retrieve	0	No Access
	Retrieve	1	Self Only
	Retrieve	2	Self Only Based on Position
	Retrieve	4	Access Based on Position
	Retrieve	9	Full Access
Project	Fetch	0	No Access
	Fetch	4	Date in Service - In
	Fetch	9	Full Access
Project	Modify	0	No Access
	Modify	4	Date in Service - In
	Modify	9	Full Access
Security	Create	0	No Access
	Create	4	Create up to Own Level
	Create	9	Full Access
Security	Fetch	0	No Access
	Fetch	4	Access up to Own Level
	Fetch	9	Full Access
Security	Modify	0	No Access
	Modify	4	Modify up to Own Level
	Modify	9	Full Access
Security	Retrieve	0	No Access
	Retrieve	4	Access up to Own Level
	Retrieve	9	Full Access
StdClause	Modify	0	No Access
	Modify	1	Create New Version
	Modify	9	Full Access

SupplierBusiness	Fetch	0	No Access
SupplierBusiness	Fetch	1	Normal Access
SupplierBusiness	Fetch	3	Normal and Tax Information
SupplierBusiness	Fetch	9	Full Access
WorkOrder	Create	0	No Access
	Create	1	System Generate Work
	Create	9	Full Access
WorkOrder	Fetch	0	No Access
	Fetch	4	Date in Service
	Fetch	9	Full Access

MSO Security Specifics

The following programs cannot be given security profiles as this would inhibit basic Ellipse EAM functionality:

- **MSO002** - District Selection
- **MSOERM** - Error Diagnostic

The following programs should not be given security profiles, although it is possible to create security profiles for these programs:

- **MSO110** - Part Number Search
- **MSO112** - Manufacturers Search
- **MSO115** - Item Name Code Search
- **MSO116** - Group Class Search
- **MSO120** - Colloquial Name Search

These programs use the security access level and standard security profile procedures to control the functions of the program:

- **MSO020** - User ID and Password Maintenance:
    - If match value = 0, access is prohibited.
    - If match value > 0, access is permitted subject to the controls placed by the Security Access field.
    - A security access of 0 or space allows review of profiles only.
    - A security access of 1, 2, 3 or 4 allows modification of user IDs and global profiles up to the user's own level.
    - A security access of 5, 6, 7 or 8 allows modification and/or creation of user IDs and/or global profiles up to the user's own level. It also enables deletion of user IDs, providing the correct password is known.
    - Security Access 9 has no restrictions. The original intent was that this security access was accorded to a system administration role and any security access < 9 would serve to delegate security maintenance to **others**. However for the **others** with security access < 9 modification of existing profiles excludes password maintenance. For creating user profiles the ability to enter a password for that user ID was provided in the case where the **bypass welcome screen** feature is not used, and therefore the password must be entered for creating user IDs. A security access of 9 allows a blank password to be specified for a user.
- **MSO010** - Table File Maintenance:
    - If match value > 0, access to the program is permitted, but Ellipse EAM-specific table files cannot be amended.
    - A security access of 9 and a match value > 0 allows amendments to all table files, including Ellipse EAM-specific files.

Programs within the Human Resources stream can relate to confidential employee information. Therefore, additional security is required. The security match values nominated below apply. In addition, the system restrict access to employee information based on the access rule and value nominated for the position chosen by the user at the time of signing on to the system. This allows users to be restricted to access to employee details based on their position, work group, and location parameters.

Alternatively, where access to all employees is required, a security match value greater than 4 (in the user profile) overrides any position-based security restrictions. Typically, this applies to users who are part of a central Human Resources or Payroll department, and who have global access to employee details.

Programs for reference code review and maintenance use their own security profile to determine access to employees, in the case where a reference code is defined as an employee.

The following programs can update reference codes:

- **MSO071** - Maintain Reference Codes
- **MSO072** - Review Reference Codes
- **MSO073** - Search for Entity by Reference Codes
- **MSO074** - Review Reference Code Parameters
- **MSO076** - Review Entry Values for an Entity
- **MSO104** - Catalogue Bulk Change
- **MSO16A** - Global RD Bulk Change
- **MSO177** - Inventory Bulk Change

Suspend Function

The **Suspend** function profile allows users to compile outstanding transactions for a district or warehouse.

The following programs have security match values to control levels of functionality within a program:

Function	Value	Capabilities
Suspend	1	Review only access to the suspended district
Suspend	>1	Full access within the suspended district

MSO001 to MSO099

Program	Value	Function
MSO001 Maintain System Control Files	0	No access allowed
	1	The user only has access to districts where they have a profile. • Maintain Warehouse Control Information

	2	The user only has access to districts where they have a profile. • Modify District HR Details
	3	The user only has access to districts where they have a profile. • Modify Program Printer Allocations
	4	The user only has access to those districts where they have a profile. • Modify Bank Accounts for a District • Modify Account Code for a District • Modify Accounting Periods for a District • Modify Current Period Information
	5 or 6	The user only has access to districts where they have a profile. • Modify District Controls • Maintain Warehouse Control Information • Modify District HR Details • Modify Bank Accounts for a District • Modify Account Code for a District • Modify Accounting Periods for a District • Modify Current Period Information • Modify District Address Details • Modify Program Printer Allocations • Modify Site Control Information
	7	Access will be for all districts. Options accessible with a match value of 7 will be: • Suspend District • Reactivate District • Close District

	8	Access will be for all districts. Options accessible with a match value 8: • Modify District Controls • Maintain Warehouse Control Information • Modify District HR Details • Modify Bank Accounts for a District • Modify Account Code for a District • Modify Accounting Periods for a District • Modify Current Period Information • Modify District Address Details • Modify Program Printer Allocations • Modify Site Control Information • Suspend District • Reactivate District • Close District
	9	Allows access to all options provided by **MSO001**
MSO00R Review System Control File	**Note:** The following programs must be secured with MSO00R for the security levels to work: MSO00A - Maintain Modules Installed MSO00B - System Control File Maintenance MSO00C - System Control File Maintenance MSO00D - System Control Journal Holding Maintenance MSO00E - System Control File Maintenance (Cont'd) MSO00G - Maintain Warehouse Control Information MSO00H - Modify District Address Details MSO00J - Maintain District Header Details	
	0	• No access allowed

	1	The user only has access to districts where they have a profile. • Review Warehouse Control Information
	2	The user only has access to districts where they have a profile. • Review District HR Details
	3	The user only has access to districts where they have a profile. • Review Program Printer Allocations
	4	The user only has access to districts where they have a profile. • Review Bank Accounts for a District • Review Account Code for a District • Review Accounting Periods for a District • Review Current Period Information
	5	The user only has access to districts where they have a profile. • Review District Controls • Review Warehouse Control Information • Review District HR Details • Review Bank Accounts for a District • Review Account Code for a District • Review Accounting Periods for a District • Review Current Period Information • Review District Address Details • Review Program Printer Allocations • Review Site Control Information
MSO011 Table File Review	<5	Associated Values hidden for tables recorded on XSAV table
	>4	Full access
MSO014 Maintain Supply Customers	>0	Create Supply Customers
	>1	Maintain Supply Customers
	>2	Create/Maintain Entitlement Items
	>3	Suspend/Close Customers
	>4	Un-suspend/Re-Open Customers
	>5	Delete Supply Customers
MSO018	>1	No restrictions.

Maintain Tax Code Definitions	<2	No access.
MSO01C Template Route Maintenance	>1	No restrictions.
	<2	Deletion not allowed.
MSO040 General Diary Entry and Maintenance	<9	Access to current user only, and unrestricted diary types.
	9	No restrictions.
MSO042 Employee Diary Maintenance	<9	Access to current user only, and unrestricted diary types.
	9	No restrictions.
MSO043 Personal Diary Maintenance	<9	Access to current user only, and unrestricted diary types.
	9	No restrictions.
MSO052 Maintain Index Types and Information	1	Cannot delete information and an index.
	>1	No restrictions.
MSO080 Request Batch Reports	1	Request single copy, single printer.
	2	Request multiple copies, single printer.
	3	Request multiple copies, multiple printers.
	4	Request and/or submit multiple copies, multiple printers.
	5	Request multiple copies, multiple printers. Submit cyclical requests.
	9	Allows immediate Batch submission.
MSO088 Maintain Group Report Requests	1	Request single copy, single printer.
	2	Request multiple copies, single printer.
	3	Request multiple copies, multiple printers.
	4	Request and/or submit multiple copies, multiple printers.
	5	Request multiple copies, multiple printers. Submit cyclical requests.
	>5	No restrictions.
MSO096 Maintain Standard Text	9	Option 6 (Modify the Welcome Message) is available.

MSO100 to MSO199

Program	Value	Function
MSO127 Maintain Standard Clause Text	1	Only the current Clause Version can be assigned.
	>1	Selected Clause Version can be assigned.
MSO140 Normal Issue Requisition	1	Create issue requisitions.
	2	Create issue requisitions and Protected Requisitions.
	3	Create issue requisitions and cost to other districts.
	4	Create issue requisitions and override the category.
	5	Create issue requisitions, protected requisitions and cost to other districts.
	6	Create issue requisitions, protected requisitions and override the category.
	7	Create issue requisitions, cost to other districts and override the category.
	>7	Create issue requisitions, protected requisitions, cost to other districts and override the category. Also nominate any Supply Customer
	<8	Must have access to nominated Supply Customer
MSO14A Enter Single Requisition Item Details	1	Create RO Stores.
	2	Create and Finalise RO Stores.
	3	Create and Finalise RO Stores to PO (preferred Supplier).
	4	Create and Finalise RO Stores to PO (any active Supplier).
	>4	No Restriction.
MSO14B Enter Requisition Item Details	1	Create RO Stores.
	2	Create and Finalise RO Stores.
	3	Create and Finalise RO Stores to PO (preferred Supplier).
	4	Create and Finalise RO Stores to PO (any active Supplier).
	>4	No Restriction.
MSO14E	1	Create store sales requisitions (must also have access to

Store Sales Requisitions		**MSO573**).
	>1	Create store sales requisitions override category.
MSO14F Enter APL Requisition Details	1	Create RO Stores.
	2	Create and Finalise RO Stores.
	3	Create and Finalise RO Stores to PO (preferred Supplier).
	4	Create and Finalise RO Stores to PO (any active Supplier).
	>4	No Restriction.
MSO14L Loan Requisitions	1	Create loan requisitions.
	>1	Create loan requisitions and override category.
	>7	Nominate any Supply Customer for Requisitioning
	<8	Must have access to nominated Supply Customer
MSO14M Recall Requisitions	1	Create recall requisitions.
	2	Create recall requisitions and override category.
	3	Create recall requisitions and cost to other districts.
	>3	Create recall requisitions, override category and cost to other districts.
	>7	Nominate any Supply Customer for Requisitioning
	<8	Must have access to nominated Supply Customer
MSO14P Purchase Requisitions	1	Access only from other requisition programs
	>1	Access directly from menu.
	>7	Nominate any Supply Customer for Requisitioning
	<8	Must have access to nominated Supply Customer
MSO14R Credit/Return Requisitions	1	Create credit/return requisitions.
	2	Create credit requisitions and override category.
	3	Create credit requisitions and cost to other districts.
	>3	Create credit requisitions, override category and cost to other districts.
	>7	Nominate any Supply Customer for Requisitioning

	<8	Must have access to nominated Supply Customer
MSO14S Short Form Requisition	1	Create issue requisitions.
	2	Create issue requisitions and override category.
	3	Create issue requisitions and cost to other districts.
	>3	Create issue requisitions, override category and cost to other districts.
	>7	Nominate any Supply Customer for Requisitioning
	<8	Must have access to nominated Supply Customer
MSO14T Rotation Requisitions	1	Create rotation requisitions.
	2	Create rotation requisitions and override category values.
	3	Create rotation requisitions and cost to other districts.
	>3	Create rotation requisitions, override categories and cost to other districts.
	>7	Nominate any Supply Customer for Requisitioning
	<8	Must have access to nominated Supply Customer
MSO143 Manual Requisitions	<6	Create manual requisitions.
	6	Create manual requisitions and override category.
	7	Create manual requisitions and cost to other districts.
	<7	Create manual requisitions, override category and cost to other districts.
	>7	Nominate any Supply Customer for Requisitioning
	<8	Must have access to nominated Supply Customer
MSO144 Maintain Requisitions	1	Modify issue requisitions with same created by user as signed on user.
	2	Amend warehouse requisitions not in warehouse service time (must also have access to the appropriate requisition header program).
	3	Amend purchase requisitions only (must also have access to **MSO14P**).
	4	Amend warehouse requisitions not in warehouse service time and purchase requisitions

	5	Amend warehouse requisitions within warehouse service time (including preposted quantities).
	>5	Amend warehouse requisitions within warehouse service time and purchase requisitions.
MSO145 Reactivate Requisitions	1	Reactivate all requisition items for this Stock Code.
	2	Reactivate up to total available quantity.
	>2	Allowed to nominate the requisition item and quantity to be reactivated. The requisitions are listed in date required sequence. The quantity outstanding is defaulted into the reactivate column up to the total available quantity.
MSO146 Create/Finalise Warehouse Transfers	>5	Can override Inventory Category.
	<6	Cannot override Inventory Category.
MSO15F Trip Maintenance or Review	>1	Update access to Trip information.
MSO15M Container Selection/Update	>1	Update access to Move and Manifest Containers.
MSO15N Container Maintenance	>5	Delete Containers.
MSO15P Returns to Supplier	>1	Provide a return price for item.
MSO15Q Waybill Selection/Update	>1	Update access to Move, Containers and Manifest Waybills.
MSO16B Concession List Maintenance	>3	Delete Concession Categories.
MSO16D Concession List/District	>3	Delete Concession Lists for a District.
MSO16E Customs Document Maintenance	>1	Modify existing Export Invoices/Inspection Report Items.
MSO16F Customs Document Items Maintenance	1	Modify Reference field only.
	>1	No restrictions.

MSO170 Maintain Inventory Control	<4	No access to Sales Tax Code/Rate.
MSO177 Create Inventory Bulk Change Selection	>8	Access to change all districts.
MSO179 Stores Algorithms	>1	Allows update of stock item with changed values.
MSO17E Update Inventory Price	>1	Access to amend inventory price/value.
MSO17G Maintain Category Costing Details	1	Access to review only.
	>1	No restrictions.
MSO185 Maintain Planned Holdings	>1	Allows update to all districts.

MSO200 to MSO299

Program	Value	Function
MSO200 Maintain Supplier Information	1	Create potential suppliers.
	2	Create normal suppliers and supplier districts.
	>3	External created/internally managed supplier and district suppliers are subject to field restrictions as configured on MSM051A - Maintain Screen Defaults
MSO201 Review Supplier Information	1	Restrict the display or entry of data into the Bank Account, Bank Account Name, Branch Code and Account Code, **WH** Tax Code, Government Identification Number, Exemption fields and Payment Method of **E** when creating or modifying Supplier Business Information.
	2	Restrict the display of the Bank Account, Bank Account Name, Branch Code and Account Code fields on the Supplier Business Information screen.
	>2	No field restrictions.
MSO20D Maintain Supplier Business Information	1	Restrict the display or entry of data into the Bank Account, Bank Account Name, Branch Code and Account Code, **WH** Tax Code, Government Identification Number, Exemption fields and Payment Method of **E** when creating or modifying Supplier Business Information.
	2	Restrict the display or entry of Bank Account, Bank Account Name, Branch Code, Account Code and Payment Method of **E** when creating or modifying Supplier Business Information.
	>2	No field restrictions.
MSO210 Maintain Purchasing Information	1	Create, modify or delete Stock Code or supplier information.
	2	Modify district purchasing information and preferred supplier.
	>2	No restrictions.
MSO212 Maintain Commentary	1	Access only from other programs as required.
	2	Access directly from menu and able to access district item comments only.
	>2	Access directly from menu and able to access global and district item comments.
MSO213	1	Review of stock code information only

Review / Maintain Commentary	>1	Create, Review, Update and Delete of stock code information.
MSO220 Maintain Purchase Order	1	Maintenance limited to orders for that purchasing officer or team.
	2	
	4	
MSO22C Maintain Purchase Order Item	2	If accessed from Invoice Entry program (**MSO26C**), can only modify Sales Tax Code.
MSO23B Modify Requisition Header	1	Access only to raising purchase requisitions.
	>7	Access to any Supply Customer.
	<8	Must have access to entered Supply Customer.
MSO23C Modify/Process Requisition Items	1	Access only to raising purchase requisitions.
	>4	No restrictions.
	<5	Cannot consolidate against a completed order.
MSO23D Maintain/Process Purchase Requisition	1	Access only to raising purchase requisitions.
	>4	No restrictions.
	<5	Cannot consolidate against a completed order.
MSO23E Create/Modify Purchase Requisition	1	Access only to raising purchase requisitions.
	<4	No access to Global Purchase Orders
	>4	No restrictions.
	<5	Cannot consolidate against a completed order.
MSO240 Inventory Purchasing	1	Stores orders only.
	2	Stores and transfers only.
	3	Purchase and transfers, preferred Supplier only.
	4	Purchase and transfers, any active Supplier.
	>4	No restrictions.
MSO24B Create/Modify Recommended Order - Stores	1	Stores orders only.
	2	Stores and transfers only.
	>2	Add/Modify Purchase Order Clauses.
	3	No access.

	<4	No access to Global Purchase Orders.
	>3	No restrictions.
MSO24C Create or Modify a Recommended Order	1	No access.
	>1	Add/Modify Purchase Order Clauses.
	2	Stores and transfers only.
	3	Transfer, Buy, Proforma and Direct Delivery Recommended Orders.
	<4	Cannot create Recommended Orders and No access to Global Purchase Orders.
	>3	No restrictions.
MSO260 Load Invoices	1	Load invoice only (not approved online).
	>1	No restrictions.
MSO275 Enter Manual Cheques	1	Cannot select invoices or print cheques online.
	2	Cannot print cheques online.
	>2	No restrictions.
MSO27A Enter Manual Payments and Sundries	>1	One off payments allowed.
MSO281 Review Cheque Run Information	<2	No access.
MSO291 Review EDI Messages	<2	Update action not available
	>2	Update action available
MSO292 Review EDI Message Items	<2	Update action not available
	>2	Update action available
MSO293 Review EDI Message Item Details	<2	Update action not available
	>2	Update action available

MSO300 to MSO499

Program	Value	Function
MSE340 Maintain Condition Monitoring Information	1	Delete option not available.
	>1	No restrictions.
MSO353 Indent Maintenance	>1	Enter recommended payment. Enter actual payment.
MSO360 Maintain Disposal/Survey Details	1	Create or maintain disposal or survey items.
	>1	Allow delete of disposal or survey items.
	>2	Allow sentencing of survey item.
	>3	Allow maintenance of costing allocations.
MSO363 Maintain Disposal Selection Information	1	Update stock class or category, Generate Transfers is not available.
	>1	No restrictions
MSO382 Record Tenderers and Replies	1	Modify and delete replies are not available.
	>1	No restrictions.
MSO400 Equipment Operating Statistics Maintenance	<5	Cannot enter shift values.
	5 & >5	No restrictions.
MSO410 Availability Statistics Maintenance	1	Modify actuals not available.
	>1	No restrictions.
MSO420 Downtime Statistics Maintenance	1,2	Warnings for shift start/stop time overlapping.
	>2	No warnings for overlaps.
MSO440 Production Statistics Maintenance	1	Maintenance to actuals not allowed.
	>1	No restrictions.
MSO470 Lost Production Statistics Maintenance	1,2	Warnings for shift start/stop time overlapping.
	>2	No warnings for overlaps.

MSO500 to MSO599

Program	Value	Function
MSO500 Maintain Customer Information	>2	Modification of credit limit allowed when credit limit is greater than zero.
MSO50D Customer Diary Entries	<9	Access to current user only and unrestricted diary types.
	9	No restrictions.
MSO51G Maintain Event Investigation History	>1	Create
	>2	Delete
MSO51K Event Environmental Impact	>1	Create/Edit
	>2	Delete
MSO514 Maintain Incident Injuries	>2	Modification/Deletion of Incident Injuries is allowed.
MSO520 Maintain Employee Medical Details	1	Review Access.
	>2	Modification and deletion of employee medical details allowed.
MSO521 Maintain Rehabilitation Details	>0	Review Access.
	>1	Creation and Modification of Rehabilitation Details.
	>2	Deletion of Rehabilitation Details.
MSO522 Maintain Medical Test Details	1	Review Access.
	>1	Creation and Modification of Medical Test Details.
	>2	Deletion of Medical Test Details.
MSO526 Maintain Position/Location JSPs	2 & >2	Deletion of position/location JSP is allowed.
MSO530 Maintain State Workers Compensation Controls	>2	Modification/Deletion of State Workers Compensation Controls is allowed.
MSO531 Maintain Workers Compensation Location Codes	>2	Modification/Deletion of Workers Compensation Location Codes is allowed.

MSO532 Maintain Absence Authority Type Codes	>2	Modification/Deletion of Absence Authority Type Codes is allowed.
MSO533 Maintain Payment Types	>2	Modification/Deletion of Payment Types is allowed.
MSO534 Maintain Recovery Types	>2	Modification/Deletion of Recovery Types is allowed.
MSO535 Maintain Weekly Payments	>2	Modification/Deletion of Weekly Payment Codes is allowed.
MSO536 Maintain Claim General Details	>2	Modification/Deletion of Claim General Details is allowed.
MSO537 Maintain Workers Compensation Claims	>2	Modification/Deletion of Workers Compensation Claims is allowed.
MSO538 Maintain Claim Estimates	>2	Modification/Deletion of Claim Estimates is allowed.
MSO53A Maintain Claim Absence Authority Details	>2	Modification/Deletion of Claim Absences is allowed.
	<3	Error when Threshold limit exceeded for period.
	>3	Warning when threshold limit exceeded for period.
MSO53C Maintain Workers Compensation Statistics	>2	Modification/Deletion of Workers Compensation Statistics is allowed.
MSO53P Maintain Claim Payments	>2	Modification of Claim Payments is allowed.
MSO53R Maintain Claim Recoveries	>2	Modification of Claim Recoveries is allowed.
MSO53S Claim Selections	>2	Creation of Claims is allowed.
MSO550 Event Corrective Actions	>0-3	Review own.
	>3	Review all.
	>2-4	Modify own.
	>4	Modify all.

	>5	Modify completion all.
	>3	Delete own.
	>6	Delete all.
MSO56F Create Work Order/Project Invoices	>1	Invoice Type field is mandatory if the credit term is not cash only.
MSO56H Maintain Credit Notes	1	Create Credit Note.
	2	Create/Modify Credit Note.
	>2	Create/Modify Credit Note for CASH Customer.
	3	Create/Modify/Cancel Credit Note.
MSO56I Maintain Write Offs	1	Create Write Off.
	2	Create/Modify Write Off.
	3	Create/Modify/Cancel Write Off.
MSO560 Maintain Invoices	0	No access to program.
	1	Creation of Cash Invoices permitted.
	2	Creation and update of Cash Invoices permitted only.
	3	Creation of all Invoice types permitted.
	4	Creation and update of all invoice types permitted.
	5	Creation, update and cancellation of all invoice types permitted.
MSO570 Process Cash Receipts or Refunds	>1	Process cash refunds.
MSO573 Process Stores Sales	>2	Warning only if customer breaks credit limit, otherwise an error.
	>1	Creation of cash invoices allowed. (Must also have access to **MSO14E**.)
MSO580 Document Maintenance	1	Deletions not allowed.
	>1	No restrictions.

MSO600 to MSO799

Program	Value	Function
MSO600 Equipment Register Maintenance	1	Create and modify in own district.
	2	As for 1, plus Delete in own district.
	3	As for 1 and 2 plus Create and Modify in other districts.
	4	As for 1, 2, and 3 plus Delete in other districts.
MSO603 Maintain Equipment List	<9	Must be the owner to modify or delete the Equipment List details.
	9	No restrictions override the owner.
MSO693 Standard Job Task Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO720 Maintain Work Group	1	Create, Maintain and Delete are not available.
	2	Create and Maintain are available.
	>2	Create, Maintain and Delete are available.
MSO722 Maintain Work Group Auto Requisition Details	8,9	The Category field can be modified.
	5,9	The Protected Requisitions field can be modified.
MSO723 Maintain Work Group Employee/Equipment Details	>2	Deletion is available. **Note:** Additional security using the AH - Action Code Help Table codes may be applied.
MSO76P Review Employee Personnel Details	>1	User-definable fields are displayed, along with Legal Rep, Veteran Status & Handicapped indicator.
	>2	The following fields are displayed, Nationality, Birth Country, Citizenship & Ethnicity.
MSO775 Maintain Training Program	1	Access by Training Program owners only.
	>1	Deletion of Training Program available.
MSO777 Maintain Employee Training Plan	1 & 2	Access to Employee Training Plan.
	3	Access to Session Results.
	4	Access to Attending Training History.
	>4	No restrictions.

MSO785 Maintain Employee Salary Benefits	>2	Deletion is allowed.
MSO786 Maintain Benefit Transactions	>2	Deletion is allowed.

MSO800 to MSO899

Program	Value	Function
MSO801 Maintain Earnings Code	>3	Create/Modify/Delete is allowed.
MSO803 Maintain Deduction Code	>3	Create/Modify/Delete is allowed.
MSO805 Maintain Statutory Holiday Table	>3	Create/Modify/Delete is allowed.
MSO807 Maintain Pay Group Processing Schedules	>3	Modify/Delete is allowed.
MSO808 Maintain Pay Group Details	>3	Create a Pay Group, Modify a Pay Group's General details, Modify a Pay Group's Banking details and Delete a Pay Group are available.
	9	The Update in Progress, Preview Run Number and Manual Run Number fields can be modified.
MSO80P Maintain Primary Reporting Code	>3	Create/Modify/Delete is allowed.
MSO811 Maintain Non-Employee Details	>2	Deletion of a Non-employee is available.
	>3	User-definable fields are available.
MSO816 Employee Tax Type Details	>3	Access to item views available.
MSO817 List Payroll Process	1	Access to Details of self only.
MSO818 Employee Payment Details	>2	Modification is allowed.
MSO819 Maintain Leave Accrual Codes	>3	Create/Modify/Delete is allowed.

MSO820 Maintain Employee Payroll Details	>2	Update of the following fields is available: - Paid in Advance to Date - Leave Start Date - Deduction Periods Taken - Deductions Taken from Period - Deductions Taken to Period - Start of Leave Bank - End of Leave Bank - Average RDO Bank
MSO824 Maintain Employee Tax Details	>3	The Tax File Number field is displayed and can be maintained.
MSO82T Review Employee Tax Details	>3	The Tax File Number field is displayed.
MSO838 Maintain Employee Group Certificate Details	>3	Maintain and Create access is allowed.
MSO83G Review Employee Preview/Payment Details	1	Access to Details of self only.
MSO83H Review Employee Highlight Messages	1	Access to Details of self only.
MSO845 Maintain Employee Superannuation Details	>2	Create/Modify/Delete is allowed.
MSO870 Maintain Positions	9	Security Details available.
MSO881 Review Employee Leave Summary	1	Display of Leave Type's governed by the Payslip Leave Parameters. Also the Value of Leave is not displayed.
MSO883 Review Employee Leave Details	1	Display of Leave Type's governed by the Payslip Leave Parameters.

MSO89C Review Employee Roster Transactions	>3	Display of rate amount allowed.
MSO89D Maintain Work Group Roster Transactions	>2	Allowed to exceed leave entitlement.
	>3	Allowed to cost an already costed transaction to allow amendment.
MSO89F Create Employee Exception Transactions	>2	Allowed to exceed leave entitlement.
	>3	Display of rate amount allowed.
MSO89G Review Employee Clocked Times	>4	Display of rate amount allowed.
MSO8C5 Maintain Award Service Based Redundancy Rules	>3	Create/Modify/Delete is allowed.
MSO8LT Maintain Leave Payout Exit Rules	>3	Create/Modify/Delete is allowed.
MSO8MP Maintain Miscellaneous Payment Exit Rules	>3	Create/Modify/Delete is allowed.
MSO8PA Maintain Position Details	>3	Display of Salary details is allowed.
MSO8PB Review Position Details	>3	Display of Salary details is allowed.
MSO8PC Maintain Position Evaluation Details	>3	Display of Salary details is allowed.
MSO8PD Review Position Evaluation Details	>3	Display of Salary details is allowed.
MSO8PI Maintain Plan Identifier Codes	>3	Access to update functions is allowed.
MSO8PO (Called from MSO8PR)	>2	Delete is allowed.

MSO8TD Maintain Employee Exit Deduction Details	>3	Update is allowed.
MSO8TL Modify Employee Leave Payout Details	>3	Leave Details can be maintained for actions B,D.
MSO8TM Maintain Employee Miscellaneous Payment Details	>3	Miscellaneous details can be maintained.
MSO8TN Review Employee Net Exit Details	>3	Update is allowed.
MSO8TP Maintain Employee Payout Exit Details	>3	Update is allowed.

MSO900 to MSO999

Program	Value	Function
MSO900 Short Form Journal Maintenance	1	Cannot specify single currency journals.
	1 or 4	Load journal only, current period only.
	2 or 5	Prior (re-opened) periods allowed, but only in financial years which have not yet been closed.
	3 or 6	Any opened period in any opened (or unopened) financial year. Match values 1, 2 and 3 relate to non-inter-district Match values 4, 5 and 6 are inter-district. Programs **MSO905**, **MSO906** and **MSO907** use **MSO900** security profile for security levels for period posting and inter-district processing.
MSO904 Transaction Account and Cost Correction	1	Cannot correct transaction in period which has month end processing completed.
	>1	No restrictions.
MSO905 Journal Entry Maintenance	1	Can only load Journals. You will have no access to the journal approval facility and you cannot raise journals against system control accounts or fixed asset profile accounts - capital cost and accumulated depreciation.
	2 or 5	You can access the journal approval facility, but cannot raise journals against system control accounts or or fixed asset profile accounts - capital cost and accumulated depreciation.
	3 or 6	You have access to journal approval facility, but can raise journals against system control accounts that are not used for reconciliation or fixed asset profile accounts - capital cost and accumulated depreciation.
	4 or 7	You have access to the journal approval facility and can raise journals against system control accounts that are not used for reconciliation or fixed asset profile accounts - capital cost and accumulated depreciation.
	1, 2, 3, or 5	No access to post journals online.
	6 or 7	You can access post journals online, MSO900, MSO906 and MSO907 use this program profile to control access to approve journals, post to system control accounts that are not used for reconciliation or fixed asset profile accounts - capital cost and accumulated depreciation.and post journals online.
MSO912 Exchange Rate Maintenance	1	Deletions not allowed.
	>1	No restrictions.

MSO920 Cost Centre Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO924 Account Limit Code Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO929 Links Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO930 Expense Element Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO932 Account Code Access List Maintenance	1	Cannot maintain account code access lists. Cannot maintain account code accesses for current user's employee ID or position ID. Can only maintain account code accesses for other employee and position ID's where the user also has current access.
	>1	No restrictions.
MSO936 Account Code Access by Tran Type	1	Cannot maintain accesses for operators own Employee ID or Position.
	>1	No restrictions.
MSO937 Maintain Account Code Access by Account Unit	1	Cannot maintain accesses for operators own Employee ID or Position.
	>1	No restrictions.
MSO93G Maintain Install and Remove Bill of Property Units (BPU)	>1	Permitted to update unitisation details subsequent to setting of the Handover Date.
	>2	Allowed to maintain AFUDC unitisation information. Permitted to update unitisation details subsequent to setting of the Date in Service.
MSO93H Maintain BPU Internal	>1	Permitted to update unitisation details subsequent to setting of the Handover Date.
	>2	Allowed to maintain AFUDC unitisation information. Permitted to update unitisation details subsequent to setting of the Date in Service.
MSO93I Install BPU Line Items -	>1	Permitted to update unitisation details subsequent to setting of the Handover Date.

External	>2	Allowed to maintain AFUDC unitisation information. Permitted to update unitisation details subsequent to setting of the Date in Service.
MSO93L Maintain Miscellaneous BPU	>2	Permitted to access Retire and Salvage options. Permitted to approve BPU for capitalisation.
MSO93M Maintain IBPU Line - Detail	>1	Permitted to update unitisation details subsequent to setting of the Handover Date.
	>2	Permitted to update unitisation details subsequent to setting of the Date in Service.
MSO93N Maintain RBPU Lines	>1	Permitted to update unitisation details subsequent to setting of the Handover Date.
	>2	Permitted to update unitisation details subsequent to setting of the Date in Service.
MSO93P Maintain RBPU Line - Detail	>1	Permitted to update unitisation details subsequent to setting of the Handover Date.
	>2	Permitted to update unitisation details subsequent to setting of the Date in Service.
MSO940 GL Code Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO971 Maintain Budget Information	9	Allowed to maintain General Ledger Accounts.
MSO972 Create Budget Information	9	Allowed to maintain General Ledger Accounts.
MSO973 Create Report Request for **MSB973** (Copying Budget Information)	9	Allowed to maintain General Ledger Accounts.
MSO980 GL Statistics Maintenance	1	Deletions not allowed.
	>1	No restrictions.
MSO9E1 Entity Budget Management	1 - 2	Restrict deletion of entity budget items. Restrict creation/modification of entity budget headers. Restrict copy/delete entity budget.
	3	Restrict creation/modification of entity budget headers. Restrict copy/delete entity budget.
	4	Restrict delete budget.

	>4	No restrictions.

Security - Reports

Reports

MSB021 - Create Object Security - Systems Admin

This batch process can be used to:

- Create a new administrator user, with access to all Ellipse EAM MSE objects.
- Update security data files for all new MSE applications.
- Produce a report displaying the records inserted into each data file, including a summary of the number of records inserted into each data file.

Additional Information

Parameters Enter the following information in the Report Request Selection screen for this report:

User ID This field is mandatory.

Enter the client's system administrator profile. This system profile should be the profile that has access to all of the programs within the system. If no profiles currently exist, a new profile will be created.

District Code This field is mandatory.

Enter a valid district code for the client's system. The program will use this field in conjunction with the User ID field to find if a profile exists within the system.

Default Menu This field is optional if the profile supplied is currently available on the system. Otherwise, if the profile has to be created then this field is mandatory. This will default to **GM** if this installation is a brand new system.

Enter the name of a valid default menu for the system.

Employee ID This field is optional if the profile supplied is currently available on the system. Otherwise, if the profile has to be created, then this field is mandatory.

Enter a valid employee ID.

MSR01A - Programs Protected at Selected Points Report

The **MSR01A** - Programs Protected at Selected Points report displays the MSM080B Screen.

Additional Information

Parameters

Start Point

End Point

MSR02A - Extract Programs Available to a Global Profile

The **MSR02A** - Extract Programs Available to a Global Profile report extracts programs available to a global profile, and the level of access to each program. This report also includes the point of comparison at which access is granted. The extract is used by the ***MSR02B*** - Programs Available to a Global Profile report.

This report assumes that site security in Ellipse EAM uses the following setup methodology:

- Program profiles contain a maximum of 2 values: 9 in position 001, and one value at another point.
- Security setup is documented in the Table File 'PW'; for example:

This example indicates that:

- **MSO220** has a 9 in position 001 and a value in position 060
- **MSO200** has a 9 in position 001 and a value in position 065
- **MSO203** has a 9 in position 001 and a value in position 065

Additional Information

Parameters Enter the following information in the Report Request Selection screen for this report:

Global Profile Name The name of a global profile. This allows any number of users or program profiles to have a common security access definition, making profile maintenance easier.

MSR02B - Programs Available to a Global Profile Report

The **MSR02B** - Programs Available to a Global Profile reports programs available to a global profile, and the level of access to each program. It also includes the point of comparison at which access is granted.

Note: This report cannot be requested directly. It is automatically submitted by the MSR02A - Extract Programs Available to a Global Profile report.

MSR020 - Security File Listing

Report **MSR020A** lists User, Program, Global, Function and Entity security profiles. This report should be used by users responsible for security profiles to list existing and/or changed profiles to validate any changes made. The option to include user ID/program profiles is particularly useful to check that a user does not have access to a program that should be protected.

This report can be generated at any time. The results are sorted alphabetically, with a new page for each selection type.

Additional Information

Parameters Enter the following information in the Report Request Selection screen for this report:

Include User Profiles (Y/N) Enter 'Y' to include user profiles on the report.

Owner range: From/To Enter a range of owners to restrict user profile selection.

Leave **From** blank to report from the first owner. Leave **To** blank to report to the last owner.

Userid range: From/To Enter a range of user IDs to restrict user profile selection. Leave **From** blank to report from the first user ID. Leave **To** blank to report to the last user ID.

Include Program Profiles (Y/N) Enter **Y** to include program profiles in the report.

Include Global Profiles (Y/N) Enter **Y** to include global profiles in the report.

Include Security Positions (Y/N) Enter **Y** to include Security position details in the report. This detail comes from Table File **PW**.

Include Function Profiles (Y/N) Enter **Y** to include function profiles in the report.

Include Entity Profiles (Y/N) Enter **Y** to include entity profiles in the report.

MSRIPE - Invalid Login Attempts

This report details invalid login attempts.

Additional Information

Parameters Enter the following information in the Report Request Selection screen for this report:

User Id Enter a user ID for which to report invalid login attempts.

Start Date Enter the start date of the range to report unsuccessful login attempts.

Start Time (HHMM) Enter the start time of the range to report unsuccessful login attempts.

End Date Enter the end date of the range to report unsuccessful login attempts.

End Time (HHMM) Enter the end time of the range to report unsuccessful login attempts.

Terminal Id Enter the terminal identifier to report on unsuccessful login attempts from a specific terminal.

Ellipse Security - Screens

Screens

Dialog Box - Add Security Class

Use this dialog box to grant access to existing classes.

Note: This dialog box does not allow you to create or add a new class to an application.

Class Name

The description of the security class to add, for example, Catalogue.

Access Level

Enter the level of access to be given to the class entered.

Dialog Box - Go To

Use this dialog box to search and display the required application and its associated classes.

Application Name

The name of the required application, for example, MSE100.

Dialog Box - Save As (Security Profile)

Use this dialog box to copy an existing security profile to be used to create another employee's security profile.

EXISTING PROFILE

Profile Type

A profile type. This field is mandatory.

This field defaults to Sign On.

Valid types are:

Sign On	Searches for sign on profiles stored in the Ellipse EAM system.
Global	Searches for global profiles stored in the Ellipse EAM system.

Profile Name

A security profile name. This is used as an identifier for the profile.

District Code

The district code associated with the security profile.

SAVE TO

Profile Type

A profile type. This field is mandatory.

This field defaults to Sign On.

Valid types are:

Sign On	Searches for sign on profiles stored in the Ellipse EAM system.
Global	Searches for global profiles stored in the Ellipse EAM system.

Profile Name

A security profile name. This is used as an identifier for the profile. This field is mandatory when creating a new security profile.

District Code

The district code associated with the security profile.

Default Menu

The default menu relating to a sign on profile. This can be used to filter the search for profiles. This field is only available for sign-on profiles.

Employee ID

The employee ID linked to the security profile.

Note: This field is only enabled for **Sign On** profile types.

Dialog Box - Set All Attributes

Use this dialog box to set the access level for the selected class attribute.

Access Level

The access level for the class attribute.

Note: Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a class attribute.

The access levels are:

No Access	The class attribute is removed from both the application search and detail screens.
Read Only	The class attribute is read only.
Read Write Access	The class attribute can be viewed, details can be entered and modified.

Dialog Box - Set All Methods

Use this dialog box to set the security access level for the selected class method.

Access Level

The access level description for the security class method.

For example, Full Access, No Access or Review Access.

Dialog Box - Set User Licence Type

Use this dialog box to set licence types for the selected users.

Licence Type

The licence type to set for the user. Licence types include:

- **No Licence**

  User has access to no applications

> **Note:** Regardless of the security settings for an application, if the user licence type is set to **No Licence**, the user cannot access the application.

- **ESS (Employee Self Service)**

  User has access to a subset of applications

- **Limited Use**

  User has access to a subset of applications (some applications in **Review Only** mode)

- **Full Use**

  User has access to all Ellipse EAM applications, depending on screen security.

Dialog Box - Upload System Licence

Use this dialog box to enter the encrypted system licence string provided to your organisation, if your organisation has opted to use the named licensing model.

Licence String

An encrypted system licence string.

A licence string is provided where your organisation has opted into the name licensing model or where your organisation is moving back to a named licensing model from using a concurrent user licence model.

MSE020 - Search Security

Use this screen to search for security profiles.

Search Method

The search screen provides facilities for searching for a security profile based on a specific search method and criteria.

Records found matching the search criteria display in the results grid. This field is mandatory.

Select the required search method:

All	Displays all security profiles matching the **Profile Type** entered. For example, if **Sign On** is selected in the Profile Type field, all sign on profiles display in the search results grid.
Exact Match	Displays the exact security profile based on the entries made in the search fields.
Starts From	Displays the security profiles that start from the specified characters and match the entered search criteria.
Starts With	Displays the security profiles that start with the specified characters and match the entered search criteria.

Profile Name

A security profile name. This is used as an identifier for the profile.

Profile Type

A profile type. This field is mandatory.

This field defaults to Sign On.

Valid types are:

Sign On	Searches for sign on profiles stored in the Ellipse EAM system.
Global	Searches for global profiles stored in the Ellipse EAM system.

District Code

The district code required in the search.

By leaving this field blank, this returns the profile across all districts.

If the profile type is **Global**, this field is disabled.

Employee ID

The employee ID required for the search.

FILTERS

Default Menu

The default menu relating to a sign on profile. This can be used to filter the search for profiles. This field is only available for sign-on profiles.

Global Profile

The global profile name. The search results returned will be restricted to the profile selected.

The global profile determines a user's access to various programs with Ellipse EAM.

Access to Application

The name of the application, for example, MSE100.

All profiles which have access to the application entered display in the search results grid.

MSE020 - Security detail

Use this screen to create and maintain sign on and global security profiles.

Note: A Sign On profile must be created for all users.

Ellipse EAM security provides access control over:

- Applications
- Methods and Attributes (Class Security)
- Reference Codes

The following screens are also used to maintain security details and can only be accessed using this screen:

- MSE02A - Class Security
- ***MSE02C*** - Security Classes
- ***MSE02D*** - Security Application
- ***MSE02R*** - Security Profile Reference Codes

Profile Name

A security profile name. This is used as an identifier for the profile. This field is mandatory when creating a new security profile.

Profile Type

A profile type. This can be a sign on or global profile.

District Code

The district code associated with the security profile. This identifies which district the profile belongs to. This field is mandatory for sign on profiles.

If left blank, the profile is created in all districts. If the user has access or uses multiple districts a sign on profile must be created for all districts used.

Tabs

- ***Profile Details***
- ***Applications***
- ***Class***

Profile Details tab

Owner Id

An identifier for grouping.

Note: If the security profile is a **Global** profile, only the **Owner ID** field is enabled.

Default District Flag

Indicates a default district.

Note: This flag is only enabled for **Sign-on** profiles.

Employee ID

The employee ID linked to the security profile.

Note: This field is only enabled for **Sign On** profile types.This field is mandatory when creating a security profile.

Menu Name

The default menu for the security profile. This field is only available for sign-on profiles, and identifies the menu presented to the user at login.

Login User

The logged in employee ID.

Licence Type

The licence allocated to the user if using the Named User Licence model. The value entered determines which applications a user is licensed to use.

Valid values are:

- 0 - No Licence Allocated
- 1 - ESS Licence
- 4 - Limited Use Licence
- 9 - Full Use Licence

Note: This field displays for sign on profiles only.

Global Profile

The name/ID of the global profile.

Note: This field is enabled for **Sign On** profile types only.

Profile Login Locked

If selected, indicates a sign-on profile is locked and the user cannot log in to Ellipse EAM.

A sign-on profile is locked when one of the following occurs:

- The maximum number of allowable login attempts is exceeded.
- The System Administrator manually locks the profile.

Note: This field only displays for a **Sign On** profile type.

Global Attached to Position

If selected, indicates a global profile is attached to the position.

Note: This field only displays for a **Sign On** profile type.

Applications tab

APPLICATIONS

App Name

The name of the application, for example MSE040.

App Desc

(Application Description)

The description of the application, for example, Security or Diary.

Review Flag

Indicates that the selected application has been defined as **Review Only** by the system.

Access Level

The access level for the application, for example, No Access, Full Access or Review Access.

App Type

(Application Type)

The defined owner of the application.

Note: Currently all applications are set to Mincom defined.

Class tab

The fields on this tab are described below:

Class Name

The class name associated to the security profile.

Access Level

The access level for the selected class.

No Access	The profile cannot execute this application.
Review Access	This profile can execute this application and view the data contained within the application. The profile cannot create, update or delete any data contained within this application.
Full Access	The profile has full access to this application up to the restrictions set on class and reference codes.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Class Security** - Opens the MSE02A - Update Class Security screen.
- **Reference Codes Security** - Opens ***MSE02R*** - Security Profile Reference Codes screen.
- **Program Security** - Opens the ***MSM020A*** - Maintain Security Profile screen.

MSE02C - Search Security Classes

Use this screen to search for security class details associated with the security profile entered.

Profile Type

A profile type.

Valid types are:

Sign On	Searches for sign on profiles stored in the Ellipse EAM System.
Global	Searches for global profiles stored in the Ellipse EAM System.

Profile Name

A security profile name. This is used as an identifier for the profile.

District Code

The district code associated with the security profile.

Class Name

The class names associated with the security profile entered.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Search** - Displays the search results in the grid after entering the search criteria.
- **New Search** - Returns to the Search screen and clears the search results and the search criteria.

MSE02C - Security Classes detail

Use this screen to review and modify security class details for the selected security profile.

Access Level

The access level for the selected class.

Note: Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a class.

Levels are:

No Access	The profile cannot use this class.
Full Access	The profile has full access to the class, up to the restrictions set on the attributes and methods associated with the class.

Class Name

The description of the class selected, for example Catalogue.

Profile Name

The security profile name entered or selected in the search.

Profile Type

The profile type, global or sign on.

District Code

The district code associated with the security profile.

Tabs

- ***Methods***
- ***Attributes***
- ***Applications***

Methods tab

Class Method

An action that can be performed for the security class.

For example, Create, Modify, Delete, Copy and so on.

Access Level

The numeric level of access for the class method.

For example, if a profile has an access level of **9** to class method **Delete**, the user has **Full Access**. If the access level is **0**, the user has **No Access**.

Note: Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a class method.

Access Level Desc

The access level description for the security class method.

For example, Full Access, No Access or Review Access.

Attributes tab

Class Attribute

The class attribute name.

Class Attribute Description

The name of the field name used. This field (attribute) displays in the application.

Review Flag

Indicates that the class has been defined as **Review Only** by the system.

Access Level

The access level for the class attribute.

> **Note:** Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a class attribute.

The access levels are:

No Access	The class attribute is removed from both the application search and detail screens.
Read Only	The class attribute is read only.
Read Write Access	The class attribute can be viewed, details can be entered and modified.

Applications tab

App Name

(Application Name)

The name of the application (for example, MSE100) that uses the class and for which you have access.

App Desc

(Application Description)

The application description, (for example Catalogue) used by the class and for which you have access.

App Type

(Application Type)

The defined owner of the application.

> **Note:** Currently all applications are set to Mincom defined.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Submit** - Validates and saves the data entered.
- **Refresh** - Reloads the original data. Any changes made since the last submit are lost.
- **Save As** - Creates a new item based on the information provided by an existing item.

- **New Search** - Returns to the Search screen and clears the search results and the search criteria.
- **Application Security** - Opens ***MSE020*** - Security detail for the selected security profile.
- **Reference Codes Security** - Opens ***MSE02R*** - Security Profile Reference Codes screen.
- **Set All Methods** - Opens the Dialog Box - ***Set All Methods***, where you can set the access level for the class methods.
- **Set All Attributes** - Opens the Dialog Box - ***Set All Attributes***, where you can set the access level for the selected class attribute.

MSE02D - Update Security Application

Use this screen to review class security details. This screen can also be used to modify the access level of the selected applications.

Access Level

The access level for the application, for example, No Access, Full Access or Review Access.Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a application.

Application Description

The description of the application, for example, Security or Diary.

Application Name

The name of the application, for example MSE040.

Application Type

The defined owner of the application.

District Code

The district code associated with the security profile.

Profile Name

The security profile name entered or selected in the search.

Profile Type

The profile type, global or sign on.

Review Flag

Indicates that the selected application has been defined as **Review Only** by the system.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Submit** - Validates and saves the data entered.
- **Refresh** - Reloads the original data. Any changes made since the last submit are lost.
- **Save As** - Creates a new item based on the information provided by an existing item.
- **Open** - Displays a menu list with the following options:
  - Open Security
  - Open Application
  - Open Class

  Select the required option, this displays a dialog box to enter existing item details.
- **New Search** - Returns to the Search screen and clears the search results and the search criteria.
- **Application Security** - Opens ***MSE020*** - Security detail for the selected security profile.
- **Reference Codes Security** - Opens ***MSE02R*** - Security Profile Reference Codes screen.
- **Go To** - Opens the Dialog Box - ***Go To***.
- **Reset to Root Node** - Displays the MSE02A - Update Class Security screen and returns you to the root node at last save point.

MSE02R - Search Security Profile Reference Codes

Use this screen to search for security profile reference codes.

Search Method

The search screen provides facilities for searching for a reference codes associated with a security profile based on a specific search method and criteria.

Records found matching the search criteria display in the results grid.

Select the required search method:

All	Displays all Reference Codes matching the selection criteria entered.
Exact Match	Displays the exact Reference Code based upon the entries made in the search fields.
Starts From	Displays the Reference Codes that start from the specified characters and match the entered search criteria.
Starts With	Displays the Reference Codes that start with the specified characters and match the entered search criteria.

Profile Name

A security profile name. This is used as an identifier for the profile.

Profile Type

A profile type.

Valid types are:

Sign On	Searches for sign on profiles stored in the Ellipse EAM System.
Global	Searches for global profiles stored in the Ellipse EAM System.

District Code

The district code associated with the security profile. This identifies which district the profile belongs to. This field is mandatory for sign on profiles.

If left blank, the profile is created in all districts. If the user has access or uses multiple districts a sign on profile must be created for all districts used.

Employee Id

The employee ID required for the search.

FILTERS

Default Menu

The default menu for the security profile. This field is only available for sign-on profiles, and identifies the menu presented to the user at login.

Global Profile

A global profile. If the sign-on profile is using a global profile, the name of the global profile displays in this field.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Search** - Displays the search results in the grid after entering the search criteria.
- **New Search** - Returns to the Search screen and clears the search results and the search criteria.
- **New** - Displays the screen to create a new item related to the application.

MSE02R - Update Security Profile Reference Codes Detail

Use this screen to review and modify security profile reference code details.

District Code

The district code associated with the security profile.

Profile Name

A security profile name. This is used as an identifier for the profile.

Profile Type

The profile type, global or sign on.

Owner Id

The employee ID of the owner of the profile.

Default District Flag

Indicates a default district.

Note: This flag is only enabled for **Sign-on** profiles.

Employee Id

The employee ID linked to the security profile.

Note: This field is only enabled for **Sign On** profile types.

Employee Name

The employee name associated with the employee ID.

Default Menu

The default menu for the security profile. This field is only available for sign-on profiles, and identifies the menu presented to the user at login.

Menu Description

The default menu description. The name/description given to the default menu ID.

Global Profile

A global profile. If the sign-on profile is using a global profile, the name of the global profile displays in this field.

GRID

Ref Code Entity

(Reference Code Entity)

The system defined name of the application's reference codes.

Ref Code Desc

(Reference Code Description)

The system defined description of the applications reference codes.

Access Level

The reference code access level.

> **Note:** Refer to ***Setting Security Access Levels for Applications, Classes, Methods and Attributes*** for information on applying the correct access level to a reference code.

Levels are:

No Access	The profile cannot view the related reference code or data associated with it.
Read Only	This profile can view the reference code and data associated with it.
Read Write Access	The profile can view the reference code and make changes to related data.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Submit** - Validates and saves the data entered.
- **Refresh** - Reloads the original data. Any changes made since the last submit are lost.
- **New** - Displays the screen to create a new item related to the application.
- **Save As** - Creates a new item based on the information provided by an existing item.
- **Delete** - Displays a confirm deletion dialog box to confirm deletion of the current item.
- **Open** - Displays a dialog box to enter an existing item to display its detail.
- **New Search** - Returns to the Search screen and clears the search results and the search criteria.
- **Application Security** - Opens ***MSE020*** - Security detail for the selected security profile.
- **Class Security** - Opens the MSE02A - Update Class Security screen.

MSM020A - Maintain Security Profile

Use this screen for maintaining and reviewing security profiles.

Options

Enter one of the following options:

Review Profile	Use this option to review profile details.
Create Profile	Use this option to create a new profile.
Modify Profile	Use this option to modify an existing profile.
Delete Profile	Use this option to delete a profile that is no longer required. When deleting a global profile ensure no user IDs are linked to the profile. The user IDs will no longer have the correct security access once the profile is deleted.

Profile type

Select the profile type to create, modify, or review. This field is mandatory.

The available options are:

E - Entity Profile	Used to secure data entities, to which reference codes may be linked.
F - Function Profile	Used to define the access level required for a particular function.
G - Global Profile	Used to define groups of users with common access requirements.
P - Program Profile	Used to secure an Ellipse EAM program from unauthorised user access.
S - Sign On Profile	Allocated to each Ellipse EAM user.

Profile name

The name of the profile to work with. This can be a user, program, global profile, or entity profile. This field is mandatory.

For batch programs, enter the profile name in the format **MSB01001** where the Table File program (MSB010) is the program name and 01 is the request number.

An example for utility batch programs is MSU0200101. An example for cross-reference batch programs is MSX13001.

Format

Select the format in which to display the information. The default is **S**. This field is mandatory.

Available options are:

S	Short display. All details are displayed on one screen.
L	Detailed display. Long form display is useful when creating Sign On (S) and Global (G) type profiles, and the Table File PW - Security Profile Position Descriptions identifies the profile positions at which programs are protected.

District

This field displays for multi-district systems only.

The name of the district to which the profile relates. Leave this field blank to create a profile in every district. If you enter a district, the profile will apply to only that district.

Entry is not required for Global - (**G**), Program (**P**), Entity (**E**), and Function (**F**) type profiles.

This field is mandatory when reviewing or modifying Sign On (**S**) type profiles.

Existing Profile

The name of an existing profile to be used as a copy for the new profile. Use an existing profile that is similar to the one you want to create.

The existing profile must be of the same type as that being created, for example, Sign on to Sign on.

Note: This field displays when the **Create Profile** option is selected.

In District

The district of the existing profile being used as a copy for the new sign-on profile.

This field is mandatory when creating sign-on profiles and an existing profile is being used as a template.

Note: This field only display when the **Create Profile** option is selected.

MSM020B - Maintain UserID Profile (Long Form)

Use this screen to create, modify, or review the selected security profile information in a long format, where the description of each profile position is extracted from the Table File PW - Security Profile Position Descriptions.

If a position is not defined, only the position number displays in the grid and the description does not display.

Position details can also be viewed in short format by clicking the **Short form** button.

Name

The name of the profile displays in this field as allocated on the ***MSM020A*** - Maintain Security Profile screen.

District

The district in which this profile exists. If this field is blank, the profile exists in more than one district.

This field displays for user profiles only.

Owner

This field displays the person responsible for a profile. This field is for documentation purposes only.

Global Profile

The name of a global profile. This allows any number of users or program profiles to have a common security access definition, making profile maintenance easier.

Emp Id.

(Employee ID)

The ID of the employee linked to the security profile.

Default for Emp

(Default for Employee)

This field displays for user profiles only.

Enter **Y** to indicate that this profile is to be used as the default user profile for the employee. It cannot be selected as the default user profile if the user exists in more than one district, or is assigned to more than one position.

Enter **N** to indicate that this profile is not the default user profile for the employee.

Default

This field displays for user profiles only.

Enter **Y** in this field to select this district each time this user logs in.

Menu

This field displays for sign-on profiles only.

Enter the name of the menu to be displayed whenever this user logs in.

Profile Login Locked

This indicator identifies whether a sign-on profile is to be locked. A sign-on profile is locked when the System Administrator manually locks the profile.

- **Y** - The security profile is locked. The user cannot log in to Ellipse EAM.
- **N** - The security profile is not locked.

Note: This field displays for System Administrator access only.

Enter Profile Position to Restart Display

This field allows you to restart the long form display of a profile from any valid profile position. Enter the profile position from which the display is to be restarted.

Security Access

This field displays for user profiles only.

Enter the security access level for this user profile. The security access level cannot be changed to a value greater than that of the profile of the user making the modification.

This field is used by some programs to restrict the functions available to lower level users.

Security Access

This field displays for sign on profiles only.

Enter the security access level for this user profile. The security access level cannot be changed to a value greater than that of the profile of the user making the modification.

This field is used by some programs to restrict the functions available to lower level users.

Licence Type

The licence allocated to the user if using the Named User Licence model. The value entered determines which applications a user is licensed to use.

Valid values are:

- 0 - No Licence Allocated
- 1 - ESS Licence
- 4 - Limited Use Licence
- 9 - Full Use Licence

Note: This field displays for sign on profiles only.

POSITION GRID

Pos.

(Position)

This field displays the position of the security profile, starting at any position from 1 to 250.

Description

The position description profile.

Maximum

This field displays the maximum value that can be assigned to each profile position.

Value

Enter the actual access level value for the position. Users cannot allocate a value greater than the one contained in their own profile.

The system administrator can allocate any value from zero to nine in any profile position.

Program profiles should always have a 9 in the first profile position. Placing a 9 in the first profile position of a user profile makes the user an administrator, with access to all applications.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

MSM020C - Maintain UserID Profile (Short Form)

Use this screen to create, modify, delete, or review the selected security profile information. The selected security profile information displays in short format.

Short format displays the entire 250-character numeric string, which is all the profile positions. The display takes the format of three numeric lines, labelled **Max**, **Val**, and **Cmp**. These lines indicate the profiles of the logged-in user (**Max** - the maximum value you can assign to each profile position), the profile being reviewed (**Val** - the values of the profile being reviewed), and the profile being compared with (**Cmp** - the comparison profile).

Position details can also be viewed in long format by clicking the **Long form** button.

Name

This field displays the profile name. It cannot be edited.

District

In multiple district installations, this field indicates the district that the profile applies to, but displays for S-type profiles only.

Tabs

- ***Access***
- ***General***

Access tab

The Access tab displays the entire 250-character profile, without descriptions, from the Table File PW - Security Profile Position Descriptions.

A profile value can be entered at each position required to construct the profile. Values that can be entered are 0-9. The positions the values are entered is from 1-250.

Users cannot allocate a value greater than the value contained in their own profile, at each profile position.

Each position can be assigned a value, if required, or left blank. Those with a value assigned are used by the comparison function to determine the level of access the user has, while executing programs protected at that position.

Program profiles have a 9 in the first profile position.

Placing a 9 in the first profile position of a users profile makes the user an Administrator with access to all applications.

Max

(Maximum Profile Value)

This field displays the maximum value that can be assigned to each profile position.

Val

(Profile Value)

This field displays the values of the profile being reviewed.

Cmp

(Comparison Profile)

This field displays the comparison profile.

Security

This field displays for user profiles only.

Enter the security access level for this user profile.   The security access level cannot be changed to a value greater than that of the profile of the user making the modification.

This field is used by some programs to restrict the functions available to lower level users.

Type

The type of profile to compare.

The **Type**, **Name**, **District** and **Compare Value** fields allows you to compare two profiles. By comparing profiled, this helps to determine if a **Sign on** or **Global** type profile has the correct level of access to a program.

The profile types are:

E	Compare an entity profile.
F	Compare a function profile.
G	Compare a global profile.
P	Compare a program profile.
S	Compare a user profile.

Name

Enter the name of the profile to be compared with the current profile.

District

This field is only required when the compare profile is an S-type profile.

Enter the District Code of the profile to be compared with the current profile, if the compared profile is a sign-on profile.

Compare Value

This field displays the result of a profile comparison, and is a number between 0 and 9. Where a sign-on profile is being compared with a program global or function profile, a value of zero indicates that users of the profile being reviewed would not have access to any program protected by the profile it is being compared with.

General tab

Owner

This field displays the person responsible for a profile. This field is for documentation purposes only.

Global Profile

The name of a global profile. This allows any number of users or program profiles to have a common security access definition, making profile maintenance easier.

Emp ID

(Employee ID)

The ID of the employee linked to the security profile.

Default for Emp

(Default for Employee)

This field displays for user profiles only.

Enter **Y** to indicate that this profile is to be used as the default user profile for the employee. It cannot be selected as the default user profile if the user exists in more than one district, or is assigned to more than one position.

Enter **N** to indicate that this profile is not the default user profile for the employee.

Licence Type

The licence allocated to the user if using the Named User Licence model. The value entered determines which applications a user is licensed to use.

Valid values are:

- 0 - No Licence Allocated
- 1 - ESS Licence
- 4 - Limited Use Licence
- 9 - Full Use Licence

Note: This field displays for sign on profiles only.

Default

This field displays for user profiles only, and identifies the value in the District field as the default district for this S-type profile. As a result, the user will not need to identify a district during log in. Ellipse EAM automatically selects the default.

Enter **Y** in this field to select this district each time this user logs in.

Menu

This field displays for sign-on profiles only.

Enter the name of the menu to be displayed whenever this user logs in.

Profile Login Locked

This indicator identifies whether a sign-on profile is to be locked. A sign-on profile is locked when the System Administrator manually locks the profile.

- **Y** - The security profile is locked. The user cannot log in to Ellipse EAM.
- **N** - The security profile is not locked.

Note: This field displays for System Administrator access only.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Long Form** - Opens the ***MSM020B*** **-** Review Program Profile screen.

MSM025B - System Menu

Use this screen to create and maintain menu options and related information.

Menus display differently according to the number of options viewable by the user. Menus may also contain:

- Options for other menus
- Options for MSO programs
- Options for batch or report processes
- Other options for MSE programs

It is useful to be aware of this when creating or modifying menus.

Menus are restricted to a maximum of 30 menu options, each of which can be a program or another menu.

Note: Avoid creating multiple menus that are similar in content, as these tend to increase the maintenance task.

Menu Name

The name of the menu.

Parameter Type

Select the parameter type. Options are:

E	The employee is validated and used for employee/position based screens.
P	The position is validated and used for employee/position based screens.

The reason this parameter is required is because some Ellipse EAM programs for example, Human Resource programs, require the user's employee or position number to be known before the program can be accessed.

For this reason, menus are configured with a parameter type of **E** or **P**. If the program demands the employee or position number, **Y** is inserted against the program description. The value entered continues to be used for employee/position-based screens until it is changed.

District

The district linked to the menu.

Heading

The heading text that displays when this menu is displayed.

Line

The line number.

Description

Enter up to 50 characters of free-form text describing the menu option.

Program

Enter the program to be executed when the menu option is selected.

Notes:

• Both this and the **Menu Name** field can be left blank. This effectively creates a comment line on the menu. When the menu is built, this entry is not given an option number.

- If this field and the menu name are completed, and the security field contains **Y**, Ellipse EAM checks the users profile against the profile of this program to determine if the user should see this option.
- To set up an **MSE100YYYYYY** application, for example **MSE100Create** place the first 6 characters in this field **(MSE100)** and the rest **(Create)** in the adjacent **Data Passed** field.
- Reports and batch programs are established as menu options by entering **MSO080** in the **Program** field and the report identifier in the **Data Passed** field.

Menu Name

Enter the name of a menu to be displayed if this menu option is selected. In this case, the previous field (**Program**) is only used for security clearance validation.

Both this and the **Program** field can be left blank, to create a comment line on the menu.

Data Passed

Enter any data to be made available to the specified program.

Notes:

- Reports are established as menu options by entering **MSO080** in the **Program** field and the report identifier in the **Data Passed** field. If the report has multiple requests, such as **MSB070**, the **Data Passed** field should contain the report name, followed by two spaces and the request number (for example, **MSB070A 01)**. Security is checked against the program **MSO080** not the report number.
- To set up, for example an **MSE100YYYYYY** application, place the characters from the seventh position onwards in this field. For example, the **MSE100 Create** application **Create** would be placed in this field.

Security

Select an option to set security for the menu item:

N	Menu options with this security value do not display. This may be used for example, during development or while rebuilding menus.
Y	The menu item only displays to users with adequate security access. The security process works by comparing the users profile to the profile of the program identified in the **Program** field, prior to displaying the menu. This involves some system overhead in performing the security check prior to displaying the menu. If the user has no access to the program, the option does not display on the menu.
Blank	Leaving the security option blank results in the menu item always displaying to all users. No security check are made **Note:** This may result in users seeing menu options to which they have no access.

Param Mandatory

(Parameter Mandatory)

Note: You can only complete this field if you completed **Parameter Type**.

Enter **Y** to make the parameter value mandatory when choosing a menu option from the Main Menu screen.

Actions

Select an action. The following actions are available, depending on the level of user access and the modules installed:

Delete a New Line	Delete a new line.
Insert a New Line	Inserts a new blank line below the current line.
Repeat a Line	Repeats the current line by creating a new line with the same data below the current line.

MSELIC - Search Licence Management

Use this screen to search for named user licences and nominate licence types for users.

Licence types can be nominated in instances where:

- A user has no licence type
- A user licence type requires an update

The licence type nominated determines if the user has access to applications within Ellipse EAM.

Licence types include:

- **No Licence**

  User has access to no applications

  > **Note:** Regardless of the security settings for an application, if the user licence type is set to **No Licence**, the user cannot access the application.

- **ESS (Employee Self Service)**

  User has access to a subset of applications

- **Limited Use**

  User has access to a subset of applications (some applications in **Review Only** mode)

- **Full Use**

  User has access to all Ellipse EAM applications, depending on screen security.

Licence types can also be set when creating a new user profile in the following screens:

- ***MSE020*** - Security
- ***MSM020B*** Create User Profile (Long Form)
- ***MSM020C*** - Create User Profile (Short Form

Licence types for users can be bulk updated using Smart Excel.

You can also use this screen to open ***MSEALT*** - Review List Application Licence Type and review a list of applications, the application licence type and the application access type.

Related Process and Activities

Licence Type

The licence type in which to search. Options are:

- No Licence
- Full Licence
- Limited Use Licence
- Employee Self Service Licence

Global Profile

The global profile in which to search for licences.

Position

The position in which to search for licences.

Employee

The employee in which to search for licences. On return of search results, the grid displays the type of licence the employee holds.

LICENCE INFORMATION

Issue Date

The date the licence was generated.

Issue Time

The time to licence was generated.

ALLOCATED

Full Use Licences

The number of full use licences allocated to your organisation.

Limited Use Licences

The number of limited use licences allocated to your organisation.

ESS Licences

The number of employee self service licences allocated to your organistation.

USED

Full Use Licences

The number of full use licences in use in your organisation.

Limited Use Licences

The number of limited use licences in use in your organisation.

ESS Licences

The number of employee self service licences in use in your organisation.

AVAILABLE

Full Use Licences

The number of full use licences still available for use in your organisation.

Limited Use Licences

The number of limited use licences still available for use in your organisation.

ESS Licences

The number of employee self service licences still available for use in your organisation.

SUMMARY GRID

User

The user ID of the employee.

Employee

The employee ID and name.

Licence Type

The type of licence the employee is using. Options are:

- No Licence
- Full Licence
- Limited Use Licence
- Employee Self Service Licence

Position

The position held by the employee.

Global Profile

The global profile held be the employee.

Grid Actions

Grid actions allow you to perform an action relating to the item in the grid. For more information, refer to Grids.

The following grid actions are available:

- **Set User Licence Type** - Opens Dialog Box - ***Set User Licence Type***, where you can set a licence type for an employee.

Functions and Actions

Function and Actions allow you to perform a command or task in an application. For more information, refer to Ellipse EAM Application Toolbar.

- **Upload System Licence** - Opens Dialog Box - ***Upload System Licence*** where the system licence string can be entered.
- **List Application Licence Type** - Opens the ***MSEALT*** - Review List Application Licence Type screen, where you can review a list of applications and the licence type the application holds.

Related Screens

MSEALT - Review List Application Licence Type

Use this screen to review a list of applications and the application licence type. The screen also displays the applications access type (for example, Review Only).

Note: This screen can only be accessed through ***MSELIC*** - Search Licence Management.

Application ID

The ID of the application, (for example MSEXXX or MSOXXX).

Application Name

The name of the application, that is MSE name or MSO name.

Minimum Licence Entitlement Required For Use

The minimum licence type required to access the application.

The following licence types display:

- Full Use
- Limited Use
- ESS (Employee Self Service Licence)

Entitlement Restriction

The type of application access, for example Review Only.