

# Configuring OpenEnterprise™ Security Reference Guide (V3x)

**Revision Tracking Sheet**

**September 2017**

This manual may be revised periodically to incorporate new or updated information. The revision date of each page appears at the bottom of the page opposite the page number. A change in revision date to any page also changes the date of the manual that appears on the front cover. Listed below is the revision date of each page (if applicable):

<b>Page</b>	<b>Revision</b>
All pages	September 2017
All pages	August 2017
Initial issue	May 2016

# Contents

<b>1</b>	<b>Overview .....</b>	<b>1</b>
1.1	Security Concepts .....	1
1.1.1	Users and Groups.....	2
1.1.2	The Hierarchy of Users and Groups .....	3
1.1.3	Active Directory Overview .....	4
1.2	Tokens.....	5
1.2.1	Application Tokens .....	6
1.2.2	File Tokens.....	6
1.2.3	OPC Item Token Types.....	6
1.2.4	Custom Tokens.....	6
1.2.5	Token Wildcards .....	9
1.2.6	Token Pattern Matching .....	9
1.2.7	Token Security Hierarchy .....	11
1.3	Access Areas .....	12
1.4	Database Privileges .....	12
1.5	Security Manager .....	13
1.5.1	Workstation Login Client .....	14
1.5.2	Container Security Login.....	14
1.5.3	Security and Workstation Views.....	15
1.5.4	Security and Administrative Tools .....	15
1.5.5	The Security Configuration Tool.....	15
1.5.6	Access to OpenEnterprise Login dialogs .....	15
1.5.7	Applied Security Settings .....	15
1.5.8	Security Group Privileges Editor .....	15
1.5.9	Security Manager User Interface .....	16
<b>2</b>	<b>Security Configuration Tool.....</b>	<b>21</b>
2.1	Menu Bar .....	21
2.1.1	File Menu .....	22
2.1.2	Edit Menu .....	22
2.1.3	Tools Menu - Options.....	31
2.1.4	Help Menu .....	32
2.2	The Tree Pane .....	32
2.2.1	Default Group Node.....	33

- 2.2.2 Users Node ..... 33
- 2.2.3 User Nodes ..... 34
- 2.2.4 Groups Node ..... 35
- 2.2.5 Group Nodes ..... 38
- 2.2.6 Tokens Node ..... 38
- 2.2.7 Access Areas Node..... 43
- 2.3 The List Pane ..... 45
- 2.4 Security Configuration Dialogs..... 46
  - 2.4.1 User Properties: Properties tab..... 46
  - 2.4.2 User Group - Properties..... 53
  - 2.4.3 User Properties: Account tab ..... 55
  - 2.4.4 User Properties: Summary tab ..... 57
  - 2.4.1 User Properties: Access Areas tab..... 59
  - 2.4.2 User Properties: Application Token tab ..... 60
  - 2.4.3 User Properties: Custom Token tab..... 62
  - 2.4.4 User Properties: File Token tab..... 64
  - 2.4.5 User Properties: OPC Item Token tab ..... 66
  - 2.4.6 User Properties: User Token Group tab..... 68
- 2.5 Token Group Properties ..... 70
- 2.6 Token Properties Dialog..... 72
- 2.7 Token Summary Dialog..... 73
- 2.8 SQL Import-Export File Dialog ..... 74
- 2.9 Options Dialog..... 75
  - 2.9.1 Options Dialog: Token Drag Tab ..... 75
  - 2.9.2 Options Dialog: Message Tab..... 76
- 3 Using the Security Configuration Tool ..... 79**
  - 3.1 Managing Security Objects ..... 79
    - 3.1.1 Creating a New User ..... 79
    - 3.1.2 Creating New User Groups..... 79
    - 3.1.3 Adding Default Groups ..... 80
    - 3.1.4 Creating New Token Groups ..... 80
    - 3.1.5 Creating Custom, File and OPC Item Tokens ..... 81
    - 3.1.6 Creating New Application Tokens ..... 82
    - 3.1.7 Creating New Access Areas ..... 82
  - 3.2 Modifying Security Objects ..... 83

3.2.1	Modifying Default Group Settings.....	83
3.2.2	Modifying User Account Settings.....	83
3.2.3	Adding a New User to a Group .....	84
3.2.4	Removing All Users from a Group .....	85
3.2.5	Modifying Token Groups .....	85
3.2.6	Linking Tokens with a Token Group .....	86
3.2.7	Linking Tokens or Token Groups with Users or Groups .....	86
3.2.8	Modifying Custom, File and OPC Item Tokens.....	87
3.2.9	Viewing and Breaking Token Links .....	87
3.2.10	Modifying Access Areas .....	88
3.2.11	Deleting Security Objects .....	89
3.3	Logging into the Container for the First Time .....	90
3.4	Changing the SYSTEM User Password.....	92
3.4.1	On a SingleBox Solution and Standalone Server .....	92
3.4.2	On a Redundant System.....	93
3.4.3	On a Remote Communication Controller .....	93
3.4.4	On a Reporting or Messaging Server .....	93
3.4.5	On a Standalone Workstation .....	94

**4 Security Group Privileges Editor ..... 95**

4.1	Main Dialog.....	95
4.1.1	Groups .....	97
4.1.2	Tables and Views .....	97
4.1.3	Assigning Privileges .....	97
4.1.4	Changed Privileges .....	98
4.1.5	User Groups.....	98
4.2	Main Dialog Menu .....	98
4.2.1	File.....	99
4.2.2	Edit.....	99
4.2.3	View .....	99
4.2.4	Tools .....	100
4.2.5	Help Menu .....	100
4.2.6	SQL Batches Dialog .....	100
4.2.7	SQL Execution Dialog.....	101
4.2.8	SQL Errors.....	103

**Appendix A. Glossary ..... 105**

**Appendix B. Application Tokens ..... 111**

- 1. Abstract Layers Tokens..... 112
- 2. AdHoc List Tokens..... 112
- 3. Alarm Banner Tokens ..... 113
- 4. Alarm View Tokens..... 113
- 5. Calculations Tokens ..... 115
- 6. Container Tokens..... 115
- 7. Data Collection Tokens ..... 116
- 8. DataView Tokens ..... 117
- 9. Device Configuration Tokens - HART ..... 117
- 10. Device Templates Tokens..... 117
- 11. Driver Configuration Tokens ..... 118
- 12. Equipment Tokens ..... 118
- 13. Graphics View Tokens ..... 118
- 14. History Editor Tokens ..... 122
- 15. Network Configuration Tokens ..... 122
- 16. Notes View Tokens..... 123
- 17. OE Alarm Client Tokens..... 124
- 18. OEDesktop Tokens..... 127
- 19. Report Selector Tokens ..... 129
- 20. Secure Desktop Tokens..... 130
- 21. Session Manager Tokens ..... 132
- 22. Sites Tokens..... 132
- 23. SQL View Tokens..... 133
- 24. Trend View Tokens..... 134
- 25. Workflows Tokens..... 136

**Index ..... 139**

# 1 Overview

This manual, *Configuring OpenEnterprise Security Reference Guide*, provides an overview of the concepts you use and the tasks you perform to configure security for OpenEnterprise. This manual contains the following chapters:

Chapter	Description
Chapter 1	Provides an overview of the general structure of the manual, describes various formatting considerations, and introduces the concepts of security as they apply to OpenEnterprise.
Chapter 2	Describes the interface and dialogs for the Security Configuration tool.
Chapter 3	Details the tasks you can accomplish using the Security Configuration tool and how to manage the SYSTEM user password.
Chapter 4	Discusses the use of the Security Group Privileges Editor and the use of the Archive File tool, which you use to manage archive files.
Appendix A	Provides a general glossary of OpenEnterprise terms.
Appendix B	Presents a reference of application tokens.

This manual is just one of several manuals describing how to use OpenEnterprise. However, you should always refer to the extensive online help provided with the OpenEnterprise software. It is the most current and is the primary source of information on effectively managing OpenEnterprise.

This chapter provides an overview of the security components in OpenEnterprise and briefly discusses the Security Manager, the Security Configuration tool, and the Security Group Privileges Editor, software tools OpenEnterprise provides to help you configure security.

## 1.1 Security Concepts

At its core, a security system enables you to define who can access what information. To most effectively configure security for your OpenEnterprise system, you need to understand the security system components – users, groups, tokens, access areas, privileges, workstations, and servers – and how they relate to each other.

A properly implemented security policy can help protect your system from accidental changes or deletions to configuration tables or other critical areas of the database. System administrators should establish a security policy for all users of OpenEnterprise Server and OpenEnterprise Workstation(s).

## 1.1.1 Users and Groups

OpenEnterprise draws significant differences between the primary components. There are important differences between *users*, *groups*, and the *Default Group*. (In this manual, *user* is the generic name given to anyone who can log onto an OpenEnterprise workstation.) OpenEnterprise stores users and groups in the Users table, while the OpenEnterprise database treats users and groups as different types of users. The following is a definition of all three security object types.

Term	Description
User	An individual who can log on to OpenEnterprise from a workstation to view and update data. OpenEnterprise assigns users a type 0 (zero) in the database.
Groups	A group is essentially a <i>collection of users</i> having similar security settings. A user group acts like a security template for users. Any user assigned to a parent group inherits the security settings of that group. You can assign each user to only one <b>other</b> group (in addition to their automatic inclusion in the Default Group). All users belong to the Default Group, and may belong to one <b>other</b> group created by an Administrative user (or a “System Administrator”). OpenEnterprise assigns groups a type 1 in the database. <b>Note:</b> OpenEnterprise provides the following pre-defined groups: Administrators, Engineers, Operators, Dispatchers, and Guests. System Administrators can, of course, create additional groups (with appropriate security) to meet your organizations’ requirements.
Default Group	<b>All</b> users – including System Administrators – automatically belong to the Default Group, and automatically inherit the security settings of the Default Group. You cannot remove users from the Default Group. OpenEnterprise assigns the Default Group a type 2 in the database.

Security configuration applies to Users and user groups. It is important to understand how users and user groups relate to each other in OpenEnterprise.

OpenEnterprise applies security to users and user groups in these ways:

- **Through Tokens**

OpenEnterprise uses “tokens” to determine workstation-level security. When associated with users or groups, tokens permit or deny access to specific Human Machine Interface (HMI) functionality. Tokens are required for file access, OPC write



access, built in application context menus, and custom menus. You use the Security Configuration tool to configure token security.

- **Through Access Areas**

Every device, every plant area, and every signal in the OpenEnterprise database belongs to an access area. Access Area security controls what objects within a table a user can view. Users must be granted permission to the access area of an object to view it in the HMI. You use the Security Configuration tool to configure access area security.

- **Through Database Privileges**

Database privilege security grants access to whole tables or views within the OpenEnterprise database. Without privileges and the access they provide, a user can neither see nor manipulate the data within the database. You use the Security Group Privileges Editor (accessed from the Administrative Tools pane on the Container) to configure database privileges for a user in addition to the database privileges the user inherits from its parent user group.

- **Active Directory**

Provides an option to add OpenEnterprise user account linked with an organization's Windows® Active Directory®(AD) user. This re-delegates control of the usernames, passwords, and login for linked users to AD.

## 1.1.2 The Hierarchy of Users and Groups

The security hierarchy of users and groups determines how users and groups acquire (or “inherit”) security account settings.

You configure security account options at any one of the three levels: default, group, and user. When you create a user or a group, it immediately inherits the security account settings of the Default Group. If you assign a user to another group, that user inherits that group's security account settings *in addition to* the security settings for the Default Group. A group may change some settings to suit particular requirements. These override the Default Group settings. Likewise, a user may override its group settings (if it belongs to a group) as well as its Default Group settings.

Figure 1-1. User and Group Hierarchy

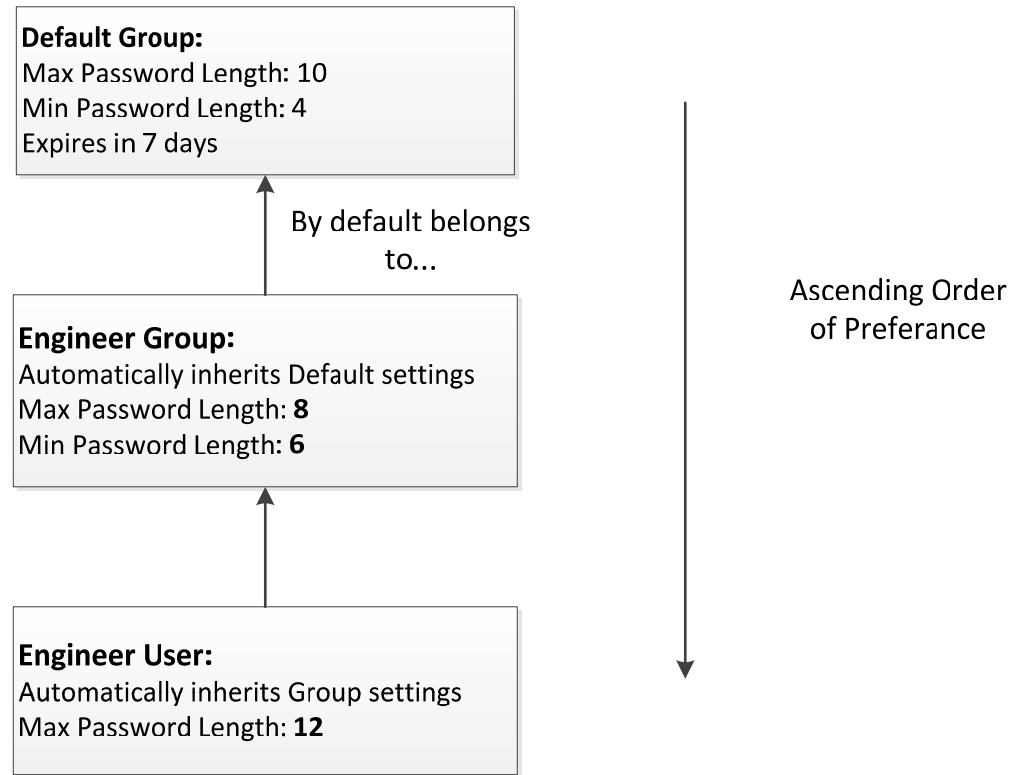


Figure 1-1 shows the hierarchy of user (Engineer User), the additional group to which that user belongs (Engineer Group), and the Default Group to which **all** users belong. This example shows how the user, Default Group, and Engineer Group interact to define password length and expiration.

The Default Group sets a maximum password length of 10 characters, a minimum password length of 7 characters, and a password lifespan of 7 days. The Engineer Group (to which the user belongs) sets a maximum length of **8** characters (2 **less** than the Default Group), a minimum length of **6** characters (2 **more** than the Default Group), and accepts the 7-day lifespan. Finally, the user's settings are a maximum length of **12** characters (overriding both the Engineer Group and Default Group values), a minimum length of **6** characters (using the Engineer Group's values), and a lifespan of 7 days (the value inherited from the Default Group).

**Note**

If a user belongs **only** to the Default Group, the middle group level would not apply.

### 1.1.3 Active Directory Overview

The integration of Microsoft's Active Directory into OpenEnterprise allows you to add an OpenEnterprise user account linked to an Active Directory user account in your organization. This provides:

- Single sign-on for the OpenEnterprise Container and OpenEnterprise Desktop
- Centralized access control
- Improvements to overall security.
- Reduction of user management time and effort.

With this integration, for example, you can disable an OpenEnterprise user account by disabling the corresponding Windows user account.

### Logging on using Credential Mapping

The OpenEnterprise credential mapping functionality can be used to map an OpenEnterprise user to a Windows user to automatically logon to a Workstation using their Windows username. This functionality does not reference the Active Directory and only automatically logs on a user to OpenEnterprise the **first** time the Workstation starts.

The Active Directory functionality automatically logs an OpenEnterprise user onto the workstation or Container using their Windows credentials. This functionality has no connection with the existing credential mapping logon functionality.

---

#### Note

You should remove any user login mappings and use the Active Directory.

---

## 1.2 Tokens

Tokens are tickets or passes that grant a user certain privileges. By adding tokens into a user's Include or Exclude Token list, you can permit (include) or deny (exclude) that user's access to workstation functionality. (Not including a token is functionally the same as explicitly placing a token in the Exclude Token list.) You use the Settings Editor to assign Application, Custom, File, and OPC Item tokens to users and groups.

You can also set up templates for all tokens by creating a new Token Group with the Security Configuration tool. You can then assign these token group templates to users and user groups through the Security Configuration tool's Token Group Property tab. You can still grant individual users extra privileges by using their Application Tokens Tab.

- Application Tokens disable View functions (such as changing to Configure mode).
- Custom Tokens disable Custom Menus or prevent named windows from being closed.
- File Tokens control user access to View files on the workstation.
- OPC Item Tokens control write access to process points on OpenEnterprise Graphical displays.
- Token Groups serve as templates to grant or deny access to a range of View component functions to users or user groups.

### 1.2.1 Application Tokens

Application Tokens define actions that a user may perform within an OpenEnterprise component. System Administrators cannot create or edit application tokens, although they can assign or deny the tokens individually to users or groups. These tokens represent functions available from menu items within the component application, such as the "Acknowledge All" context menu available within the Alarm View component.

For some users, you may find it desirable to remove this option from the Alarm View. To do this, you add this token to the user's Exclude List of Application tokens. Each OpenEnterprise component has its own set of Application Tokens.

### 1.2.2 File Tokens

File tokens are strings that are used to deny access to files on the workstation. The string represents the name of the file.

For example, you can create a file token with the name `*.gdf`. If you place that token in a user's Exclude token list, that user would not be able to load any Graphics View files into the OpenEnterprise Desktop (since graphics files use the file extension `.gdf`).

### 1.2.3 OPC Item Token Types

OPC (Object Linking and Embedding for Process Control) tokens are strings that permit or deny write access to OPC points displayed on the workstation. The string may represent part or all of the OPC string. When representing a part of the OPC string, you must use asterisks as wildcards.

For example, you create an OPC token with the name `*RTU1*` (note the asterisk wildcards at each end of the string), representing the name of an RTU. If the Default user **does not** have any OPC tokens, then all other users or groups must have the OPC token for that RTU specifically granted to them to be able to write to signals belonging to that RTU from a data entry point on a Graphics View display.

If the token were then placed in a user's Include OPC Token list, that user could then change the value of any data entry process points on OpenEnterprise Graphics displays which reference RTU1.

Note that:

- Although a user cannot write to a data entry OPC point without the necessary OPC token, that user can still *view* the point, although it is greyed out and cannot be selected.
- OPC tokens do not affect writes made through the OpenEnterprise Menus Message Bus using the OEOPCDAServer.

### 1.2.4 Custom Tokens

Custom Tokens are strings that can be security protected using tokens. Following are some examples of how you can use custom tokens to provide workstation security.

### 1.2.4.1 Disabling Custom Menus

To disable an OpenEnterprise custom menu for a user, insert a string that matches the name of the custom menu into the Custom Token Excluded list for that user.

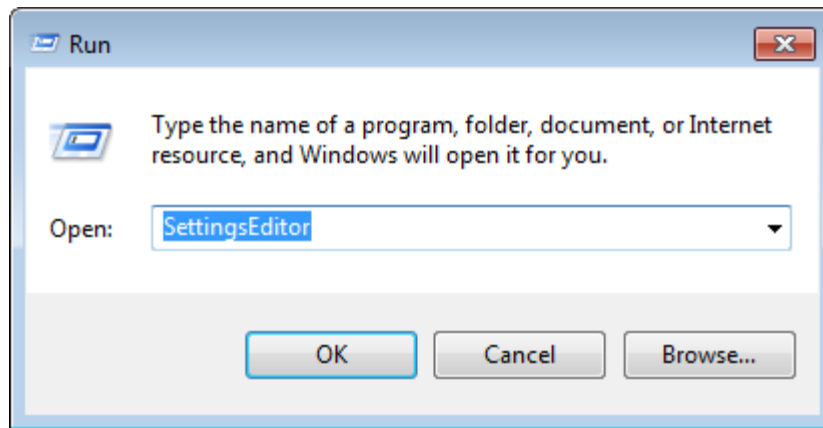
### 1.2.4.2 Disabling Administrative Tools Components

You can disable configuration tools within Administrative Tools on a per-user or per-user group basis by inserting the Editor's Program ID into the Exclude list on the Custom page of the User Properties dialog for a user or user group.

To find the Program ID of an editor, use the Settings Editor application to find the key of that editor under the following key:

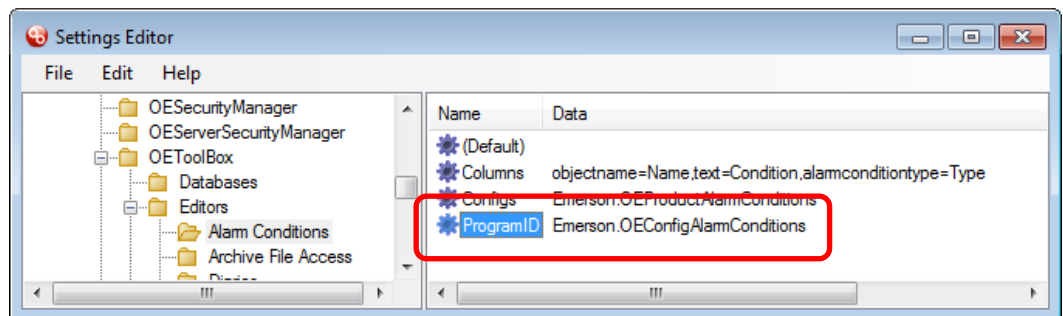
Launch the Settings Editor using the Windows Run dialog.

**Figure 1-2. Window Run dialog**



Each Editor's key has a string value named **ProgramID** (see *Figure 1-3*). Insert this string into the Exclude list for the user or group for which this editor should be excluded.

**Figure 1-3. Settings Editor Program ID string**



String = Emerson.OEConfigAlarmConditions

Inserting the string *Emerson.OEConfigAlarmsConditions* into the Custom Token Exclude list for a user or a group prevents this tool from appearing in the Administrative Tools pane when that user or a member of that group is logged onto a workstation.

---

### Note

You can also remove an editor from appearing on the Administrative Tools pane on a per-workstation basis by first removing its key from under the Editors key (if present) and then removing its ProgramID from the list of editors found in the Editor string value on the Editors key (if present).

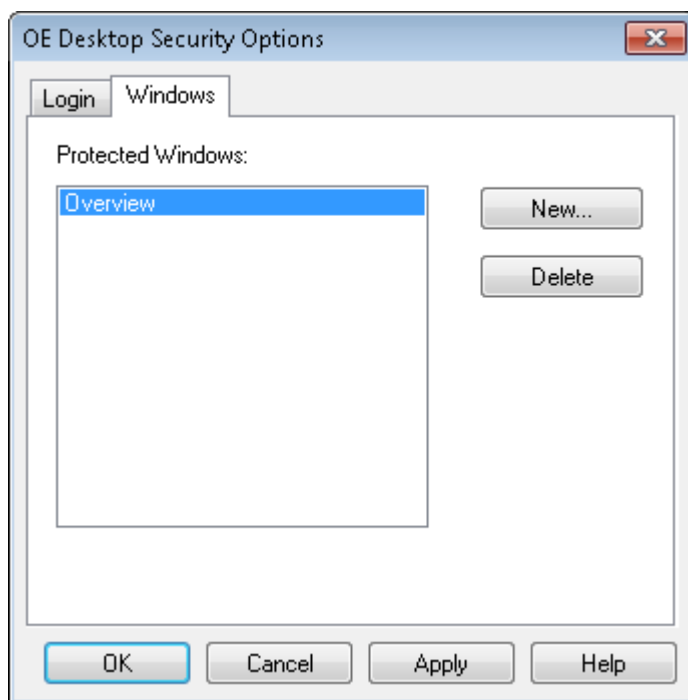
---

### 1.2.4.3 Protecting Windows

You can also prevent users from closing protected windows within the OpenEnterprise Desktop environment. To do this, you must first include the Window name in the Protected Windows list on the Windows tab of the OE Desktop Security Options dialog. Access this list from the **OE Desktop Security > Configure** menu.

---

**Figure 1-4. OE Desktop Security Options dialog – Windows tab**



Once you have defined the window name on the Desktop Security Options dialog (and clicked **Apply** to add that configuration to the database), you then need to enter the name of the protected window in the user's Custom Token Exclude list. Access that list using the Security Configuration tool.

### 1.2.4.4 Token Groups Node



Token Groups

Use the Token Groups node context menu to create new token groups. Refer to the *Creating New Token Groups* online help topic.

**Figure 1-5. Token Groups node context menu**

When you expand the Token Groups node, it displays the Token Group type nodes. For more information on Token Group, refer to the *Token Group Nodes* online help topic..

Token groups are collections of tokens, which can form a token template you can associate with a user or a user group. User-generated token groups may consist of a combination of any of the four types of tokens.

The system also maintains several special groups of Application tokens that are grouped by their component name (OpenEnterprise Alarm Banner, OpenEnterprise Alarm Client, OpenEnterprise Alarm Printer, OpenEnterprise Desktop, OpenEnterprise Graphics, OpenEnterprise Notes Client, OpenEnterprise SQL Viewer and OpenEnterprise Trend Client) and are maintained independently of the system administrator. You cannot edit these token groups.

## 1.2.5 Token Wildcards

Individual token types (with the exception of Application Tokens and Token Groups) may contain wildcard characters, defined by an asterisk (\*) or a question mark (?). The asterisk is a multiple-character wildcard, and the question mark is a single character wildcard.

## 1.2.6 Token Pattern Matching

At runtime, the system compares the strings present in the Include and Exclude lists for each active user and group until access is denied. The comparison uses the following sequence:

1. The Token string is compared with each string in the Include list until a match is found. If no match is found, access is denied.
2. If a match is found in the Include list, the token string is compared with every string in the Exclude list. If no match is found in the Exclude list, access to the point is granted, and no further testing of active groups and users occurs.

---

### Note

An Exclude list may only **remove** rights granted in the same item's corresponding Include list. For example if user Larry belongs to the Operators group and the Operators groups grants access to OPC point "xyz," **adding** point "xyz" to Larry's Exclude list has no effect.

---

### 1.2.6.1 Wildcards and Charlists

The entries in the Include and Exclude lists allow pattern matching to provide a versatile tool for string comparisons. The pattern-matching features allow you to use any combination of wildcard characters, character lists, or character ranges to match strings.

The following table shows the characters allowed in patterns and what they match:

Character(s) in pattern	Matches in string
?	Any single character
*	Zero or more characters
#	Any single digit (0 - 9)
[charlist]	Any single character in charlist
[!charlist]	Any single character not in charlist

A group of one or more characters (charlist) enclosed in brackets ( [ ] ) can be used to match any single character in string and can include almost any character code, including digits.

---

### Note

The special characters left bracket ([), question mark (?), number sign (#), and asterisk (\*) can be used to match themselves directly only by enclosing them in brackets. The right bracket (]) can't be used within a group to match itself, but it can be used outside a group as an individual character.

---

In addition to a simple list of characters enclosed in brackets, charlist can specify a range of characters by using a hyphen (-) to separate the upper and lower bounds of the range. For example, [A-Z] in a pattern results in a match if the corresponding character position in string contains any of the uppercase letters in the range A through Z. Multiple ranges are included within the brackets without any delimiters.

The meaning of a specified range depends on the character ordering valid at run time (as determined by the locale setting of the system the code is running on). The range [A - E] matches A, a, À, à, B, b, E, e. Note that it does not match Ê or ê because accented characters fall after unaccented characters in the sort order.

Other important rules for pattern matching include the following:

- An exclamation point (!) at the beginning of charlist means that a match is made if any character except the ones in charlist is found in string. When used outside brackets, the exclamation point matches itself.
- The hyphen (-) can appear either at the beginning (after an exclamation point if one is used) or at the end of charlist to match itself. In any other location, the hyphen is used to identify a range of characters.
- When a range of characters is specified, they must appear in ascending sort order (from lowest to highest). [A-Z] is a valid pattern, but [Z-A] is not.
- The character sequence [ ] is ignored: it is considered a zero-length string.

## 1.2.6.2 File Tokens

The runtime processing and wildcard pattern matching for the Point Property Page apply here as well with the following differences:

- The pattern matching is done on the file extension, separate from the file name to match the DOS wildcard semantics. For example the wildcard string to indicate all files is “ \*.\* ” (two asterisks separated by a period).



- A match is considered to have occurred if both the file name and extension match the given pattern.
- File names entered without a path are considered a match no matter what directory they are in.

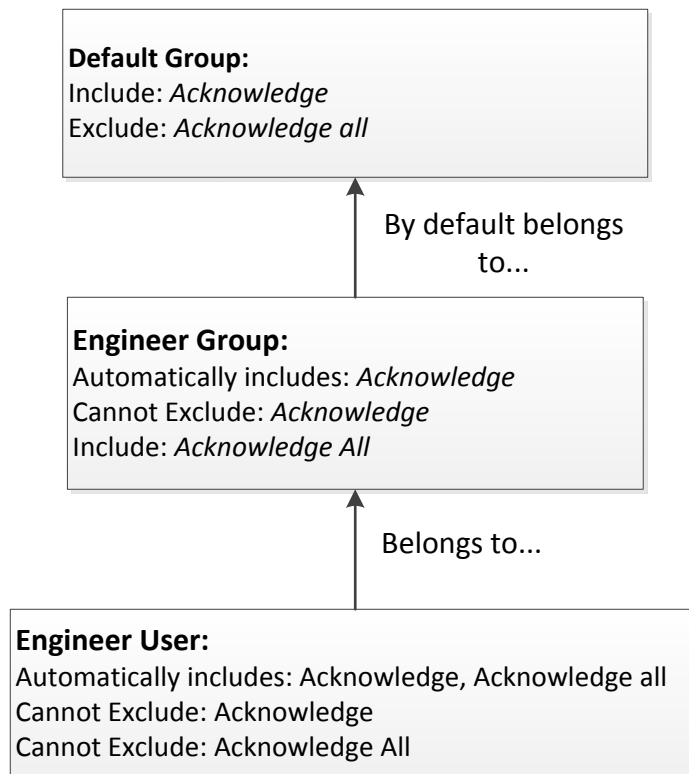
## 1.2.7 Token Security Hierarchy

This differs significantly from user and group security hierarchy in that what is included at one level may **not** be overridden by being excluded at a different level. There are two rules to remember when configuring OpenEnterprise component security:

- Everyone inherits from the Default Group. Users belonging to another group also inherit settings from that group.
- What is included at one level cannot be excluded at a different level.

Refer to *Figure 1-6*.

**Figure 1-6. Token Security Hierarchy diagram**



### 1.3 Access Areas

Each object has an associated Access Area. You use the AccessArea table to grant or deny each user the appropriate Access Areas for their operational needs. Users can only access objects belonging to the Access Areas which they have been granted access.

The system creates database views and provides this access when the user logs onto the workstation. Database views have the same name as the table from which they were created, but do not have the "\_table" extension. These database views include only those objects to which the logged in user has access, according to the AccessArea table. To complete the implementation, all the Workstation View components (for example Trend View, Alarm View) are configured to retrieve objects from the database *views*, rather than the tables.

### 1.4 Database Privileges

Database privileges on tables (read-only or read-write) are granted to user groups through a special configuration editor called the Security Privileges Editor. You can access this Editor either from the User Properties dialog or from the Administrative Tools pane.

You must create user groups before the Security Privileges Editor can work effectively. The OpenEnterprise database contains the following pre-defined groups, which meet most functional requirements. Of course, this does not prevent you from creating other groups to meet your organization's unique requirements.

- **Administrators**  
Have unrestricted access to all OpenEnterprise functionality.
- **Engineers:**  
Require configuration access to all system features except those related to controlling security privileges of other users.
- **Operators:**  
Require the abilities to change set points, to acknowledge alarms, and to perform basic **workstation** configuration (but have no need to perform Server configuration).
- **Dispatchers:**  
Require read-only access to all operational and process data. They are not required to change set points.
- **Guests:**  
Require read-only access to all operational and process data. Guests are not required to change set points.

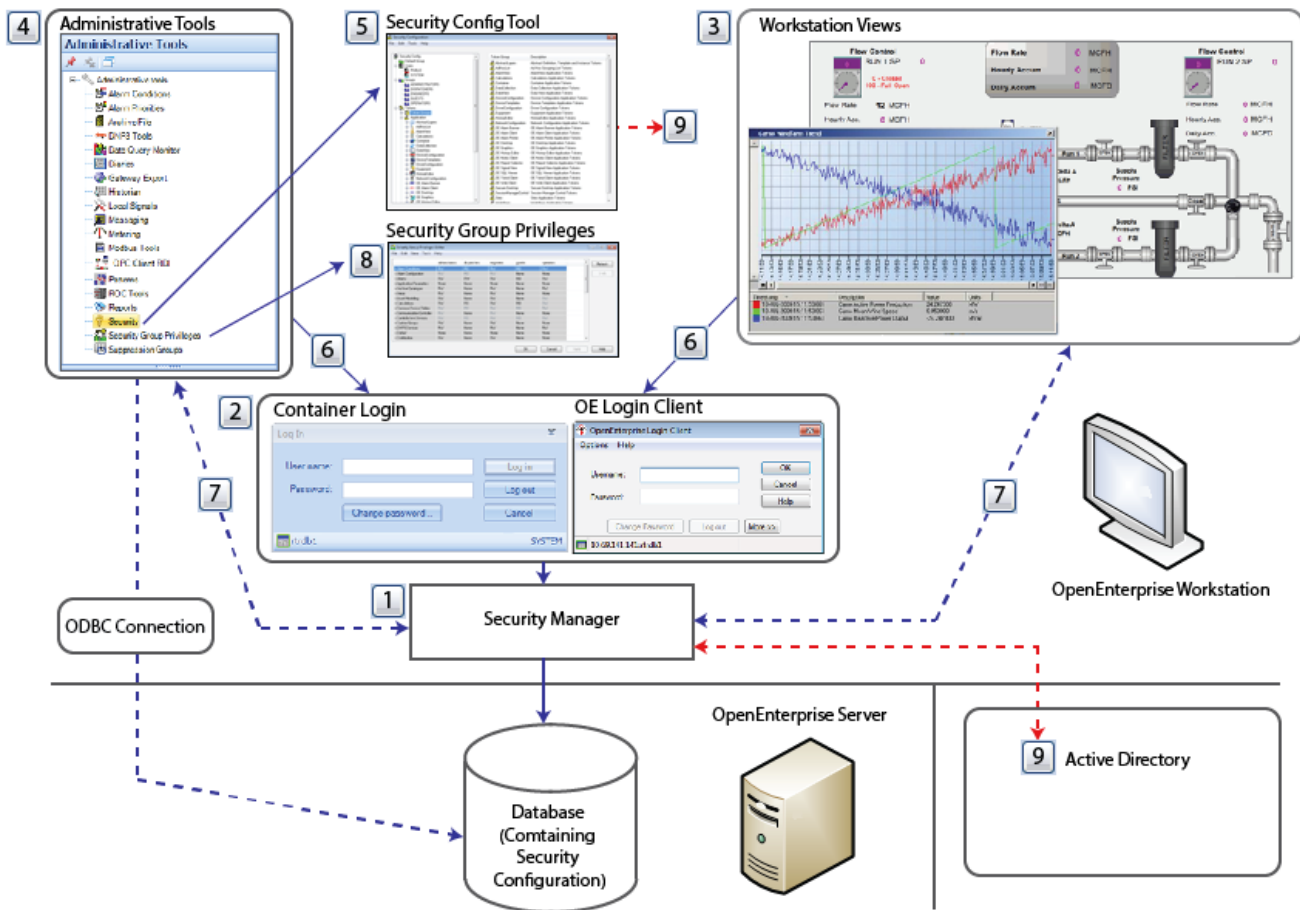
Finally, you assign Users to a user group so they can inherit the privileges appropriate to their required level of access.

## 1.5 Security Manager

The Security Manager is a background application that manages all aspects of user runtime security. The Security Manager acquires user account details for the currently logged in User from the database. It also informs the Workstation View components about the logged-in user's Security Token privileges, such as Application, File, OPC Item, and Custom Tokens.

Figure 1-7 shows how you implement security between the OpenEnterprise server and workstation.

Figure 1-7. OpenEnterprise Security Overview



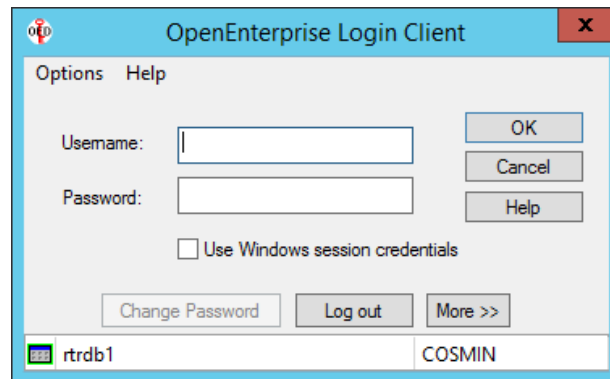
- 1 Security Manager: a background application that manages all aspects of user runtime security. The Security Manager acquires user account details for the currently logged in user from the database. It also informs the Workstation View components about the logged-in User's Security Token privileges, such as Application, File, OPC Item, and Custom Tokens.
- 2 Container login
- 3 Workstation view: Application tokens assigned to a user control what functionality is available to the User.

- 4 Administrative Tools: Security ensures that Users can see only the menus for which they have string token access.
  - 5 Security Configuration Tool: an OpenEnterprise configuration editor accessed from the Administrative Tools pane, and accessible only by System Administrators.
  - 6 OE Login Client: access is provided from the Security menu of the OpenEnterprise Container or from the workstation login client. The Security Manager applies all aspects of workstation and Container security.
  - 7 Security Settings applied: the Security Manager applies security settings to the OpenEnterprise HMI and the Administrative Tools pane.
  - 8 Security Group Privileges: the Security Group Privileges Editor enables System Administrators to set table or view privileges for user groups.
  - 9 Active Directory in OpenEnterprise allows you to add an OpenEnterprise user account linked to a Microsoft Windows Active Directory user account in your organization.
- 

### 1.5.1 Workstation Login Client

Select **All Programs > Emerson OpenEnterprise > Workstation > Login**. The system displays the Workstation Login Client dialog.

**Figure 1-8. Workstation Login Client**



This dialog enables a user to log into OpenEnterprise from a workstation. The Login Client dialog connects to the Security Manager. The user can also click **Change Password** to change their password through this dialog.

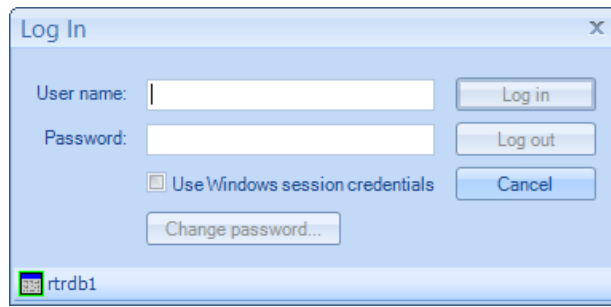
The **Use Windows session credentials** is used with Active Directory; see. *Logging in to OpenEnterprise*.

### 1.5.2 Container Security Login

You use the Container Security Log In dialog to enable a user at an OpenEnterprise Container to log on to OpenEnterprise. Users can also click **Change password** to change their password at the Container Login.

---

**Figure 1-9. Container Security Log In**



### 1.5.3 Security and Workstation Views

The Security Manager directly provides all Workstation View components with application token information. The application tokens assigned to a user control what functionality is available to that user when using these components.

### 1.5.4 Security and Administrative Tools

To access the Administrative Tools editors, Users must login using the Container Login which can be invoked from the Security menu of the Container or at launch. Once the user is logged in, security ensures that users are only able to see the editors context menus in the Administrative Tools window for which they have the necessary String Token access.

### 1.5.5 The Security Configuration Tool

The Security Configuration tool is one of the OpenEnterprise configuration editors that are accessed from the Administrative Tools pane. Only SYSTEM users can access and use the Security Configuration tool.

### 1.5.6 Access to OpenEnterprise Login dialogs

Login access is provided from the Security menu of the OpenEnterprise Container or the Workstation Login client; all aspects of Workstation and Container security are applied through the Security Manager.

### 1.5.7 Applied Security Settings

Security settings are applied to the OpenEnterprise HMI and the Administrative Tools via the Security Manager.

### 1.5.8 Security Group Privileges Editor

The Security Group Privileges Editor enables Administrative users to set table or view privileges for user groups.

### 1.5.9 Security Manager User Interface

The Security Manager component provides security on an OpenEnterprise Workstation. It starts automatically when you start any OpenEnterprise component. Once started, it remains running until the Workstation closes down.

The Login Client passes login requests to the Security Manager, which then negotiates the login request to the database. The Security Manager then informs all OpenEnterprise Workstation components (Desktop, Views, and Toolbox) of the current user's security status.



While running, the Security Manager displays an icon in the system tray. The color of the border of that icon visually indicates the Security Manager's database connectivity status:

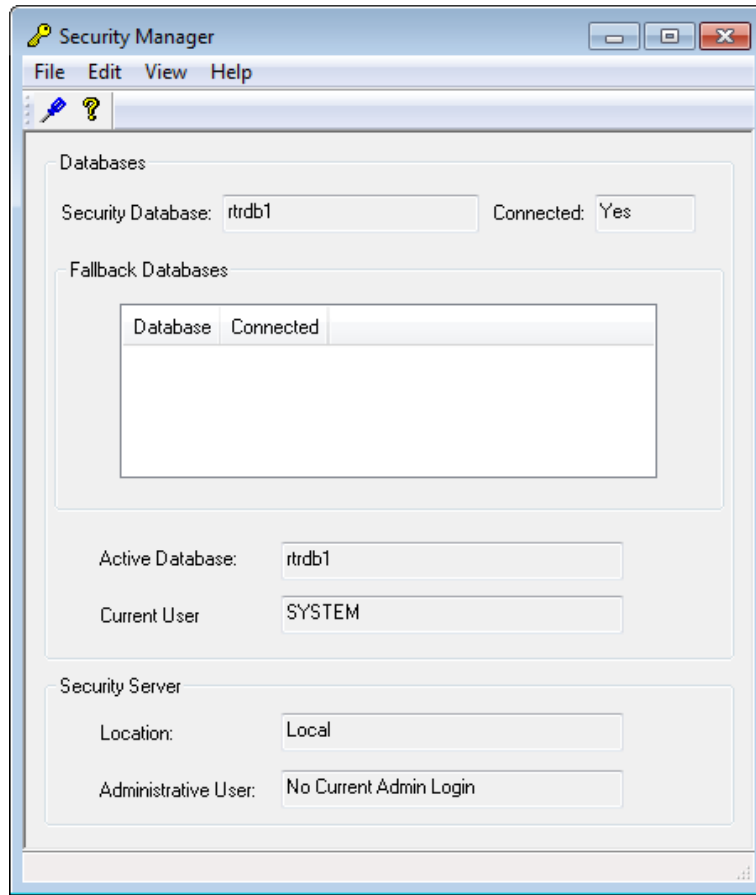
- A green border indicates that the Security Manager is connected to the Security Configuration database.
- A blue border indicates that the Security Manager is currently connected to one of the fallback databases.
- A yellow border indicates that the Security Manager is using its internal cache to satisfy the workstations' security requirements.
- A red border indicates that the Security Manager never managed to connect to either the Security Configuration database or any fallback databases.

Double-click the Security Manager icon to open its User Interface (UI). This provides information and the ability to configure the behavior of the UI.



#### 1.5.9.1 Main Dialog

The Security Manager provides information concerning its connectivity to the designated security database and any fallback database that may have been configured. It also displays the name of any currently logged in user, the location of the Security Manager, and the Administrative user being used by the Security Manager to obtain security information.

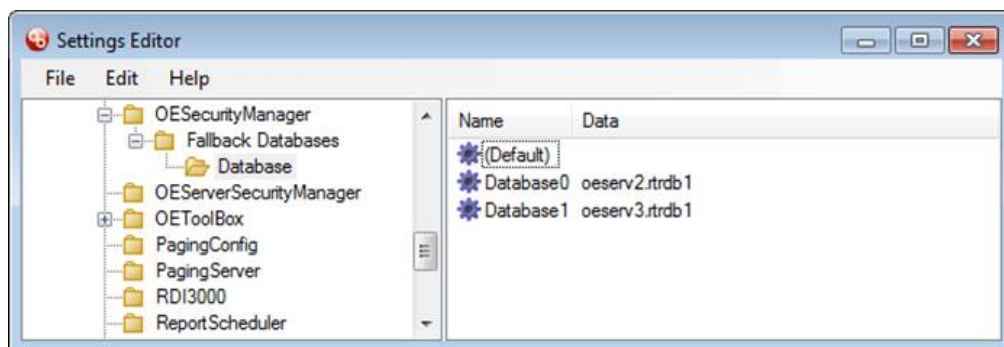
Figure 1-10. Security Manager dialog



Option	Description
File Menu	Exits the application, which closes the application as a Windows process if the Security Manager is not currently supplying data to a client. If the Security Manager is supplying data, it hides but remains a running process. To redisplay the User Interface, double-click its icon in the system tray.
Edit Menu	Opens the Properties dialog, which you use to configure pre-connected databases and the behaviour of the User Interface.
View Menu	Provides two options: Toolbar (which when selected displays a toolbar under the Menu) and Status Bar (which when selected displays a status bar at the bottom of the Main Dialog window, showing the current status of the Security Manager).
Help Menu	Opens the About dialog, which provides information on the version and build of OpenEnterprise being used as well as contact information.
Toolbar	Provides two utility icons

Option	Description
	Opens the Security Manager Properties dialog.
	Opens the About dialog, which provides information on the version and build of OpenEnterprise being used and contact information.
Security Database	<p>Identifies the default Security Database (rtrdb1). This is the default Security Database. It is stored in the data for the <i>Database</i> value, found on the <i>OpenEnterprise\Tasks\OESecurityManager</i> key in the OpenEnterprise settings file. OpenEnterprise defines this value during the installation process. You can view this key and its value with the Settings Editor, although it should normally never be changed.</p> <p>The Security Manager always attempts to connect to this database first to retrieve security information. If the database is unavailable, the Security Manager then attempts to connect to any of the configured fallback databases. If none of these databases is available and the Security Manager has previously run, it uses its internal cache to provide security information.</p>
Fallback Databases	<p>Displays a list of all configured fallback databases, along with their connection status. You must manually configure any fallback database by creating a new key under the <i>OpenEnterprise\Tasks\OESecurityManager</i> settings key. You can view and modify this key with the Settings Editor.</p> <p>You must name the new key <i>Fallback Databases</i>. Then create another key under this called <i>Database</i>. On this key, create the string values <i>Database0</i>, <i>Database1</i>, <i>Database3</i>, and so on. The Value data should contain the data source string for each fallback database (such as <i>oeserv3:rtrdb1</i>). <i>Figure 1-11</i> shows an example.</p>


**Figure 1-11. Settings Editor – Fallback Databases**



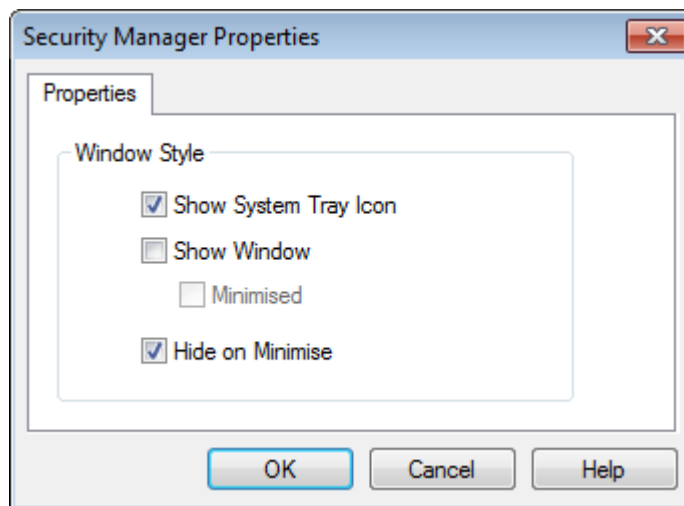



Option	Description
Connected	Indicates the connection status of the Security Manager to the defined Security database.
Active Database	Displays the currently active database that the Security Manager is currently using for security information.
Current User	Displays the user currently logged onto OpenEnterprise on the workstation.
Location	Indicates the Iconics Security Server, which usually runs on a local machine. Thus, the usual value for this field is <b>Local</b> . The Workstation Security Manager updates the Iconics Security Server with security information on the logged in user. The Iconic Security Server then uses this information to control access to functions and objects within OpenEnterprise graphics.
Administrative User	Identifies the Administrative user (OpenEnterprise System Administrator) the Security Manager is using to log onto the Iconics Security Server to provide security information for OE graphics.

### 1.5.9.2 Properties Dialog

Click  on the Toolbar to open the Security Manager’s Properties pane. You use this dialog to configure the behaviour of the Security Manager’s User Interface. OpenEnterprise applies any changes to make on this dialog when you click **OK** (at the bottom of the dialog).

**Figure 1-12. Security Manager Properties dialog**



Option	Description
Show System Tray Icon 	Displays the Security Manager icon in the Windows System Tray (at the lower right corner of the screen) whenever the Security Manager is running.

## Configuring OpenEnterprise Security

D301796X012

September 2017

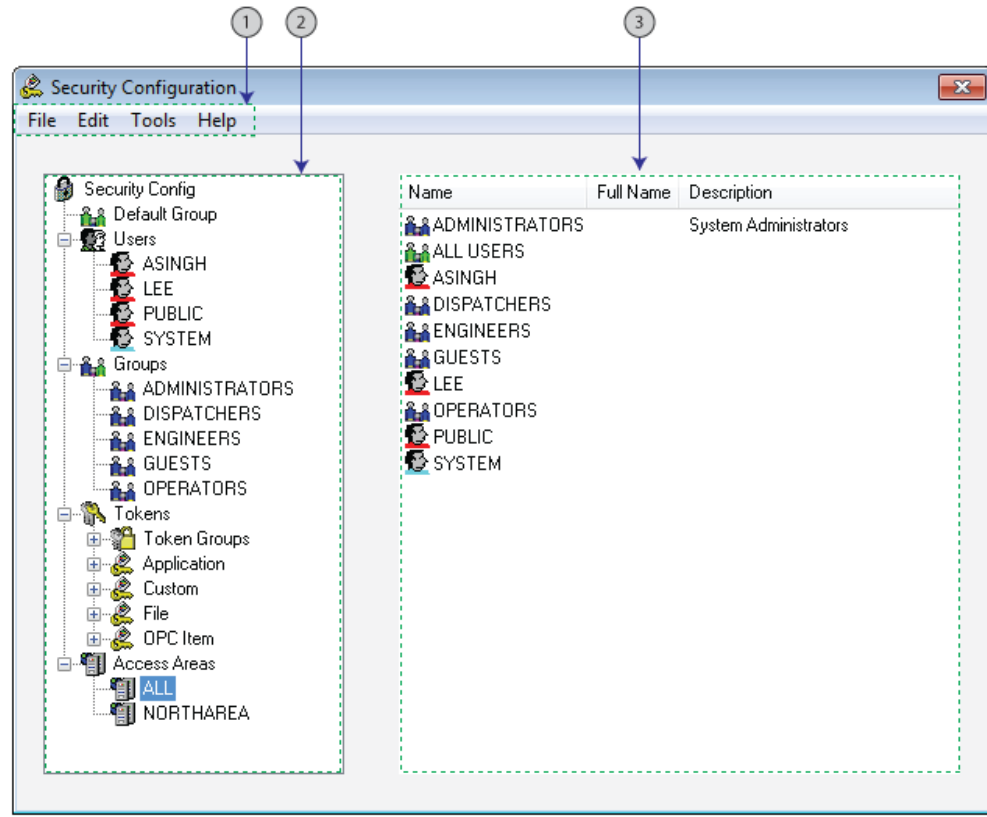
Option	Description
	Double-clicking this icon opens the Security Manager's User Interface.
Show Window	Displays the Security Manager's User Interface on system startup.
Minimised	Displays the Security Manager's User Interface as a minimised icon on the Windows task bar. The system activates this option <b>only</b> if you select the Show Window option.
Hide on Minimise	Hides the minimized Security Manager's User Interface. If you select this option, the system hides the User Interface when you minimize it. <b>Note:</b> To show the Security Manager's User Interface at startup, select the Show System Tray <b>and</b> the Show Windows options at the time you select this option. If the User Interface is not shown at startup, you can restore the Interface. Use the Settings Editor to manually change the <i>ShowtrayIcon</i> value on the <i>OpenEnterprise\Tasks\Notes Client Server</i> key to 1. You also need to restart the system for the changes to take effect.
OK	Click to close the dialog; the system sends any configuration changes to the database.
Cancel	Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.
Help	Click to access the online help system for OpenEnterprise.

## 2 Security Configuration Tool

This chapter describes the Security Configuration tool and the various dialogs you use to configure OpenEnterprise security.

Figure 2-1 shows the main Security Configuration tool screen. As an OpenEnterprise System Administrator, you use it to configure all aspects of OpenEnterprise security. The screen has three major sections: Menu bar (1), Tree pane (2), and List pane (3).

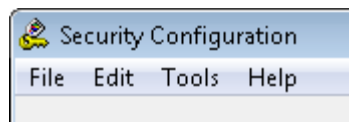
**Figure 2-1. Security Configuration tool main interface**



### 2.1 Menu Bar

The Security Configuration tool's menu bar provides access to the following functions.

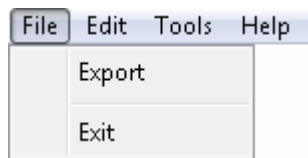
**Figure 2-2. Security Configuration tool menu bar**




## 2.1.1 File Menu

This menu contains two options, Export and Exit.

**Figure 2-3. Security Configuration tool File menu**

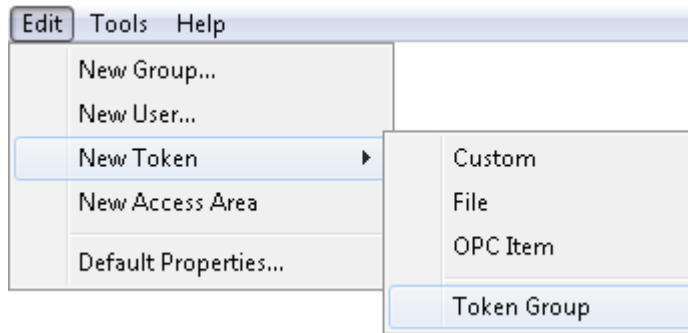


Option	Description
Export	Enables you to save the Security Configuration for the current database to an SQL script file, which you can then use later to restore your security settings (should that prove necessary). When you select <b>Export</b> from the drop-down menu, the system displays the Security Export dialog (also known as the SQL Import-Export File dialog). This enables you to use the default SQL export file or select another file. Once the system completes the export, it displays a information dialog:
	
	Click <b>Close</b> to exit this dialog.
Exit	Closes the Security Configuration tool.

## 2.1.2 Edit Menu

The options on this menu enable an **OpenEnterprise System Administrator** to create new groups, Users, tokens, token groups, and access areas, and to edit settings for the Default Group.

**Figure 2-4. Security Configuration Tool Edit menu**

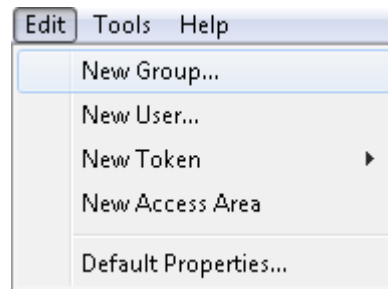


### 2.1.2.1 Creating a User Group

You can create a new **group** using any of the following methods:

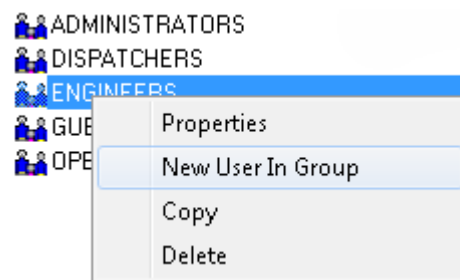
- Select **Edit > New Group** from the Security Configuration tool menu bar.

**Figure 2-5. Security Configuration Tool Edit menu –New Group**



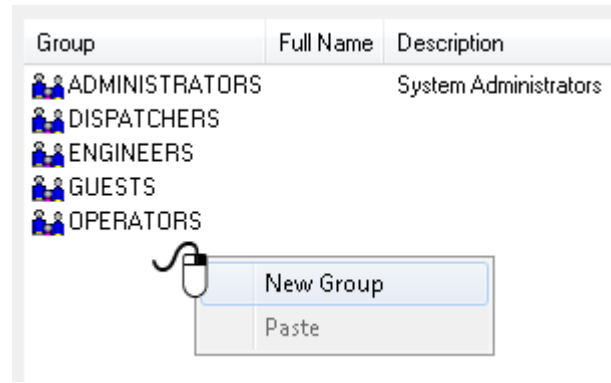
- Select the **New User In Group** menu item from the tree pane.

**Figure 2-6. Security Configuration Tool Edit menu –New User in Group**



- Right-click the Groups node in the Tree pane and select the **New Group** option from the context menu.

**Figure 2-7. New Group floating context menu**



Once you select **New Group**, the List pane displays all the currently configured groups and inserts a new blank entry at the top of the list. Enter a valid name and press the **Enter** key. The system displays the Group Properties dialog, which allows further configuration.

### Note

Once you enter the new Group name, you cannot change it.

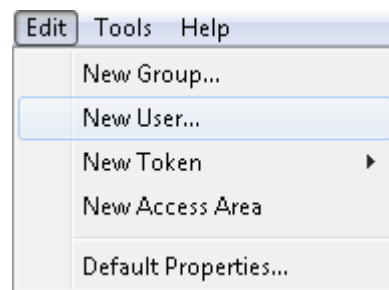
## 2.1.2.2 Creating a User

You can optionally add an OpenEnterprise user linked to the Windows Active Directory. This section describes how to add a new OpenEnterprise user that is **not** linked to Active Directory. See *Creating a New User linked to Active Directory*.

You can create a new **user** using any of the following methods:

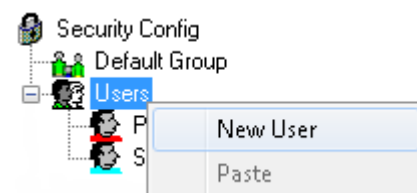
- Select **Edit > New User** from the Security Configuration tool’s menu bar.

**Figure 2-8. Security Configuration tool Edit menu –New User**



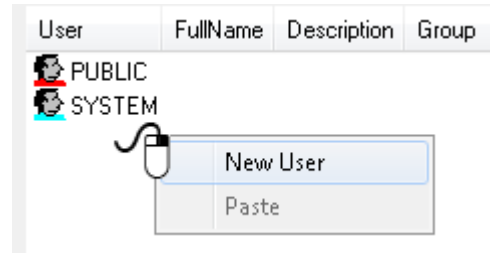
- Right-click the Users icon in the tree pane to display the New User context menu.

**Figure 2-9. New User context menu**



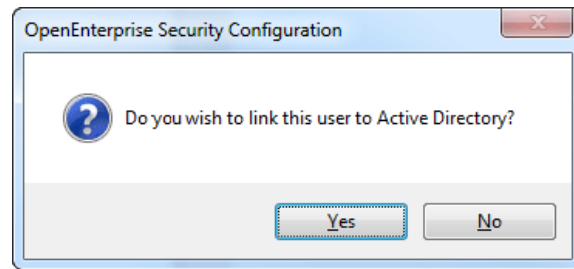
- Right-click in the list pane to display the **New User** floating context menu.

**Figure 2-10. New User floating context menu**



The prompt to link the new OpenEnterprise user to the AD displays:

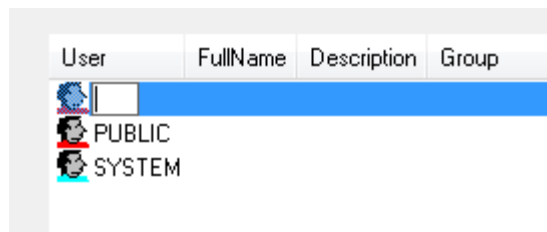
**Figure 2-11. Do you wish to link this user to AD message**



- Click **No**.

Once you select **New User**, the List pane displays all the currently configured users and inserts a new blank entry at the top of the list.

**Figure 2-12. New User with a new blank entry inserted**



Enter a valid name and press the **Enter** key. The system displays the User Properties dialog, which allows further configuration.

**Note**

Once you enter the new user name, you cannot change it.

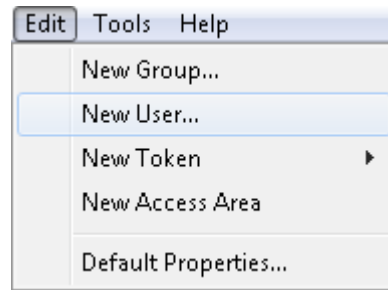
### 2.1.2.3 Creating a New User Linked to Active Directory

You can Link a new OpenEnterprise user to the Active Directory (AD) when you create a new user using the Security Configuration tool.

You can create a new user using any of the following methods:

- Select **Edit > New User** from the Security Configuration tool's menu bar.

**Figure 2-13. Security Configuration tool Edit menu –New User**



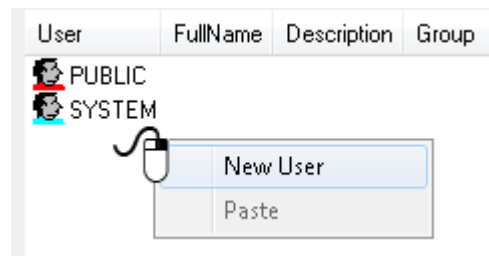
- Right-click the Users icon in the tree pane to display the New User context menu.

**Figure 2-14. New User context menu**



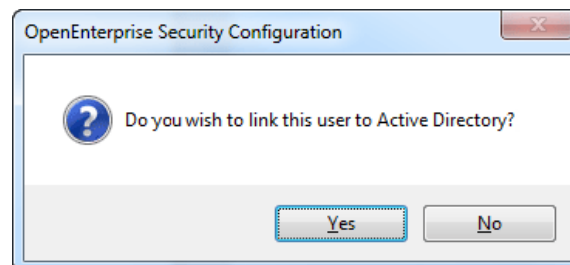
- Right-click in the list pane to display the **New User** floating context menu.

**Figure 2-15. New User floating context menu**



The prompt to link the new OpenEnterprise user to the AD displays:

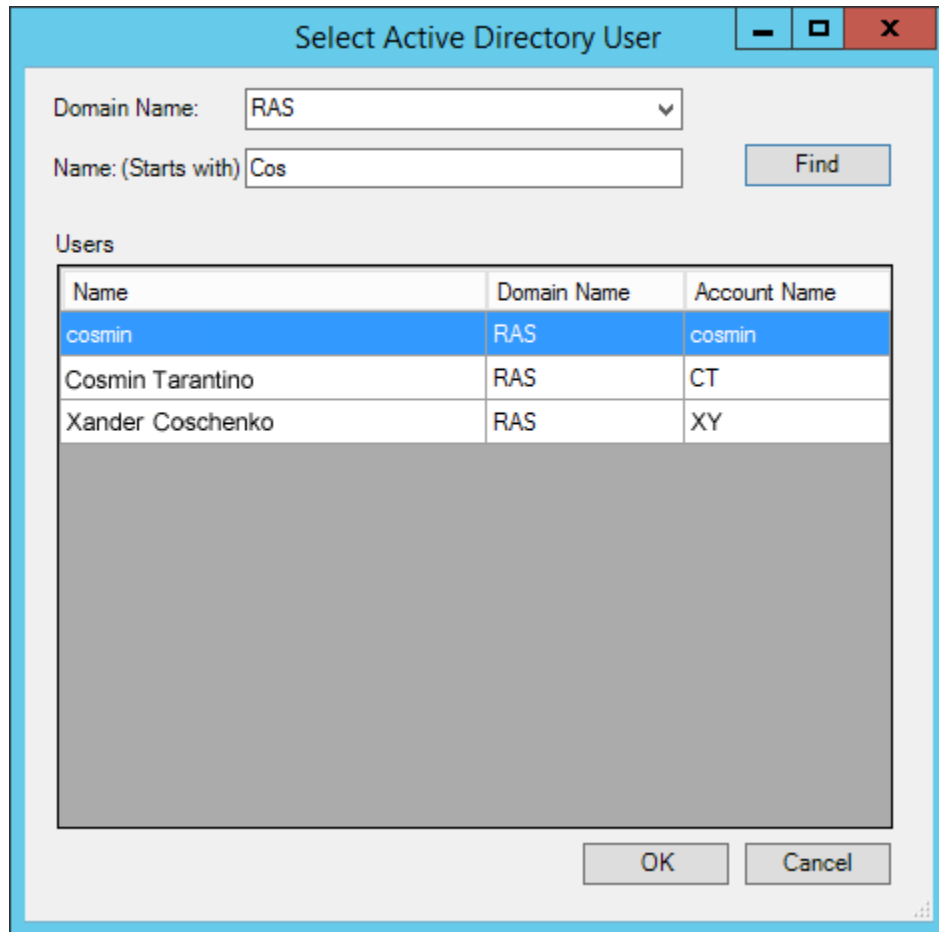
**Figure 2-16. Do you wish to link this user to AD message**



- Click **Yes**; the **Select Active Directory User** dialog displays.

You can perform a search for a user in the Active Directory (AD) Domain using the Select Active Directory User dialog.



**Figure 2-17. Select Active Directory User dialog**

The dialog displays all AD users that have a surname and/or forename beginning with the partial username entered irrespective of case. For example, entering a partial name of “jack” displays the AD users “Jack Smith” and “Bob Jackson.”

AD user names must comply with the following format rules.

- Must begin with a letter (a-z, A-Z).
- May only contain characters a-z, A-Z, 0-9 or \_ (underscore).

---

**Note**

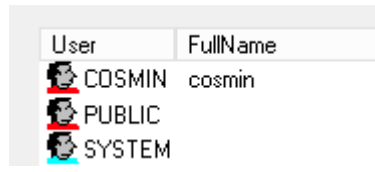
This form **does not** display any disabled AD user accounts.

---

You can link only one OpenEnterprise user to an AD user. The system generates an error message if the username and domain is already linked to an existing OpenEnterprise user. OpenEnterprise users cannot be unlinked from AD. To break the link, you must delete and then re-add the OpenEnterprise user.

The List pane displays all the currently configured users and inserts a new entry at the top of the list.

**Figure 2-18. New User linked to Active Directory**



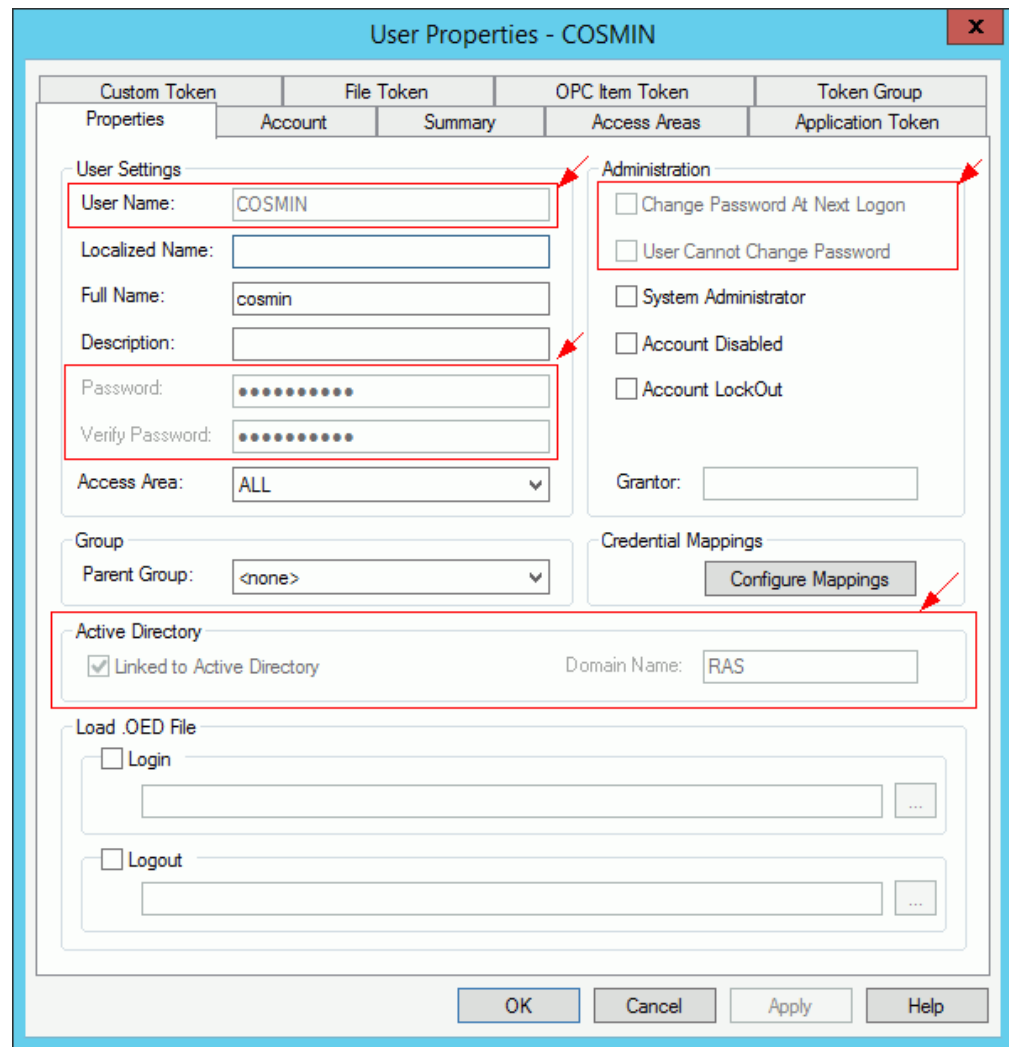
AD manages the username and password. The system displays the User Properties dialog, which allows further configuration.

## 2.1.2.4 Managing OpenEnterprise Users and Active Directory

Open the Security Configuration tool, right-click on a user and select **Properties** from the context menu.

Active Directory is used to manage the properties highlighted in the image below.

**Figure 2-19. User Linked to Active Directory - User Properties**



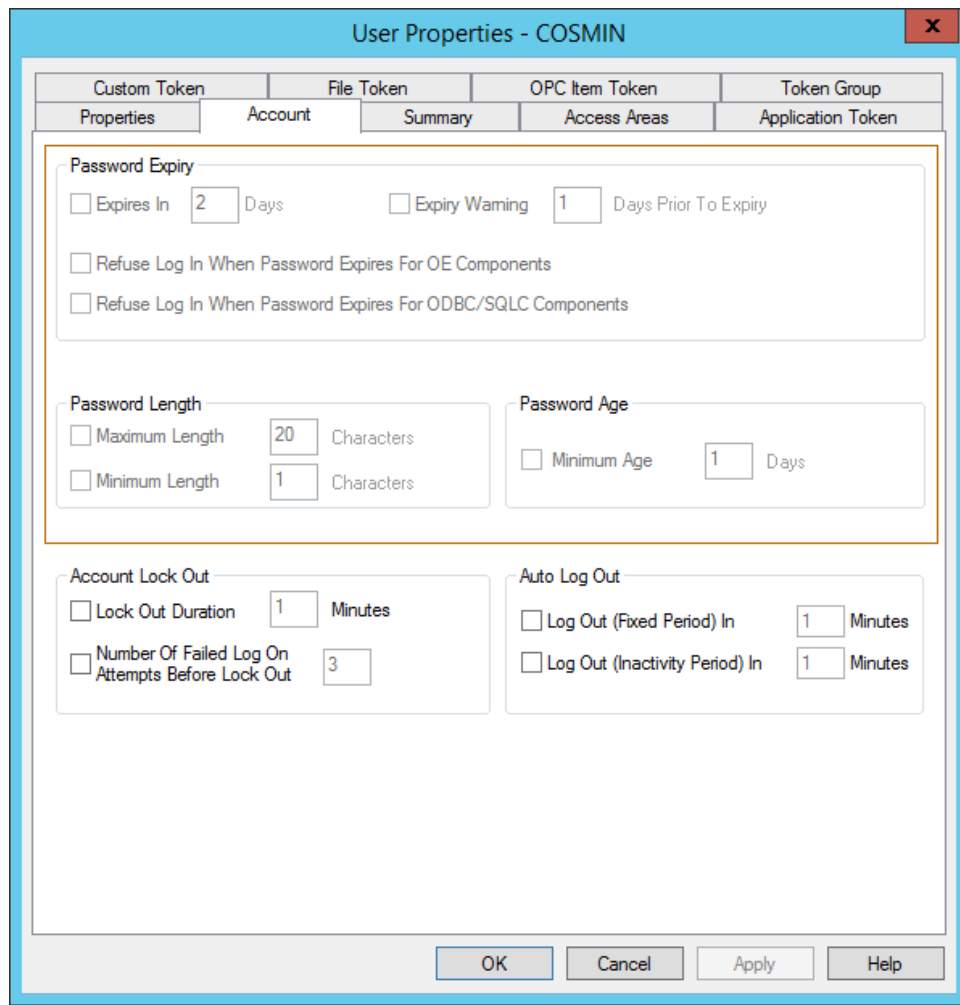
### User Properties - Account Settings

From the **User Properties > Account** tab you can configure **only** the *Account Lock Out* and *Auto Log Out* settings.

The system grays out the Password Expiry and Password Length sections of the Account tab when a user is linked to the AD.

Windows AD defines and manages password policies.

**Figure 2-20. User Linked to Active Directory – Account Tab**

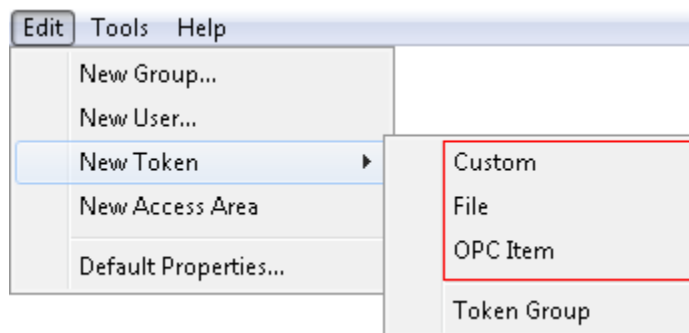


### 2.1.2.5 Creating Tokens (Custom, File, and OPC Item)

You can create Custom Tokens, File Tokens, and OPC Item Tokens using any of the following methods:

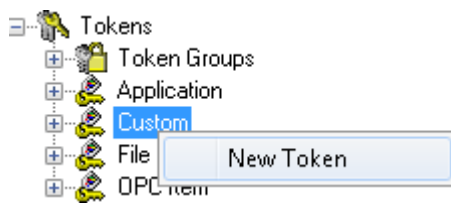
- Select **Edit > New Token** from the Security Configuration tool’s menu bar. Then select the desired option (**Custom**, **File**, or **OPC Item**) from the sub-menu.

**Figure 2-21. Security Configuration tool Edit menu –New Token**



- Right-click a token node and select **New Token** menu item from the expanded Tokens node in the Tree pane.

**Figure 2-22. Token node menu**



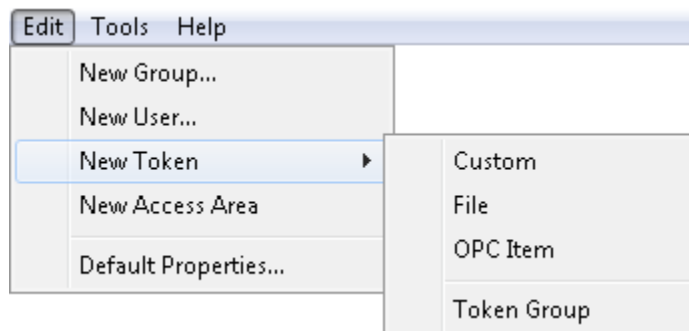
Once you select this menu item, the system completes the List pane with all the currently configured Token Groups, and inserts a new entry with a blank name at the top of the list. Enter a valid and unique name for the new custom token group and press the **Enter** key. The system displays the Token Properties dialog for the kind of token you have selected. Use it for further configuration.

## 2.1.2.6 Creating New Token Groups

You can create a new **token group** using any of the following methods:

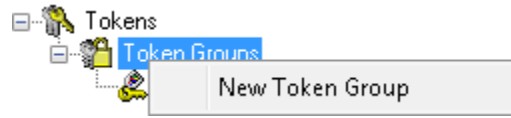
- Select **Edit > New Token > Token Group** from the Security Configuration tool’s menu bar.

**Figure 2-23. Security Configuration tool Edit menu –New Token menu**



- Select the **New Token Group** menu item from the expanded Tree pane:

**Figure 2-24. Token Group node menu**



Once you select this menu item, the system completes the List pane with all of the currently configured Token Groups, and inserts a new entry with a blank name at the top of the list. Enter a valid and unique name for the new token group and press the **Enter** key. The system displays the Token Group Properties dialog, which allows further configuration.

**Note**

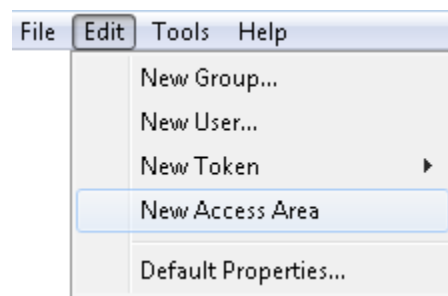
Once you have entered the name for the new token group, you cannot edit it later.

### 2.1.2.7 Creating New Access Areas

You can create a new **access area** using any of the following methods:

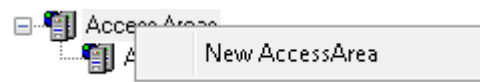
- Select **Edit > New Access Area** from the Security Configuration tool’s menu bar.

**Figure 2-25. Security Configuration tool Edit menu –New Access Area**



- Right-click the Access Area node to display the **New Access Area** content menu.

**Figure 2-26. Access Area node menu**



Once you select this menu item, the system completes the List pane with all of the currently configured access areas, and inserts a new entry with a blank name at the top of the list. Enter a valid and unique name for the new access area and press the **Enter** key. The system displays the Access Area Properties dialog, which allows further configuration.

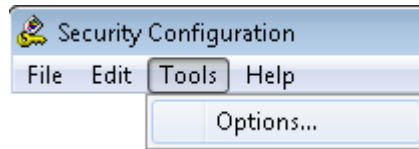
**Note**

Access Area names are case-sensitive and must be unique within Access Areas only.

## 2.1.3 Tools Menu - Options

You use this menu to configure the behaviour of certain functions within the Security Configuration tool.

**Figure 2-27. Security Configuration tool Tools menu –Options**



## 2.1.4 Help Menu

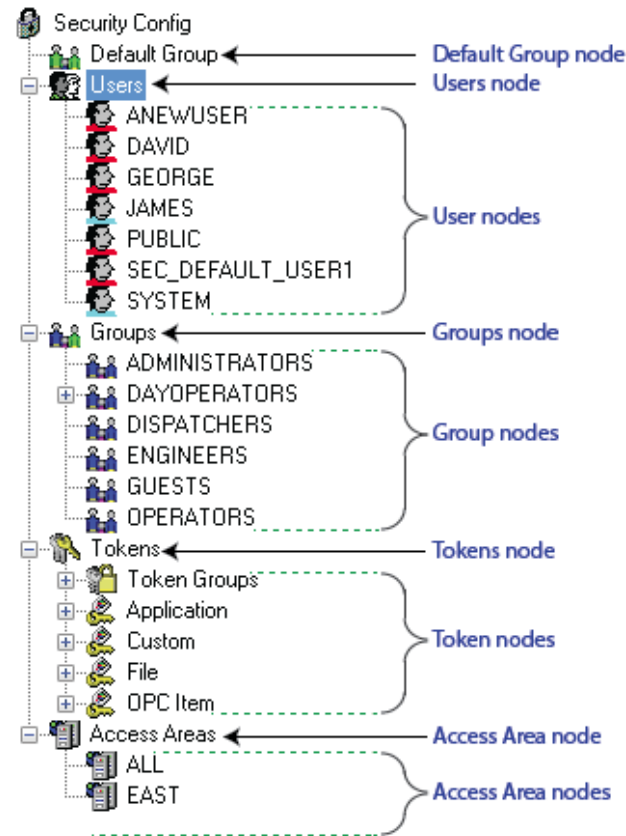
Select the **Help** option to display the online help file for OpenEnterprise. Select the **Action** option to display information about the version, build number and contact details for OpenEnterprise.

## 2.2 The Tree Pane

The Tree pane uses a tree structure to provide a graphical overview of the current configuration. The tree consists of a number of object-type nodes (Users, Groups, Tokens, and Access Areas), under which the system displays configured Security objects. See *Figure 2-28*.

Most object type nodes have a context menu, which you display by right-clicking on the object. Use these menus to create a new object of that type beneath the node.

**Figure 2-28. Tree pane**



All configured object elements in the Tree pane have a context menu, which provides access to the Properties dialogs for that object, as well as other options, depending on the type of object selected.

## 2.2.1 Default Group Node

The Default Group node has one context menu option. This opens the Properties dialog for the Default Group. The Default Group settings apply to every user, so they must be set at the lowest possible token and access area security level.

**Figure 2-29. Default Group node**



## 2.2.2 Users Node

The Users node has a context menu that provides two options.

**Figure 2-30. Users node**



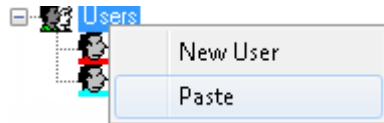
## 2.2.2.1 Creating a New User

For instructions on creating a new user, refer to *Section 2.1.2.2*.

## 2.2.2.2 Paste a User Configuration

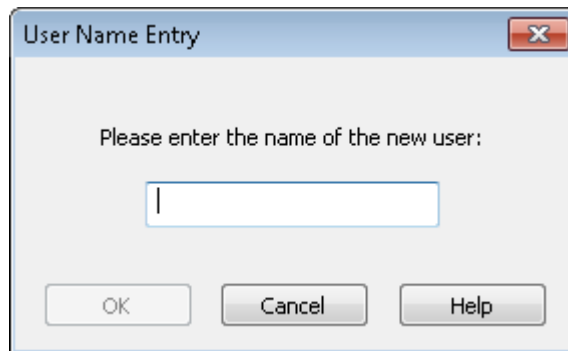
The Paste option on the Users Node menu enables you to “paste” (copy or overlay) a previously copied user's security configuration details to a new user. If you have not copied a user, the system disables the Paste option.

**Figure 2-31. Users node menu – Paste Option**




When you click **Paste**, the system displays the User Name Entry dialog. It prompts you for the name of the new user. Provide a unique name. When you click **OK** the system adds the new user, applying a duplicate of the entire security configuration of the source User.

**Figure 2-32. User Name Entry dialog**



## 2.2.3 User Nodes

The system uses distinctive user node icons to visually indicate the administrative level of a user. They may be either:

 Red – Standard (non-administrative) User

 Blue - Administrative User

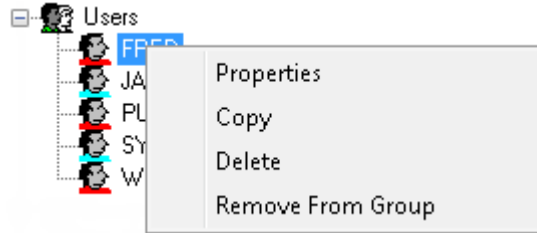


**Only** users who are members of the Administrator Group (“System Administrators”) can configure OpenEnterprise security, and **only** System Administrators can grant users administrative rights. By default, the SYSTEM user is a System Administrator.

### 2.2.3.1 Context Menu

When you right-click on any user in the list the system displays a content menu.

**Figure 2-33. User node menu**

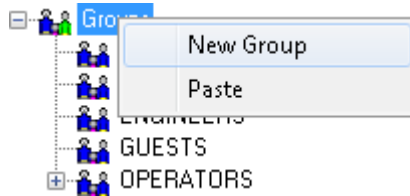


Option	Description
Properties	Opens the Properties dialog for the selected User. See the <i>User Properties: Properties tab</i> for further information.
Copy	Copies the selected User’s configuration details in preparation for pasting that configuration to a new User.
Delete	Deletes the selected User. When you select this option, the system displays a warning dialog:
	Click <b>Yes</b> to continue and delete the user or <b>No</b> to cancel the operation.
Remove From Group	Removes the selected user from the user group housing the user but <b>does not</b> delete the user from the system.

### 2.2.4 Groups Node

The Groups node has a context menu that provides two options.

**Figure 2-34. Groups node menu**

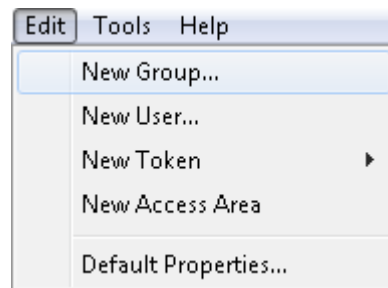


## 2.2.4.1 Creating New User Groups

You can create a new Group by any of the following methods:

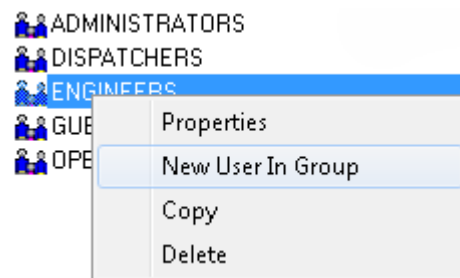
- Select **Edit > New Group** from the Security Configuration tool’s menu bar.

**Figure 2-35. Security Configuration tool Edit menu – new Group...**



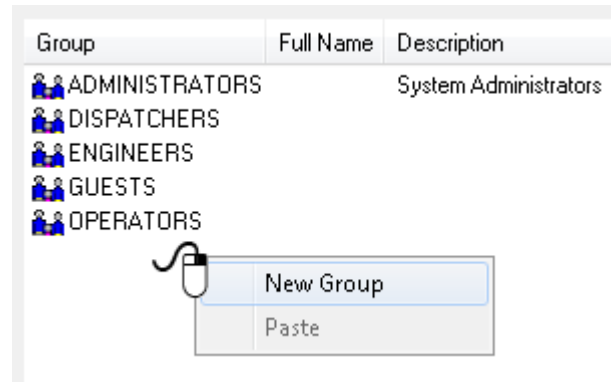
- Right-click a group node and select **New User In Group** from the displayed menu.

**Figure 2-36. Group node menu**



- Right-click the List pane and select **New Group** from the context menu.

**Figure 2-37. New Group floating context menu**



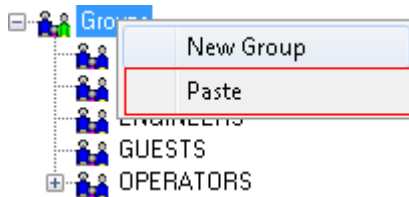
**Note**

Once you enter the new user name you cannot change it. Additionally, entering the name and display of the Group properties dialog is very similar in operation to creating a new user, except that the List pane displays configured Groups.

**2.2.4.2 Paste a Group Configuration**

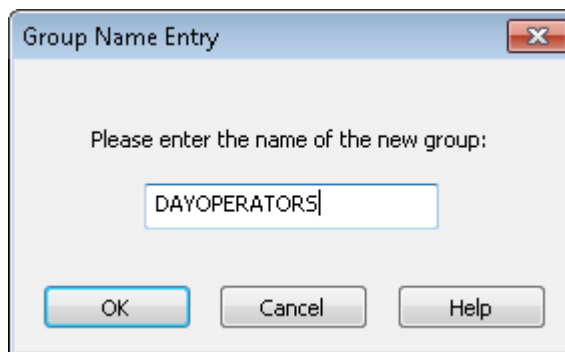
The Paste option on the Group menu enables you to “paste” (copy or overlay) a previously copied group’s security configuration details to a new group. If no group has been copied, the Paste option is disabled.

**Figure 2-38. Groups node menu – Paste**



When you click **Paste**, the system displays the Group Name Entry dialog. It prompts you for the name of the new group. Provide a unique name. When you click **OK** the system adds the new group, applying a duplicate of the entire security configuration of the source User.

**Figure 2-39. Group Name Entry dialog**

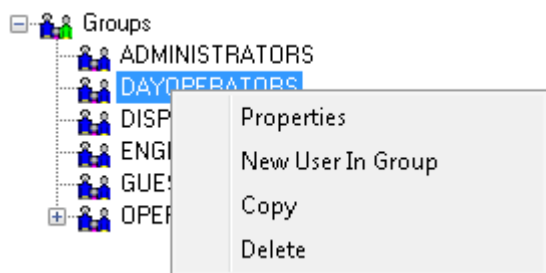


## 2.2.5 Group Nodes

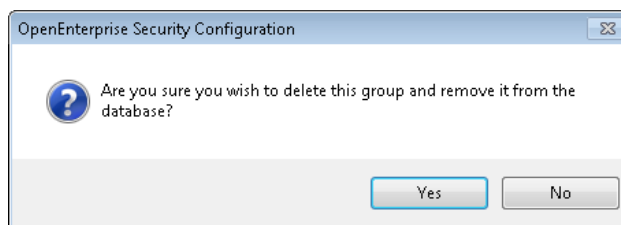


The system assigns a blue icon to any group an OpenEnterprise System Administrator creates. You can expand the group branch to display the configured individual group names and icons. Selecting a node causes the system to display the configured groups in the List pane along with any associated full names and descriptions. Finally, right-click a group node to display a context menu with four options.

**Figure 2-40. Group node menu**



Option	Description
Properties	Displays the selected user group's Properties dialog. For further information, refer to the online help topic for User Group Properties dialog.
New User In Group	Enables you to create and add a new user to the selected user group.
Copy	Enables you to copy the group's security configuration in preparation for pasting it onto a new group. <b>Note:</b> The system does not copy the users within the user group, but copies <b>only</b> the security configuration.
Delete	Deletes the selected user group. The system displays a warning



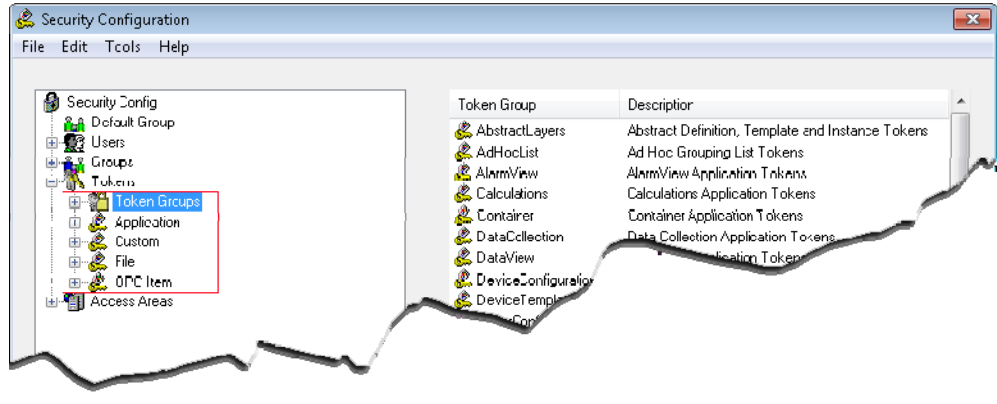
Click **Yes** to continue and delete the user or **No** to cancel the operation.

## 2.2.6 Tokens Node



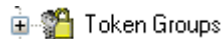
This is the root node for the all Token Type nodes. It is the only parent node that does not have its own context menu. Expanding this node displays the available Token Type nodes.

**Figure 2-41. Expanded Tokens Node**



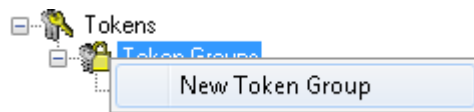
### 2.2.6.1 Token Groups Node

**Figure 2-42. Token Groups node**



Use the Token Groups node context menu (which displays when you right-click the node) to create new token groups. For further information, refer to the online help’s *Creating New Token Group* topic.

**Figure 2-43. Token Groups menu**



When you expand the Token Groups node, it displays the four types of token group nodes. For further information, refer to the online help’s *Token Group Nodes* topic.

Token groups are collections of tokens which can form a token “template” you can associate with a user or user group. User-generated token groups can be a combination of any of the four types of tokens.

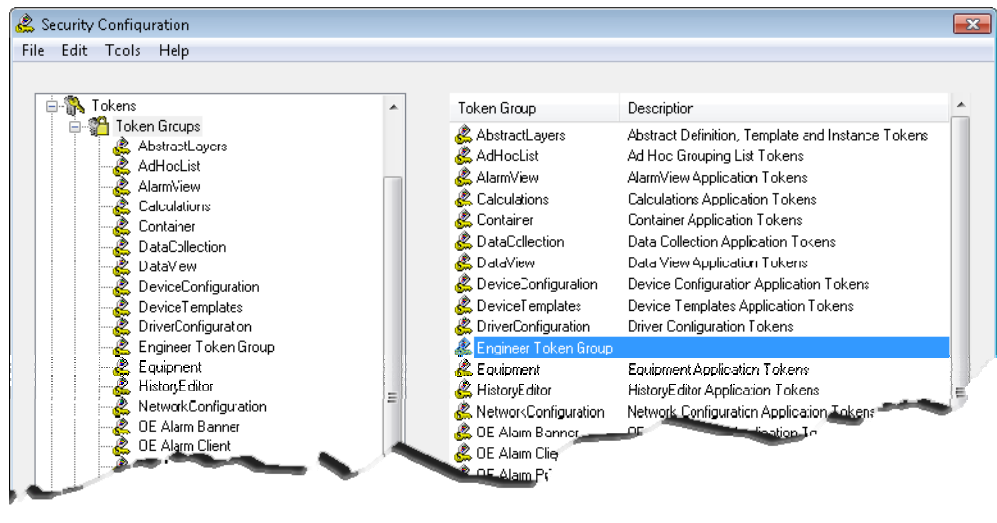
The system also maintains several special Application Token Groups independently of the system administrator. The system groups them by their OpenEnterprise component name: OE Alarm Banner, OE Alarm Client, OE Alarm Printer, OE Desktop, OE Graphics, OE Notes Client, OE SQL QL Viewer, and OE Trend Client Token Groups. You **cannot** edit these Token Groups.

### 2.2.6.2 Token Group Nodes

Expanding the token node displays all the configured token groups. Select this node to display all the token groups in the List pane, along with any associated descriptions.

By associating a token group with a user or user group, you can include or exclude all tokens configured in that token group with a user's or a user group's Security Configuration profile. Essentially, you can use token groups as templates to assign selected tokens to users or user groups.

**Figure 2-44. Expanded Token Groups node**

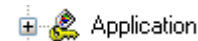


### 2.2.6.3 User Configured Token Groups

Only a **system administrator** can configure token groups. The system administrator can also add any of the default Application tokens to this token group, as well as configure Custom, File and OPC Tokens for it. You can then use the token group as a token “template” for user groups such as Operators or Engineers.

### 2.2.6.4 Application Tokens Node

**Figure 2-45. Application Tokens node**



The Application tokens node has no context menu because you cannot create, modify, or delete Application tokens. The system creates them at installation time.

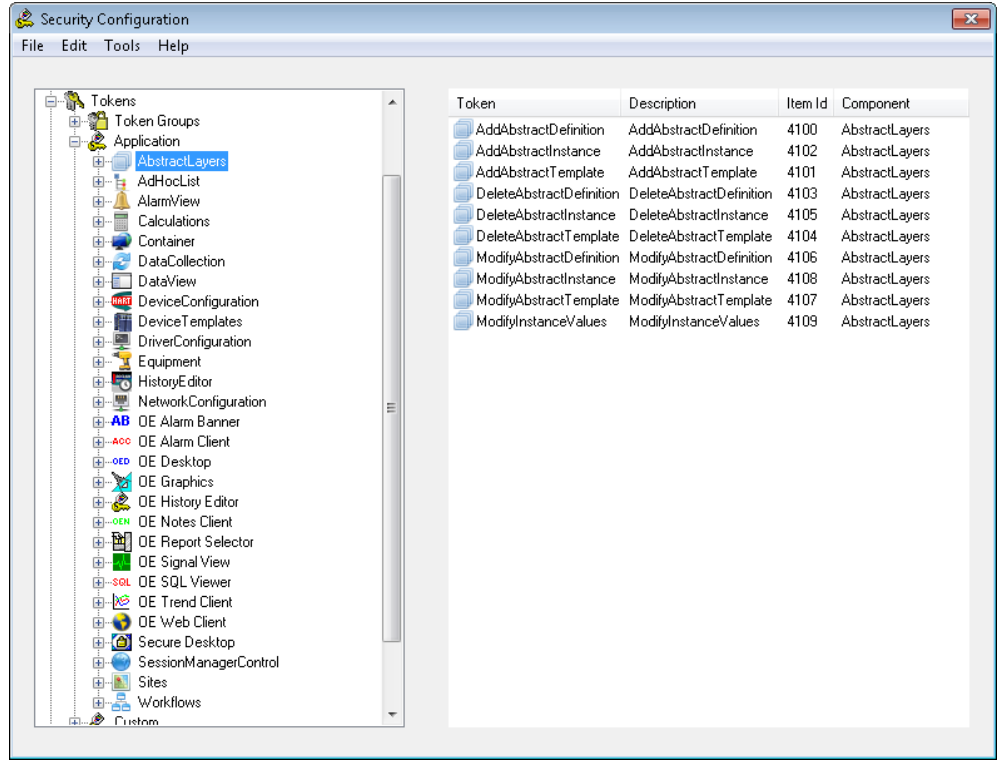
Use Application tokens to grant or deny application actions defined by the application's menu items (such as acknowledging alarms in the Alarm Viewer). Expanding the node displays the application nodes for which tokens exist.

### 2.2.6.5 Application Token Component Types

Expanding any of the application nodes (by clicking the plus sign to the left of the node) displays the associated application tokens in the tree. Selecting an application node

displays its associated tokens in the List pane, together with associated description, item id numbers, and component names. *Figure 2-46* shows the AbstractLayers tokens.

**Figure 2-46. Selected Application Token type**



### 2.2.6.6 Dragging and dropping Application Tokens

The system allows you to drag individually selected tokens from the List pane and drop them onto a user or group in the Tree pane, incorporating them into an Include or Exclude list, depending on the Drag Option setting (See *Section Drag Options* for more detail). You can also drag tokens onto token groups to add them to the token group.

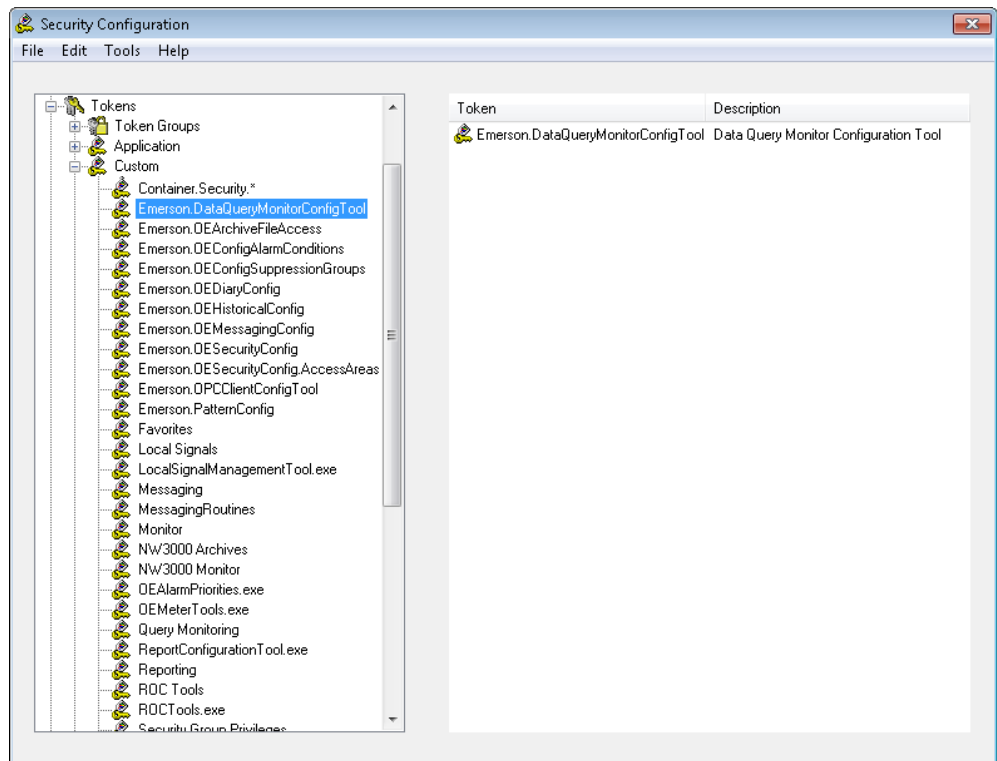
### 2.2.6.7 Custom Tokens



The Custom tokens node has its own context menu that enables a user to create new Custom Tokens. For further information, refer to the online help's Creating String Type Token topic. Custom Tokens are strings used mainly to grant or deny access to custom menus created with the OE Menu Editor.

When you expand the Custom node, the branch displays all configured Custom Tokens. When you select the node, its tokens display in the List pane, along with any descriptions.

**Figure 2-47. Selected Custom Token node**



Selecting an individual Custom Token in the tree lists the individual token in the List Pane. You can drag-and-drop tokens from the List pane onto Tree nodes such as user, group, and token groups.

## 2.2.6.8 File Tokens



The File node has its own context menu that enables a user to create new file tokens. File tokens are strings used to grant or deny access to certain files or file types. For further information, refer to the online help's *Creating Simple String Type Tokens* topic.

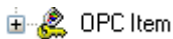
When you expand the Custom node, it displays all configured file tokens. When you select the node, the tokens display in the List pane, along with any descriptions.



Figure 2-48. Selected File Token node



### 2.2.6.9 OPC Item Tokens

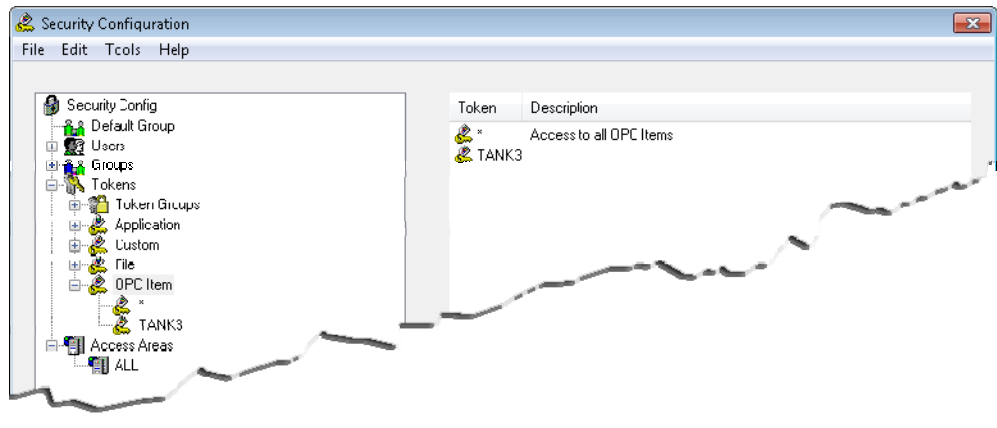


OPC Item

The OPC Item node has its own context menu that enables a user to create new file tokens. For further information on creating new OPC Item Tokens, refer to the online help’s *Creating Simple String Type Tokens* topic. OPC Item Tokens are strings which grant or deny write access to OPC tags. For further information on how OPC Item tokens work, refer to the online help’s *OPC Item Token Types* topic.

When you expand the OPC Item node the system displays all configured OPC Item Tokens in the List pane, along with any descriptions.

Figure 2-49. Expanded OPC Item node



### 2.2.7 Access Areas Node

This is the root node for all Access Area nodes. Expanding this branch displays the configured access areas. Selecting this node displays the access areas and their associated descriptions in the List pane.

The Access Areas node has one context menu option, which enables you to create a new access area.

**Figure 2-50. Access Areas node**

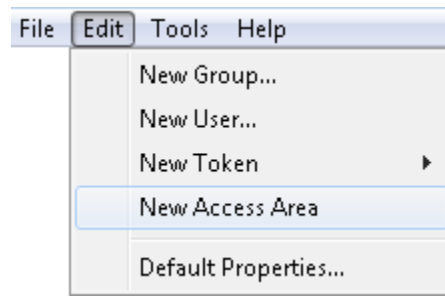


## 2.2.7.1 Creating New Access Areas

You can create a new access area using any of the following methods:

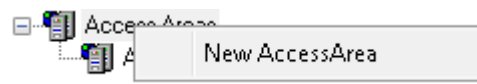
- Select **Edit > New Access Area** from the Security Configuration tool's menu bar.

**Figure 2-51. Security Configuration tool Edit menu – New Access Area**



- Selecting the **New Access Area** context menu option from the Access Areas node.

**Figure 2-52. New Access Area context menu**



Once you select **New Access Area** the List pane displays all the currently configured access areas and inserts a new entry with a blank name at the top of the list. Enter a valid name and press **Enter**. The system opens the Access Area Properties dialog, which allows further configuration.

---

### Note

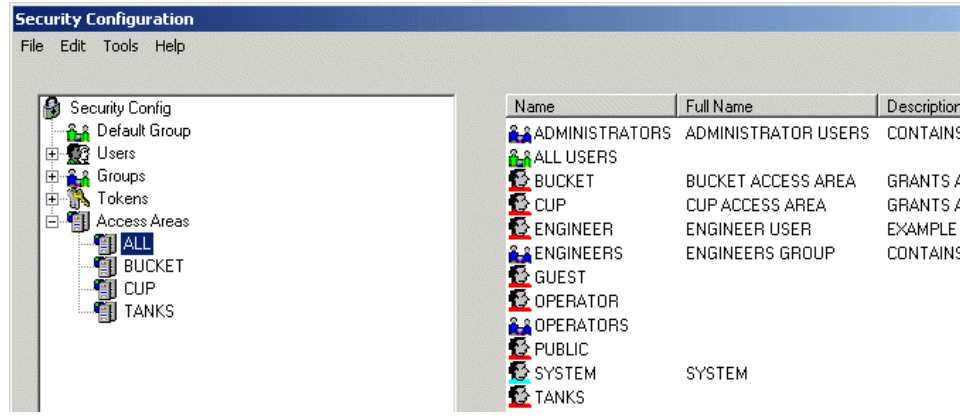
Access Area names are case-sensitive and must be unique within Access Areas only.

---

## 2.2.7.2 Access Area Nodes

Selecting an individual Access Area node in the left-hand pane displays the users and groups currently associated with the Access Area in the List pane. Right-clicking the node displays a Properties context menu, which opens the Access Area Properties dialog.

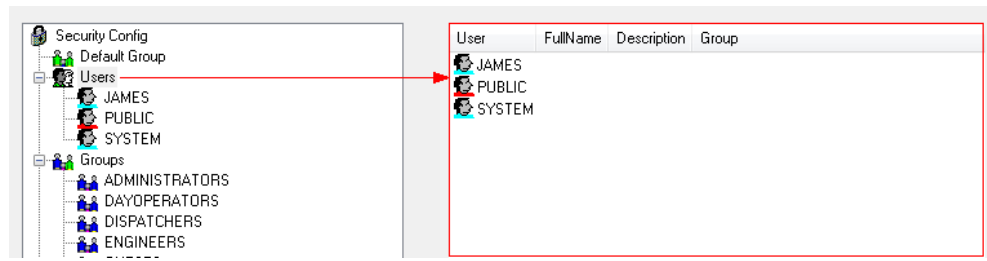
Figure 2-53. Selected Access Area



## 2.3 The List Pane

The List pane provides more detail on the particular object that you have selected in the Tree pane. If you select an object type node (such as Users), the system displays all of the configured objects that belong to that type in the List pane.

Figure 2-54. List pane showing all Users



The column headings and contents vary depending upon the type of object being displayed. The list may be ordered by any one of the available columns. The default ordering is normally on the first column in ascending order. You can re-order the display by clicking on an individual column header. You can reverse the order by clicking again on an already clicked column header. For example, if a column was sorted in ascending order, clicking its header again sorts it in descending order. Should the data exceed the capacity of the window then the system displays vertical and/or horizontal scroll bars; scroll them as necessary.

Objects in the list support a context menu that enables their Properties to be viewed, and optionally provide a summary of the object's use or its associations with other objects.

## 2.4 Security Configuration Dialogs

Using the dialogs available from the Security Configuration tool, a **system administrator** can configure every aspect of OpenEnterprise Workstation Security. You access each dialog either by a menu item or by double-clicking or right-clicking and selecting **Properties**.

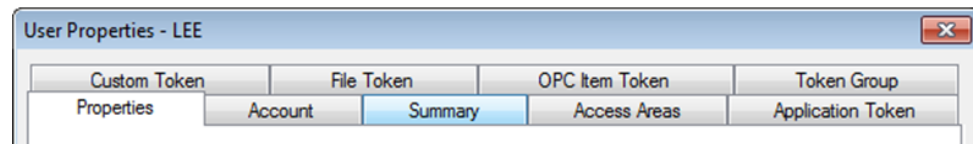
- The User
- The User Group
- The Token Group
- The Token
- The Token Summary
- The SQL Import-Export File
- The File Import
- The Options

### 2.4.1 User Properties: Properties tab

The Properties dialog enables OpenEnterprise System Administrators to configure basic security settings for each OpenEnterprise User. You access the User Properties dialog by right-clicking any user (selected from the Tree or from the List pane). As shown in *Figure 2-55*, each Properties dialog typically has nine tabs:

---

**Figure 2-55. User Properties Dialog: Tabs**



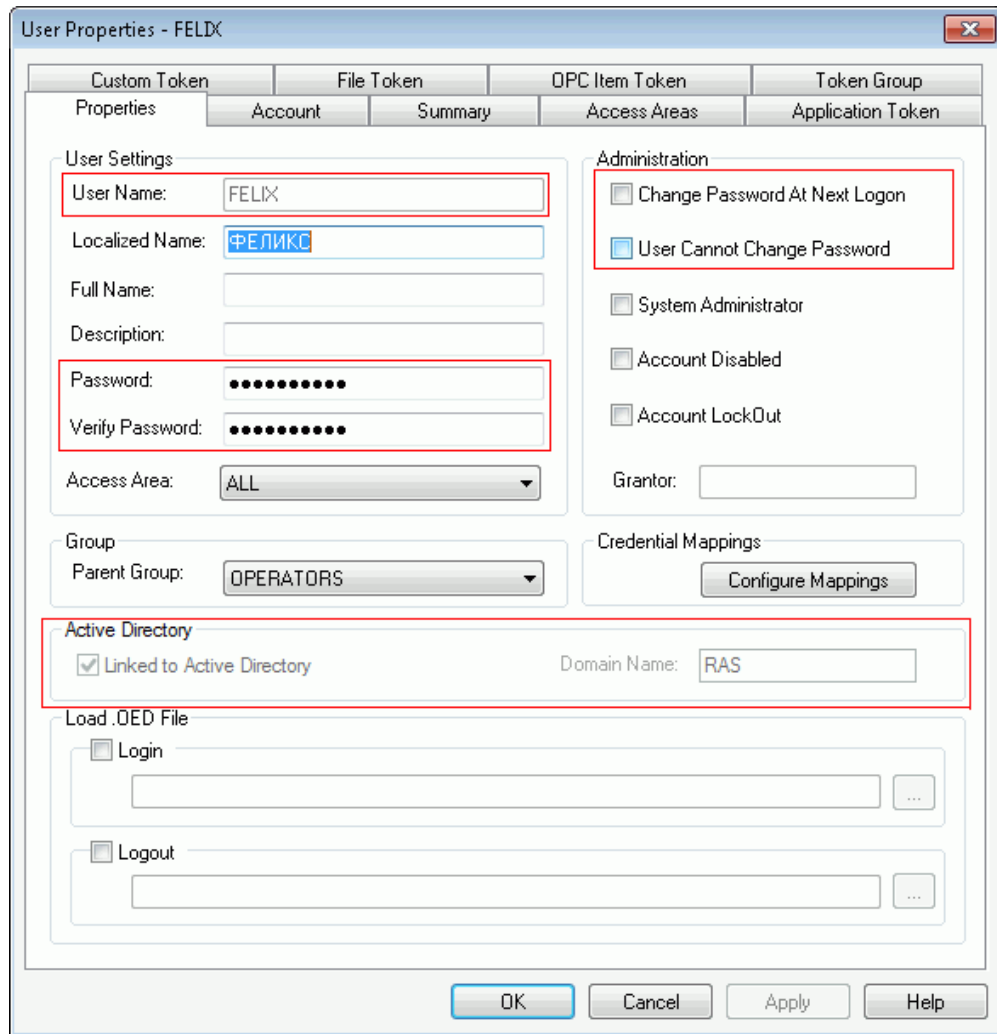
---

**Note**

The Properties dialogs for the Default Group and for any user-created groups contain no Summary tab, and the system disables the Password, Verify Password, and (where applicable) the Parent Group fields.

---

Figure 2-56. User Properties Dialog

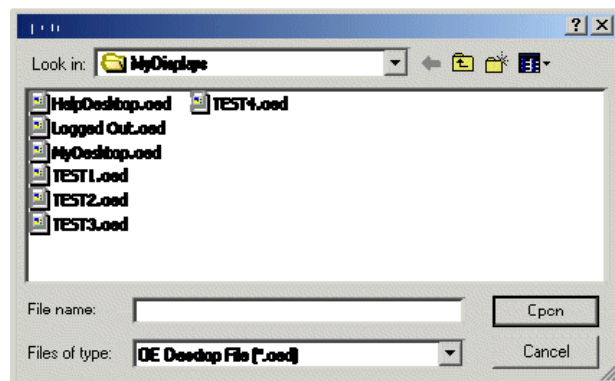


Option	Description
User Name	This <b>read-only</b> field displays the name for this User. Once you create the User, you can no longer edit the name. The Security Configuration tool displays all user names in upper case.
Localized Name	Specifically for use in Workstation Localization, this field provides an additional name on top of an OpenEnterprise user's normal name. It is an alias that the user can use to log in with their own localized name. <b>Note:</b> To see the standard OpenEnterprise user name displayed in the localized format you need to add the name and translated text to a Project Translation file.
Full Name	Specifies the full name of the user if it was abbreviated in the User Name field. This is an optional character field.

Option	Description
Description	Provides further information about the User. This is an optional field.
Password	Enables you to change the password for this User. If the logged-in user does not have sufficient privileges to change this field, the system grays it out. For security, the system displays this field as 10 bullets (•), regardless of the length of the actual password. <b>Note:</b> The system disables this field for groups, the Default Group and Users linked to Active Directory.
Verify Password	Provides an <b>exact</b> repeat of the value in the Password field. For security, the system displays this field as 10 bullets (•), regardless of the length of the actual password. <b>Note:</b> The system disables this field for groups, the Default Group and users linked to Active Directory.
Access Area	Click to display a drop-down list from which you can select an access area for this User. When you create a new user, the system defaults the access area to ALL. The System Administrator can then assign specific access areas to a particular User.
Change Password at Next Logon	Enables a System Administrator to force the user to change their password the next time the user logs onto OpenEnterprise. <b>Note:</b> You cannot use this option in conjunction with the User Cannot Change Password option. The system disables this field for users linked to Active Directory.
User Cannot Change Password	Prevents a user from changing their password. Select this option to prevent the user from changing their password. <b>Note:</b> You cannot use this option in conjunction with the Change Password at Next Logon option. The system disables this field for users linked to Active Directory.
System Administrator	Gives a created user the status of an OpenEnterprise System Administrator. Administrative rights can only be revoked by the System Administrator who initially granted those rights. Therefore, when a System Administrator who did not <b>originally</b> grant administrator rights to this user views this dialog, the system disables this field. <b>Note:</b> The system disables this field for groups and the Default Group.

Option	Description
Account Disabled	<p>Disables a User’s account, which prevents the user from logging on or changing their password.</p> <p><b>Note:</b> Only a System Administrator can re-activate a disabled user account.</p>
Account LockOut	<p>Indicates a User’s account is locked out. This prevents the user from logging on or changing their password. Although you can lock out an account manually, the most common use of account lockouts is to protect the OpenEnterprise system. For example, consecutively logon failures due to an incorrect password can lock out a User’s account.</p> <p>Unlocking an account can occur either manually (by a Security Administrator using the Security Configuration tool) or based on a time trigger (where the lock is automatically released after a specified period of time).</p>
Grantor	<p>Indicates the setting of the Grantor field, which can only be the SYSTEM user.</p> <p><b>Note:</b> The system disables this field for groups and the Default Group.</p>
Parent Group	<p>Click ▼ to display a drop-down list of available groups to which the selected user can be assigned. <b>None</b> is the <b>default</b>.</p> <p>A System Administrator uses this field to assign the selected user to <b>one and only one</b> Parent group. The system adds the security privileges of that Parent group to the User’s own privileges</p> <p><b>Note:</b> The system replaces this field with the Configure Group Privileges option on the Groups Properties dialog.</p>
Configure Mappings	<p>Click to open the Login Mappings dialog.</p>
Linked to Active Directory	<p>Specifically for use with Active Directory, this read-only field indicates that Active Directory manages the login credentials. When checked, the OpenEnterprise user is automatically logged into OpenEnterprise using their login credentials from the workstation.</p> <p>You cannot unlink an OpenEnterprise user from the Windows AD.</p>
Domain Name	<p>Specifically for use with Active Directory, this read-only field indicates the domain used to manage login credentials.</p> <p>OpenEnterprise configures this value when when adding a user and linking to Active Directory.</p>
Login	<p>Enables the selection of the Logged in OpenEnterprise Desktop (.OED) filename field and its browse button.</p> <p>Use the filename field to provide the full path name</p>

Option	Description
	<p>of the OE Desktop file the system loads when a specific user or user group logs in. You can use the browse button (located at the far right of the filename field) to search for a file. When you select a file, the system provides the path and file name.</p> <p>For further information on the OE Desktop Login Logout file precedence function works, refer to <i>OE Desktop Login-Logout File Precedence</i> below.</p>
Logout	<p>Enables the selection of the Logged out OE Desktop (.OED) filename field and its browse button.</p> <p>Use the filename field to provide the full path name of the OE Desktop file the system loads when a specific user or user group logs out. You can use the browse button (located at the far right of the filename field) to search for a file. When you select a file, the system provides the path and file name.</p> <p>For further information on how the OE Desktop Login Logout file precedence function works, refer to the section <i>OE Desktop Login-Logout File Precedence</i> below.</p>
Browse button	Click to open a Windows File Open dialog.



Select the correct OED file to be loaded and click **Open**. The dialog closes and the system enters the full path and name of the file into the appropriate OE Desktop file name field on the Properties tab.

OK	Click to close the dialog; the system sends any configuration changes to the database.
Cancel	Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.
Apply	Click to send any configuration changes to the database; the system does not close the dialog.
Help	Click to access the online help system for OpenEnterprise.



### 2.4.1.1 OE Desktop Login - Logout File Precedence

System administrators can grant users their own unique OE Desktop file (such as a special menu or a streamlined selection of typical processes) that loads when that user logs into OpenEnterprise. This is accomplished using the Security Configuration tool and associating the user with a user group that has a specific Logged in OE Desktop file assigned to it.

Once the user is linked to a “logged-in” desktop file (using the fields in the Load .OED File pane of the User Properties dialog), the system needs to determine which file to load. The loading sequence is:

1. Load the OE Desktop file specified at the user level
2. Load the OE Desktop file specified at the user group level
3. Load the OE Desktop file specified at the All (Default) Users Group level
4. Load the OE Desktop file specified by the OE Desktop file itself.

Therefore, in the example in *Figure 2-57*, the system loads the OE Desktop file specified at the user level.

### 2.4.1.2 Login Mappings Dialog

Click **Configure Mappings** on the Properties dialog to display the Login Mappings dialog. This dialog provides the system administrator with two distinct functions: configuring an OpenEnterprise workstation to automatically logon to OpenEnterprise (based on the currently logged on Windows user, which maps the Windows user to an OpenEnterprise user) **or** mapping OpenEnterprise user credentials to an application’s security credentials (which grants users access to RTUs without having to manually enter the RTU credentials).

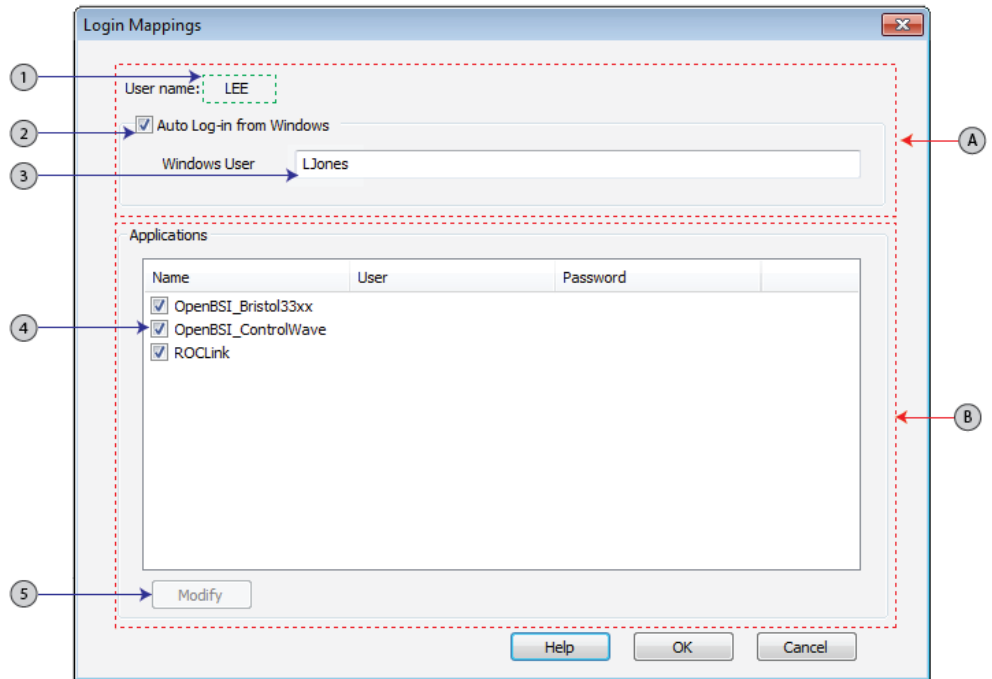
---

#### Note

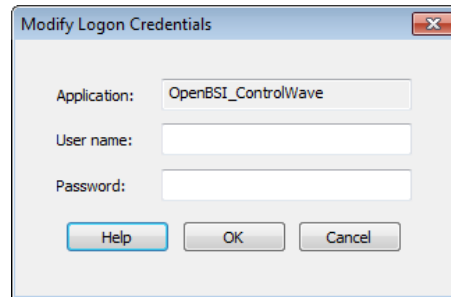
If you intend to use Active Directory, you should remove **any** Windows user login mappings (see *Logging onto OpenEnterprise using Credential Mapping*). **Do not** remove the mappings in the Applications section.

---

**Figure 2-57. Login Mappings dialog**



- A Windows User mapping area. OpenEnterprise’s Security Manager maps a Windows user to the OpenEnterprise User when you select the Auto Log-in from Windows option.
- 1 Indicates the selected OpenEnterprise user name (select **Security Configuration > Users**)
- 2 Auto log-in from Windows option
- 3 Identifies a Windows user name (without the domain name part) to map to the OpenEnterprise user name
- B Associates application credentials with an OpenEnterprise user. Typically allows access to RTUs without the user having to manually enter RTU credentials. Users can then use the application functions (such as adding a ControlWave to OpenEnterprise or launching ROCLINK for a selected RTU) without needing to logon to OpenEnterprise.
- 4 Specifies the selected applications.
- 5 Click to access the Modify Logon Credential dialog.

**Figure 2-58. Modify Logon Credentials dialog**

---

Complete this dialog to enable the OE Security Manager to facilitate application logon.

---

**Note**

The ability to use this application is subject to the access rights granted to the user specified for the application logon. For example, the system uses the OpenEnterprise application credentials for ControlWave during the insert of a ControlWave device from a connected device. Therefore, the OpenEnterprise application credentials must match those defined within the RTU. For further information, refer to the online help topic *Adding a ControlWave with a Non default RTU System Password*.

---

## 2.4.2 User Group - Properties

As a **system administrator**, you can use this tab to configure security settings for user groups. The dialog displayed in *Figure 2-59* is an example of the Default Group. Since OpenEnterprise automatically creates the Default Group, you cannot delete it. As the Default Group, its settings apply to **every** user. You can override some –but not all – of these settings at a user or at a created user group level. See the online help topic *Security Concepts* for more information.

---

**Note**

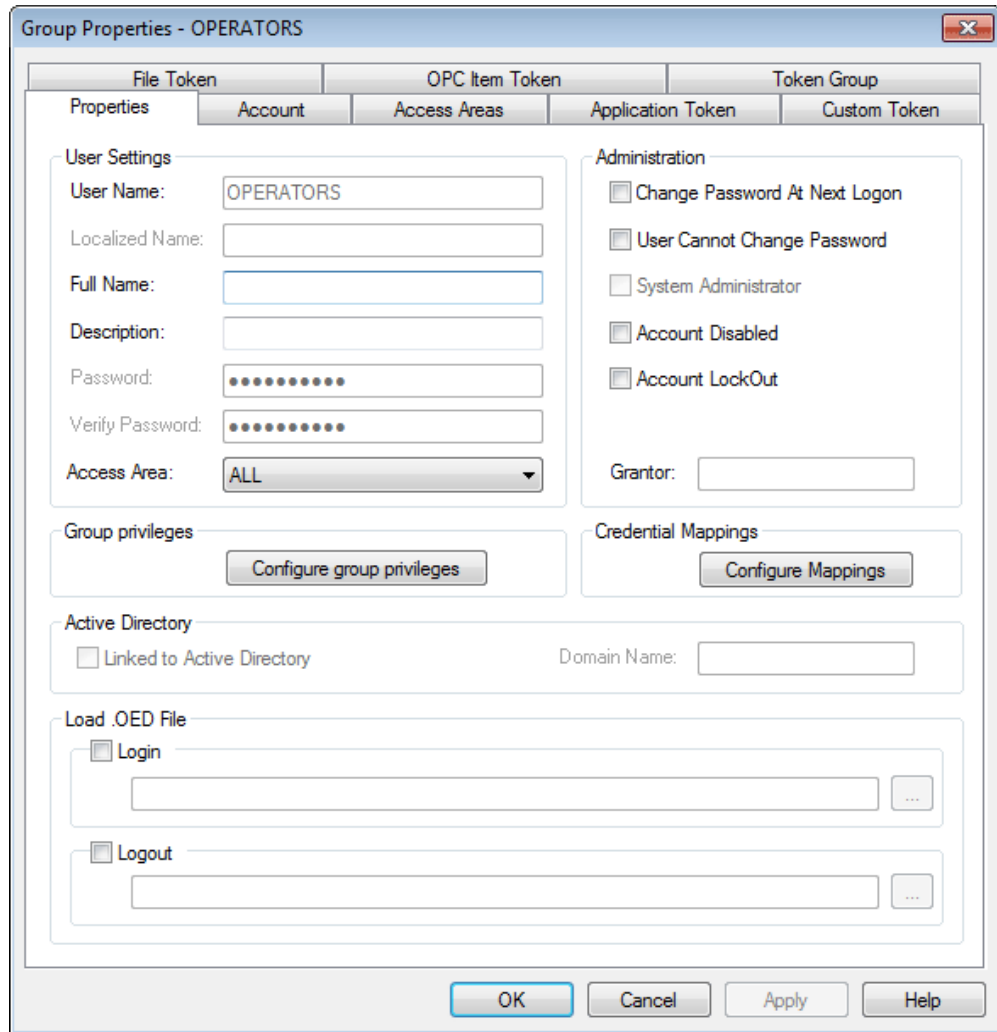
Unlike other Properties dialogs, this dialog has no Summary tab. Additionally, the system disables the Password and Verify Password fields. This is also true for the Properties dialogs for **all** created groups.

---

**Fields Not Applicable to Groups**

- **Localized Name** - Specifically for use in Workstation Localization, this field defines an alias that a user can use to log in with their own localized name.
- **Linked to Active Directory** - Specifically for use with Active Directory, this field manages an OpenEnterprise user's login credentials.
- **Domain Name** - Specifically for use with Active Directory, this **read-only** field shows the domain used to manage login credentials.

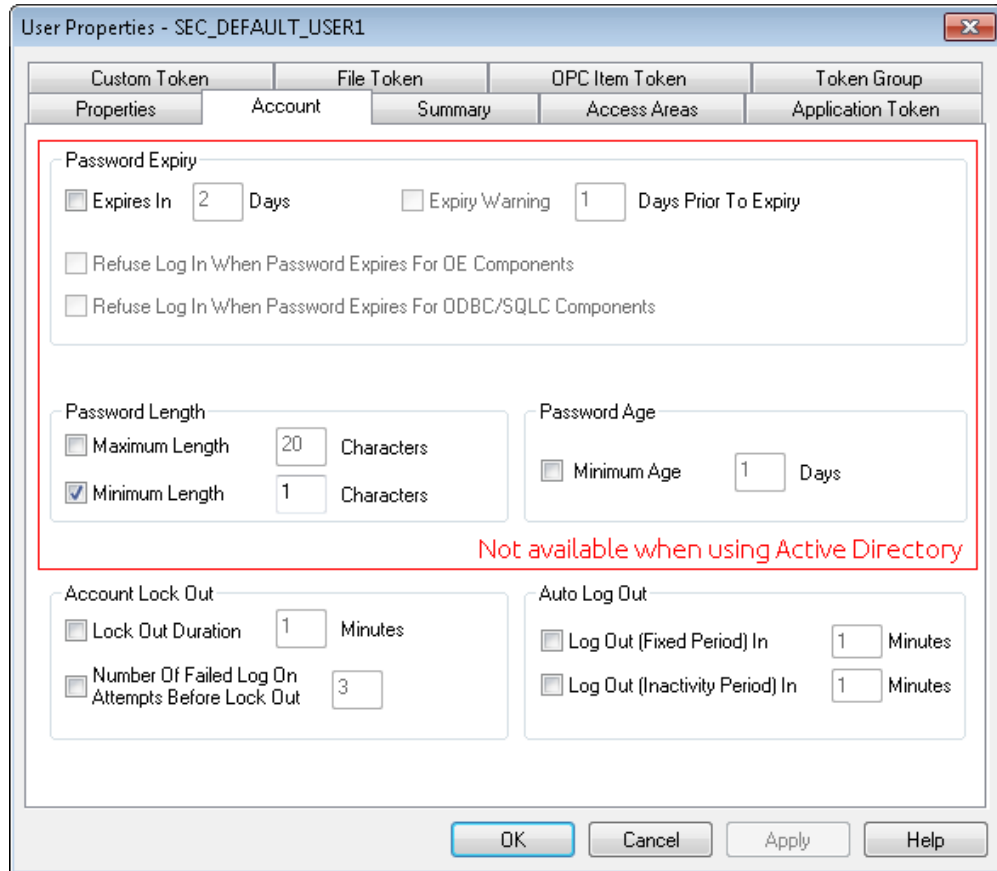
Figure 2-59. Group Properties – Properties tab



## 2.4.3 User Properties: Account tab

Use this tab to configure a User's password parameters (expiry, length, and minimum age before a new password is allowed) as well as account lockout and auto logout settings.

**Figure 2-60. User Properties – Account tab**



Option	Description
Expires in	Controls whether user passwords expire. If you <b>do not</b> select this option, user passwords <b>never</b> expire. The system then disables the other fields in this pane. If you <b>select</b> this option, the system enables the other fields in this pane. Configure password expiry in days; the system applies the value you define to the last password change for the User. For example, if a user changes the password at 11:23:07 AM on 24 November and you configure their account so that the password expires after 3 days, the system forces the user to change the password as of 11:23:07AM on 27 November.
Expiry Warning	Displays an advanced warning to the user of a pending password expiry. You <b>must also</b> complete

Option	Description
	<p>the Days Prior to Expiry field.</p> <p><b>Note:</b> The system activates this option <b>only</b> when you select the <b>Expires In</b> option.</p>
<p>Refuse Log In When Password Expires for OpenEnterprise Components</p>	<p>Controls (for OpenEnterprise components such as OPC Server, HDA Server, or Alarm Client Server) how the system acts with an expired password. You can configure the system to either prevent the user from logging onto the OpenEnterprise system <b>or</b> allow the user to log onto the OpenEnterprise system but require an immediate password change.</p> <p>The OELogin Client enforces a password change for any user configured to allow log in when a password expires. If the user then chooses not to change their password, they are automatically logged off the system.</p> <p><b>Note:</b> The system activates this option <b>only</b> when you select the <b>Expires In</b> option.</p>
<p>Refuse Log In When Password Expires for ODBC/SQLC Components</p>	<p>Controls, for ODBC/SQLC components, how the system acts with an expired password. Select this option to direct OE to refuse to log in any user using a non-OE component (such as ODBC or the SQL Client, SQLC) to access the database. Since OpenEnterprise cannot enforce a password change for non- OpenEnterprise components, select this option for users whose password is set to expire.</p> <p><b>Note:</b> The system activates this option <b>only</b> when you select the <b>Expires In</b> option.</p>
<p>Maximum Length</p>	<p>Indicates the maximum number of acceptable characters for a User's password.</p>
<p>Minimum Length</p>	<p>Indicates the minimum number of acceptable characters for a User's password.</p>
<p>Minimum Age</p>	<p>Controls how frequently a user can change a password. If you select this option, you <b>must also</b> indicate a number of days.</p> <p>The system applies the value you define based on the date of the User's last password change. For example, if you set the Minimum Age to <b>5</b> days and the user changes their password at 2:45:34 on 24 November, the user <b>cannot</b> change their password again until 2:45:34 on 29 November.</p> <p><b>Note:</b> If the value in the Minimum Age field is <b>greater</b> than the value in the Password Expiry field, that would prevent the changing of an expired password. However, the Security Configuration tool prevents this from occurring.</p>
<p><b>Account Lock Out</b></p>	<p>These fields control when and how a User's</p>

Option	Description
	<p>account is locked out, which prevents a user from logging on or changing their password.</p> <p>Although you can manually lock out an account, the most common use of this option is to protect the OpenEnterprise system, when repeated failed attempts to log on consequently trigger the account lock out.</p> <p>Unlocking a locked account can occur manually (when a Security Administrator uses the Security Configuration tool) or automatically (after a pre-defined period of time).</p>
Lock Out Duration	<p>Defines the number of minutes during which a user is locked out of their account before they can attempt another log on.</p> <p>To <b>permanently</b> lock out an account, either <b>do not</b> select this option or select the option and enter <b>0</b> (zero) in this field.</p>
Number of Failed Log On Attempts Before Lock Out	<p>Defines the number of failed logon attempts before the user is locked out of the system.</p>
<b>Auto Log Out</b>	<p>These fields ensure that unattended OpenEnterprise workstations are not left in a logged-on state.</p>
Log Out (Fixed Period)	<p>Defines the number of minutes a user can remain logged in. After this time, the system automatically logs the user out. If you select this option, you must complete the Minutes field.</p>
Log Out (Inactivity Period)	<p>Defines the number of minutes a keyboard or mouse (or other PC input device) can remain inactive before the system automatically logs the user out. If you select this option, you must complete the Minutes field.</p>
OK	<p>Click to close the dialog; the system sends any configuration changes to the database.</p>
Cancel	<p>Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.</p>
Apply	<p>Click to send any configuration changes to the database; the system does not close the dialog.</p>
Help	<p>Click to access the online help system for OpenEnterprise.</p>

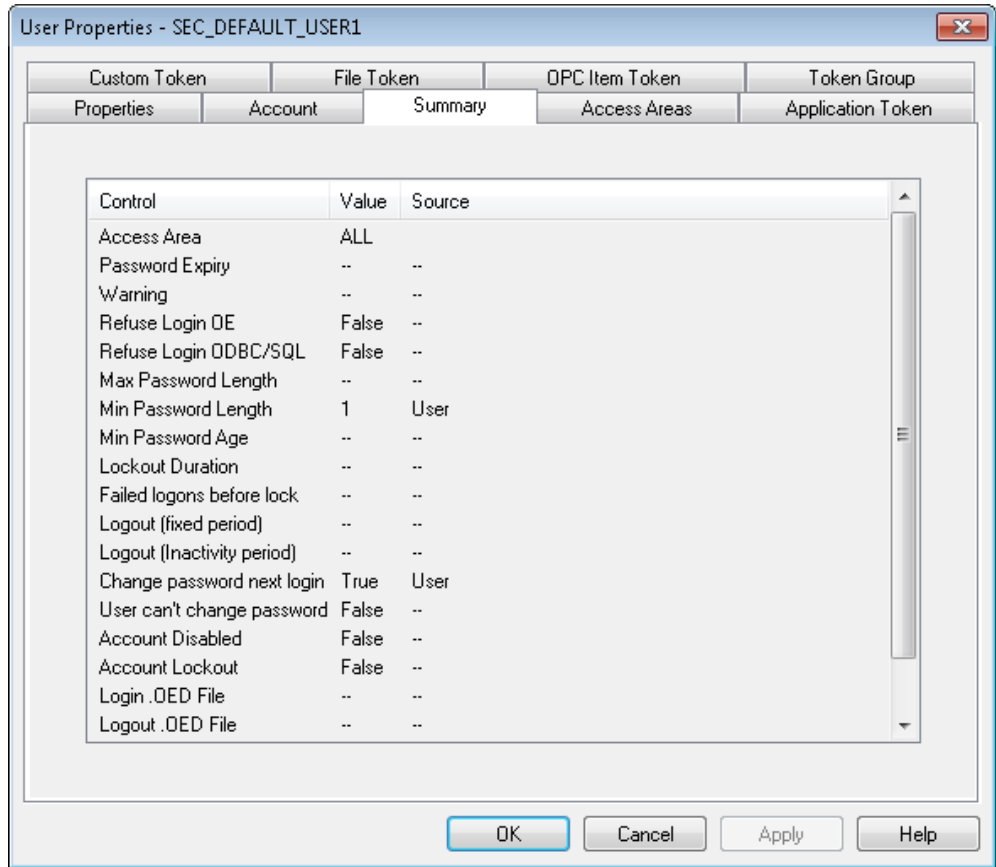
## 2.4.4 User Properties: Summary tab

This page displays a summary of the current settings for a user.

### Note

The system does not provide this for either a user-created group or the Default Group.

**Figure 2-61. User Properties – Summary tab**



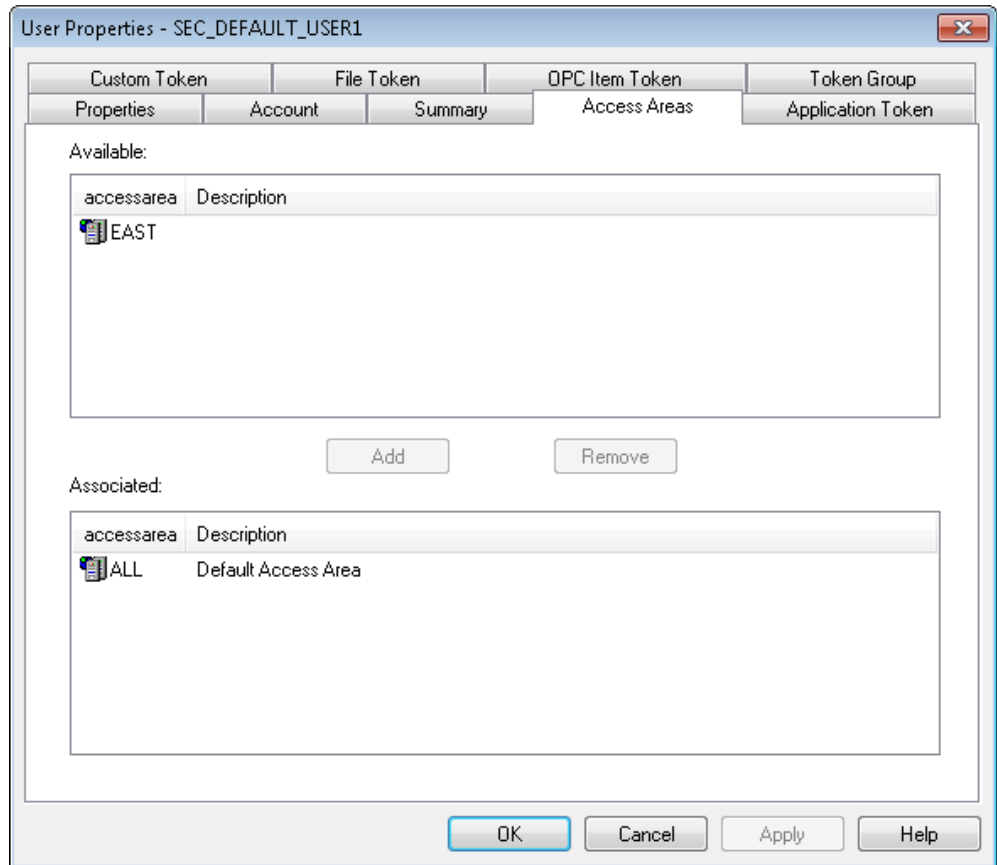
Option	Description
Summary list	This display-only field shows an <b>OpenEnterprise System Administrator</b> a summary of configuration details for a User. The display lists control items, showing their current values and the source of the control value.  For example, if a user belongs to a group for which the minimum password length has been set but has not been set for the user, the display shows the source as Group and shows the group's number. Possible Source column values are User, Group, and Default. If no value is currently in use, the system displays a double dash (--).
OK	Click to close the dialog.
Cancel	Click to close the dialog.
Apply	Disabled on this page.
Help	Click to access the online help system for OpenEnterprise.



## 2.4.1 User Properties: Access Areas tab

Use this dialog to assign Access Areas to a user or user group.

**Figure 2-62. User Properties – Access Areas tab**



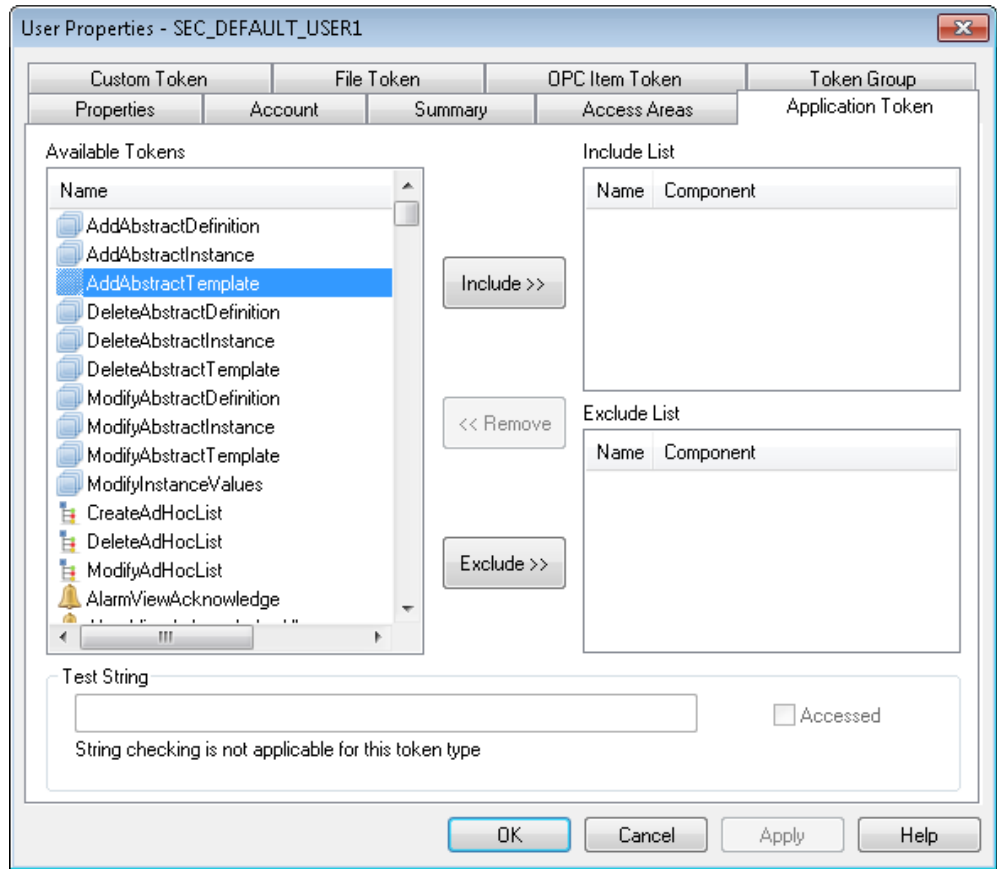
Option	Description
Available (Access Areas)	Displays available access areas which have not yet been associated with the user.
Add	Click to move the selected access area from the Available list to the Associated list for this user.
Remove	Click to move the selected access area from the Associates list to the Available list for this user. The system disassociates this access area and this user.
Associated (Access Areas)	Displays access areas already associated with the user.
OK	Click to close the dialog; the system sends any configuration changes to the database.
Cancel	Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.
Apply	Click to send any configuration changes to the

Option	Description
	database; the system <b>does not</b> close the dialog.
Help	Click to access the online help system for OpenEnterprise.

## 2.4.2 User Properties: Application Token tab

Use this table to award or deny individual Application tokens to users.

**Figure 2-63. User Properties – Application Token tab**



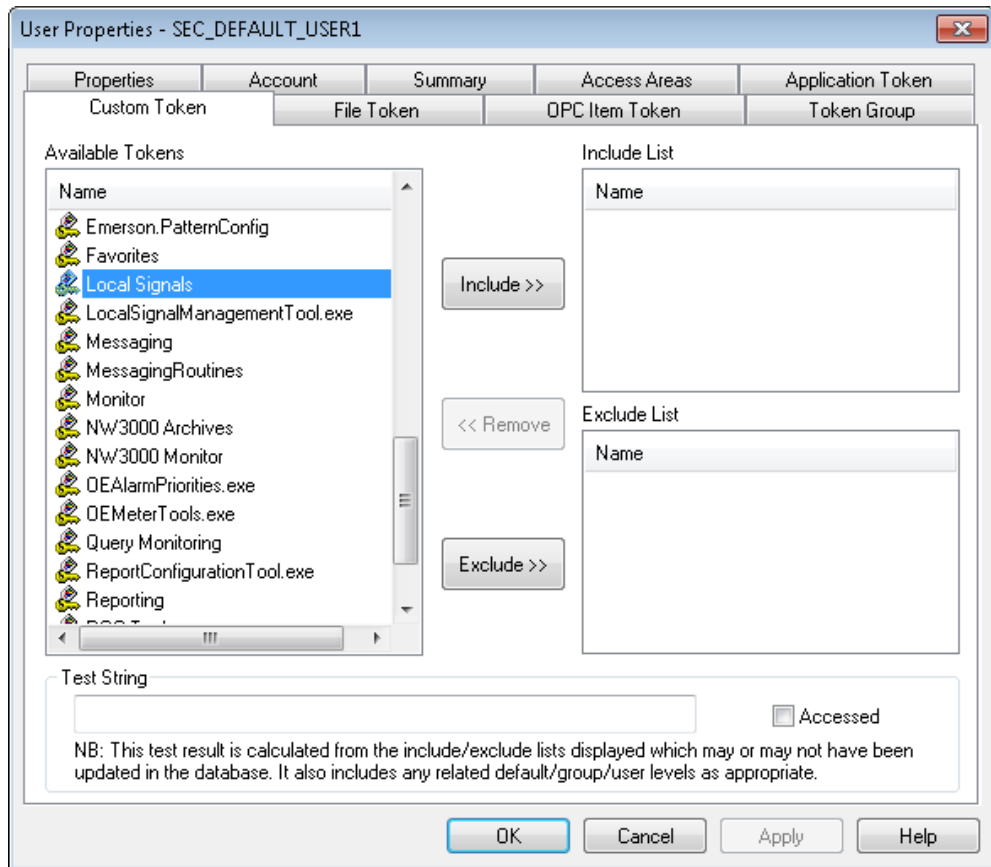
Option	Description
Available Tokens	Displays the tokens available to the User.
Include >>	Click to move the selected token from the Available Tokens list or the Exclude List to the Include List. The system removes the token from its current location.
<< Remove	Click to move the selected token from the Include List or Exclude List. The system moves the token from its current location and returns it to the Available Tokens list.

Option	Description
Exclude >>	Click to move the selected token from the Available Tokens list or the Include List to the Exclude List. The system removes the token from its current location.
Include List	<p>Displays the custom tokens that the system has awarded to the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can add items to this list by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any Custom Tokens that may have indirectly been assigned to this user via a token group, unless they have also specifically been awarded as individual tokens.</p> <p><b>Note:</b> There may be contention issues in which a user has a token explicitly Included yet has the same token excluded as a member of a token group. In this case the Include overrides the Exclude, regardless of whether the source was from an individual Token or Token Group allocation.</p>
Exclude List	<p>Displays the application tokens that the system has denied the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can move items to the Include List by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any custom tokens that may have been indirectly removed from this user via a token group, unless they have also specifically been excluded as individual tokens.</p>
Test String	Disabled on the Application Group tab.
Accessed	Disabled on the Application Group tab.
OK	Click to close the dialog; the system sends any configuration changes to the database.
Cancel	Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.
Apply	Click to send any configuration changes to the database; the system does not close the dialog.
Help	Click to access the online help system for OpenEnterprise.

### 2.4.3 User Properties: Custom Token tab

Use the Custom Token tab to award or deny users Individual Custom Tokens. This tab is very similar in operation to the Application Token tab, but these tokens do not have a displayed component.

**Figure 2-64. User Properties – Custom Token tab**



Option	Description
Available Tokens	Displays the tokens available to the User.
Include >>	Click to move the selected token in the Available Tokens list or the Exclude List to the Include List. The system removes the token from its current location.
<< Remove	Click to move the selected token from the Include List or Exclude List. The system moves the token from its current location and returns it to the Available Tokens list.
Exclude >>	Click to move the selected token from the Available Tokens list or the Include List to the Exclude List. The system removes the token from its current location.

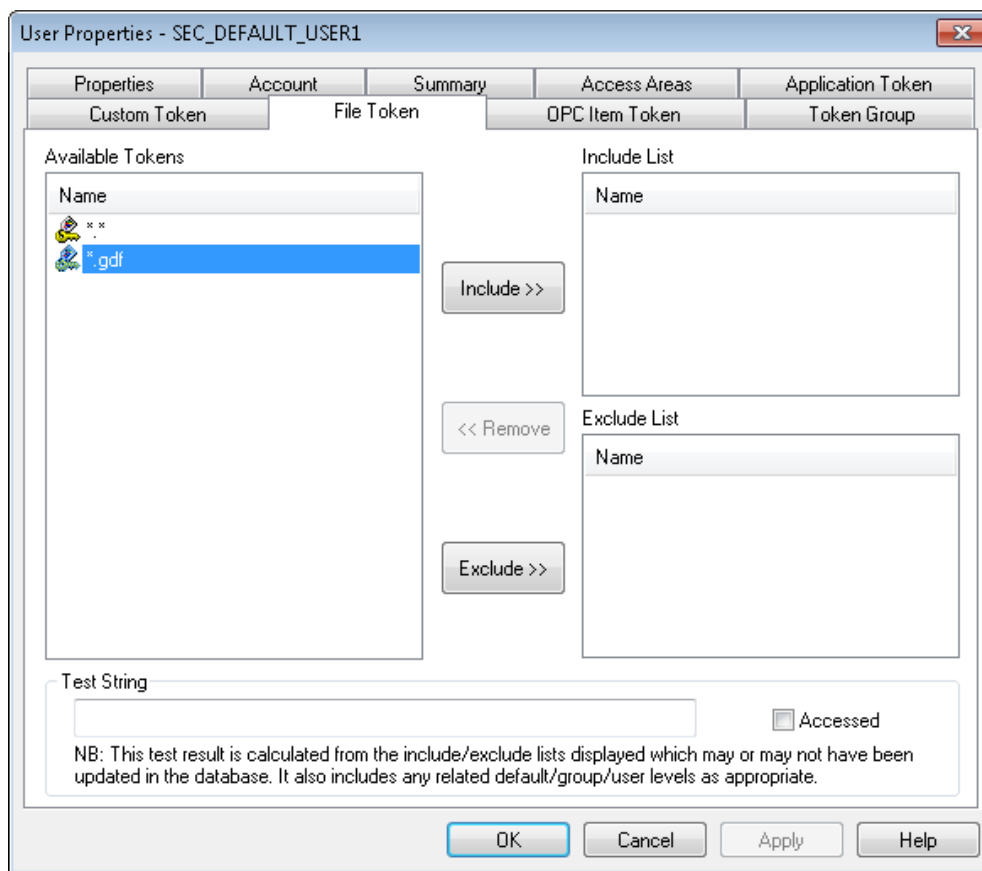
Option	Description
Include List	<p>Displays the custom tokens that the system has awarded to the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can add items to this list by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any Custom Tokens that may have indirectly been assigned to this user via a token group, unless they have also specifically been awarded as individual tokens.</p> <p><b>Note:</b> There may be contention issues in which a user has a token explicitly Included yet has the same token excluded as a member of a token group. In this case the Include overrides the Exclude, regardless of whether the source was from an individual Token or Token Group allocation.</p>
Exclude List	<p>Displays the application tokens that the system has denied the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can move items to the Include List by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any custom tokens that may have been indirectly removed from this user via a token group, unless they have also specifically been excluded as individual tokens.</p>
Test String	<p>Displays a string the system uses to verify the User's access to the token.</p> <p>If you enter a string in this field, the system performs pattern matching against the string to determine whether the user can access the token based on the currently Include and Exclude Lists for this token type.</p> <p><b>Note:</b> The system does not include any tokens indirectly assigned to the user via token groups in this pattern match. Also, the state reflects the <b>currently displayed</b> lists. Additionally, you must click <b>Apply</b> (to apply the token selections to the database) before the system can test the string for any newly added tokens.</p> <p>Refer to the <i>Token Group Matching</i> topic in the online help for an explanation of how the system matches token strings and searches the Include and Exclude list.</p>
Accessed	<p>Verifies a User's access to the token.</p> <p>The system completes this option when it verifies that the string entered in the Test String field matches a string in the User's Include List, validating that the user has access to the token.</p>
OK	<p>Click to close the dialog; the system sends any configuration changes to the database.</p>

Option	Description
Cancel	Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.
Apply	Click to send any configuration changes to the database; the system does not close the dialog.
Help	Click to access the online help system for OpenEnterprise.

## 2.4.4 User Properties: File Token tab

Use the File Token tab to award or deny individual File Tokens, which allow or deny access to files (such as certain displays) on a User’s workstation.

**Figure 2-65. User Properties – File Token tab**



Option	Description
Available Tokens	Displays the tokens available to the user.
Include >>	Click to move the selected token in the Available Tokens list or the Exclude List to the Include List. The system removes the token from its current location.

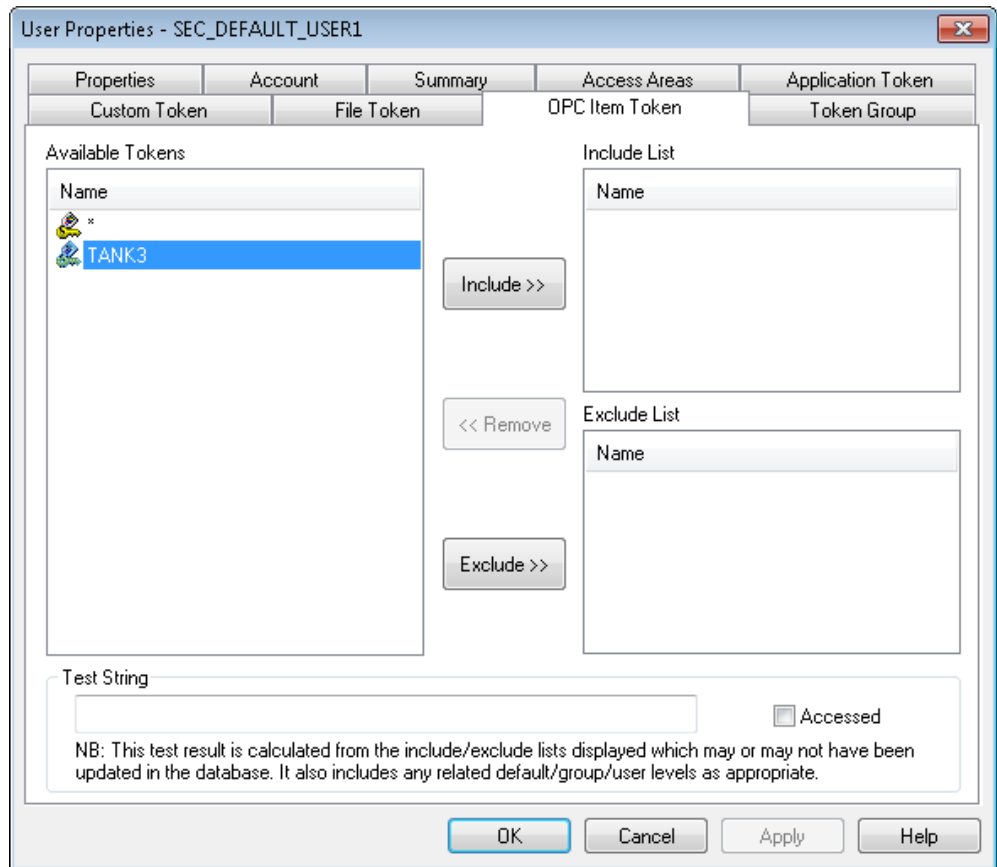
Option	Description
<< Remove	Click to move the selected token from the Include List or Exclude List. The system moves the token from its current location and returns it to the Available Tokens list.
Exclude >>	Click to move the selected token from the Available Tokens list or the Include List to the Exclude List. The system removes the token from its current location.
Include List	<p>Displays the custom tokens that the system has awarded to the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can add items to this list by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any Custom Tokens that may have indirectly been assigned to this user via a token group, unless they have also specifically been awarded as individual tokens.</p> <p><b>Note:</b> There may be contention issues in which a user has a token explicitly Included yet has the same token excluded as a member of a token group. In this case the Include overrides the Exclude, regardless of whether the source was from an individual Token or Token Group allocation.</p>
Exclude List	<p>Displays the application tokens that the system has denied the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can move items to the Include List by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any custom tokens that may have been indirectly removed from this user via a token group, unless they have also specifically been excluded as individual tokens.</p>
Test String	<p>Displays a string the system uses to verify the user's access to the token.</p> <p>If you enter a string in this field, the system performs pattern matching against the string to determine whether the user can access the token based on the currently Include and Exclude Lists for this token type.</p> <p><b>Note:</b> The system does not include any tokens indirectly assigned to the user via token groups in this pattern match. Also, the state reflects the <b>currently displayed</b> lists. Additionally, you must click <b>Apply</b> (to apply the token selections to the database) before the system can test the string for any newly added tokens.</p> <p>Refer to the <i>Token Group Matching</i> topic in the online help for an explanation of how the system matches token strings and searches the Include and Exclude list.</p>

Option	Description
Accessed	Verifies a User’s access to the token. The system completes this option when it verifies that the string entered in the Test String field matches a string in the User’s Include List, validating that the user has access to the token.
OK	Click to close the dialog; the system sends any configuration changes to the database.
Cancel	Click to close the dialog; the system does not send any configuration changes to the database.
Apply	Click to send any configuration changes to the database; the system does not close the dialog.
Help	Click to access the online help system for OpenEnterprise.

## 2.4.5 User Properties: OPC Item Token tab

Use the OPC token tab to award or deny users individual OPC tokens, which allow or deny a user from updating a value on the Graph View display.

**Figure 2-66. User Properties – OPC Item Token tab**





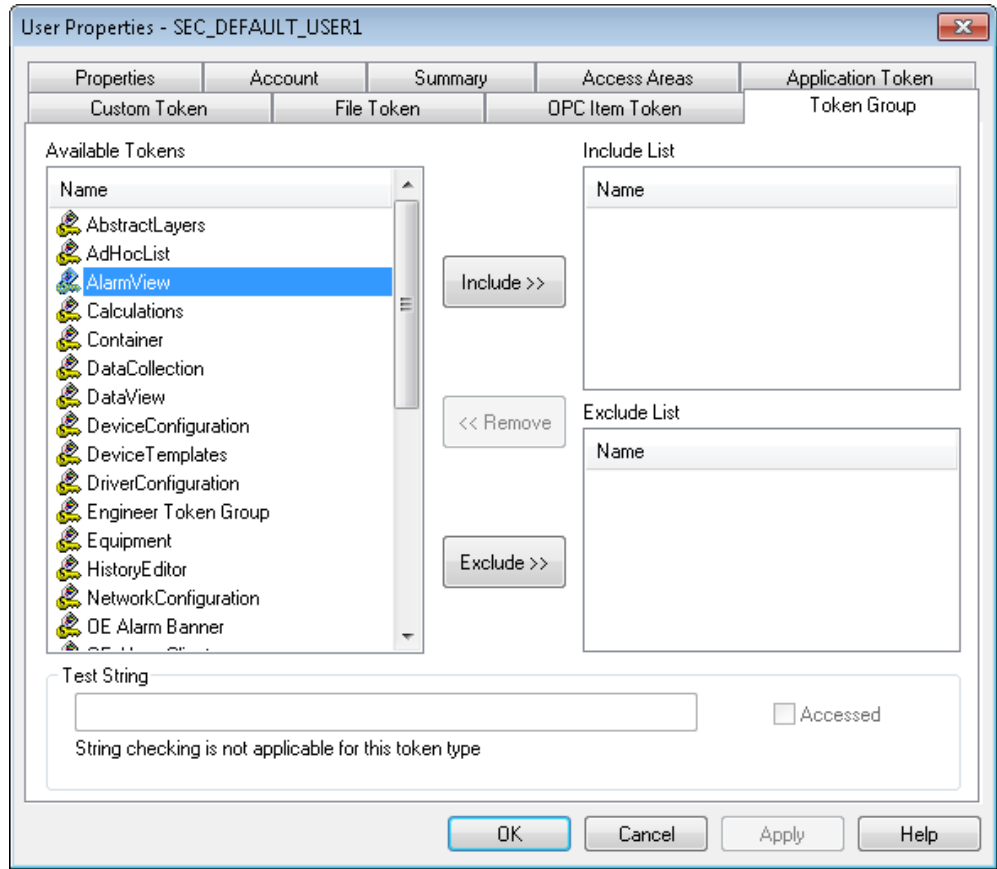
Option	Description
Available Tokens	Displays the tokens available to the User.
Include >>	Click to move the selected token in the Available Tokens list or the Exclude List to the Include List. The system removes the token from its current location.
<< Remove	Click to move the selected token from the Include List or Exclude List. The system moves the token from its current location and returns it to the Available Tokens list.
Exclude >>	Click to move the selected token from the Available Tokens list or the Include List to the Exclude List. The system removes the token from its current location.
Include List	<p>Displays the custom tokens that the system has awarded to the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can add items to this list by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any Custom Tokens that may have indirectly been assigned to this user via a token group, unless they have also specifically been awarded as individual tokens.</p> <p><b>Note:</b> There may be contention issues in which a user has a token explicitly Included yet has the same token excluded as a member of a token group. In this case the Include overrides the Exclude, regardless of whether the source was from an individual Token or Token Group allocation.</p>
Exclude List	<p>Displays the application tokens that the system has denied the User. You can remove items in this list by selecting the item and clicking <b>Remove</b>; you can move items to the Include List by selecting the item and clicking <b>Include</b>.</p> <p>This list does not display any custom tokens that may have been indirectly removed from this user via a token group, unless they have also specifically been excluded as individual tokens.</p>

Option	Description
Test String	<p>Displays a string the system uses to verify the User's access to the token.</p> <p>If you enter a string in this field, the system performs pattern matching against the string to determine whether the user can access the token based on the currently Include and Exclude Lists for this token type.</p> <p><b>Note:</b> The system does not include any tokens indirectly assigned to the user via token groups in this pattern match. Also, the state reflects the <b>currently displayed</b> lists. Additionally, you must click <b>Apply</b> (to apply the token selections to the database) before the system can test the string for any newly added tokens.</p> <p>For an explanation of how the system matches token strings and searches the Include and Exclude list, refer to the online help's Token Group Matching topic for.</p>
Accessed	<p>Verifies a User's access to the token.</p> <p>The system completes this option when it verifies that the string entered in the Test String field matches a string in the User's Include List, validating that the user has access to the token.</p>
OK	<p>Click to close the dialog; the system sends any configuration changes to the database.</p>
Cancel	<p>Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.</p>
Apply	<p>Click to send any configuration changes to the database; the system does not close the dialog.</p>
Help	<p>Click to access the online help system for OpenEnterprise.</p>

### 2.4.6 User Properties: User Token Group tab

This dialog enables a **system administrator** to configure individual tokens of any type to be included within the token group. You can then award or deny the whole token group to users or groups. This feature simplifies the process of assigning commonly used sets of tokens to users or groups.

Figure 2-67. User Properties – Token Group tab



Option	Description
Available Tokens	Displays the tokens available to the User.
Include >>	Click to move the token selected in the Available Tokens list or in the Exclude List to the Include List. The system removes the token from its previous location. <b>Note:</b> This button activates when you select a token.
<< Remove	Click to move the currently selected token in the Include List or Exclude List to the Available Tokens list. The system removes the token from its previous location. <b>Note:</b> This button activates when you select a token.
Exclude >>	Click to move the selected token from the Available Tokens list or in the Include List to the Exclude List. The system removes the token from its previous location. <b>Note:</b> This button activates when you select a token.

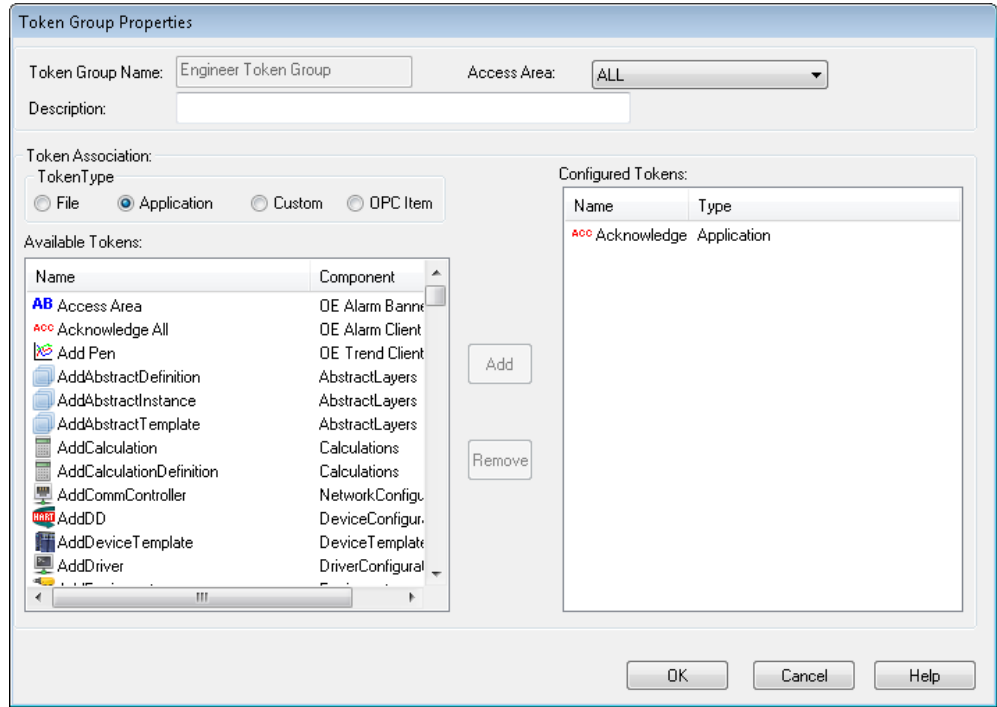
Option	Description
Include List	<p>Displays the custom tokens assigned to the user. Click <b>Remove</b> to remove selected items from this list. Click <b>Include</b> to move selected items from the Exclude List to this list.</p> <p>This list <b>does not</b> display any custom tokens that may have indirectly been assigned to this user via a token group, unless they were assigned as individual tokens.</p> <p><b>Note:</b> There may be contention issues in which a user has a token explicitly Included yet has the same token Excluded as a member of a token group. In this case the Include <b>overrides</b> the Exclude, regardless of whether the source was from an individual token or token group allocation.</p>
Exclude List	<p>Displays application tokens that have been denied to the user from this configuration page. Click <b>Remove</b> to remove items from this list. Click <b>Include</b> to move selected items from this list to the Include list.</p> <p><b>Note:</b> This list does not display any custom tokens that may have indirectly been removed from this user by means of a token group, unless they have <b>also</b> been specifically excluded as individual Tokens.</p>
Test String	Disabled on the Token Group tab.
Accessed	Disabled on the Token Group tab.
OK	Click to close the dialog; the system sends any configuration changes to the database.
Cancel	Click to close the dialog; the system <b>does not</b> send any configuration changes to the database.
Apply	Click to send any configuration changes to the database; the system does not close the dialog.
Help	Click to access the online help system for OpenEnterprise.

## 2.5 Token Group Properties

This dialog enables a **system administrator** to configure the tokens included within a User-created token group. Access this dialog by double-clicking any Token Group displayed in either the left or right panes of the Security Configuration tool. You cannot edit the default application Token Groups; additionally, the system disables the Token Association section of the dialog if you select a default token group.

Once you create the whole token group, you can include or exclude it from a User's or a group's security profile. This simplifies the process of assigning commonly used token sets to Users.

**Figure 2-68. Token Group Properties dialog**



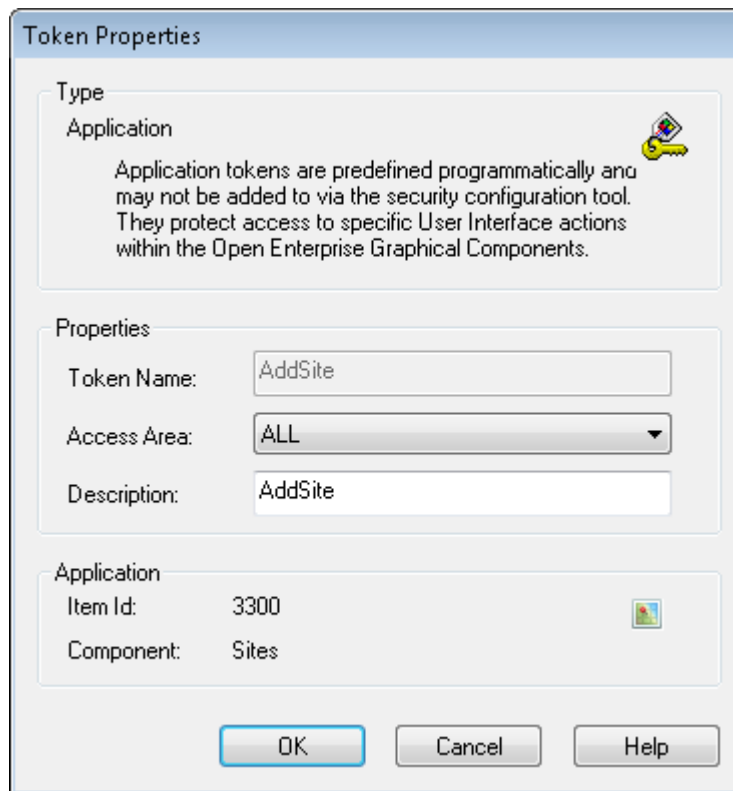
Option	Description
Token Group Name	Displays the name given to the token group when it was created. Once you create the token group, you cannot edit this field.
Access Area	Click ▼ to display a drop-down menu to select a different access area for this token. By default, ALL is the default for a new token.
Description	Provides a longer description of this token group.
Token Type	Indicates the type of tokens in this token group. As you sequentially elect each token type, the system completes the Available Tokens list with available tokens of that type. You can then select the tokens to include in this token group.
Available Tokens	Lists the available tokens (based on the selected token types). The Name column indicates the name of the token; the Component column indicates the OpenEnterprise component for which this token is valid. The system sorts this display by component, but you can click on a column heading to sort this list by either name or component. Use the scroll bar to display the entire column.
Configured Tokens	Displays the names of the OEView components for which the application token is valid. <b>Note:</b> This column applies <b>only</b> to Application tokens.

Option	Description
Add	Click to add the selected tokens in the Available Tokens list to the Configured Types list.
Remove	Click to remove selected tokens from the Configured Types list and the token group.
OK	Click to close the dialog; the system applies any configuration changes to the database and finalizes the token group.
Cancel	Click to close the dialog; the system does not apply any changes to the database.
Help	Click to access the online help system for OpenEnterprise.

## 2.6 Token Properties Dialog

This dialog enables a **system administrator** to change the description or access area of any individual token. *Figure 2-69* shows a dialog for an application token. Dialogs for the other three token types are similar, but do not display an Item Id or Component value.

**Figure 2-69. Token Properties dialog**



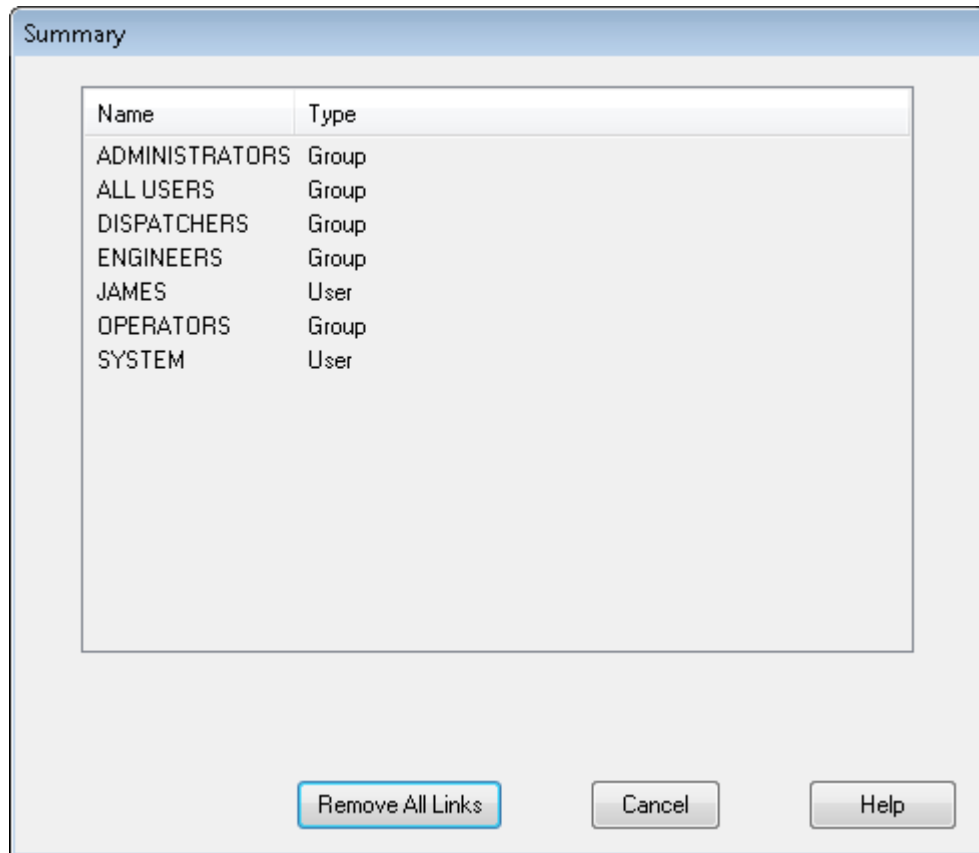
Option	Description
--------	-------------

Option	Description
Token Name	This <b>display-only</b> field shows the primary key in the Token table.
Access Area	Click ▼ to display a drop-down list an OpenEnterprise System Administrator can use to select a different access area for this token. For a new token, the default is ALL.
Description	Provides more descriptive information for this token.
OK	Click to close the dialog; the system applies any configuration changes to the database.
Cancel	Click to close the dialog; the system <b>does not</b> apply any changes to the database.
Help	Click to access the online help system for OpenEnterprise.

## 2.7 Token Summary Dialog

This dialog displays any users and groups that currently have the selected token in their Include or Exclude list.

**Figure 2-70. Token Summary dialog**

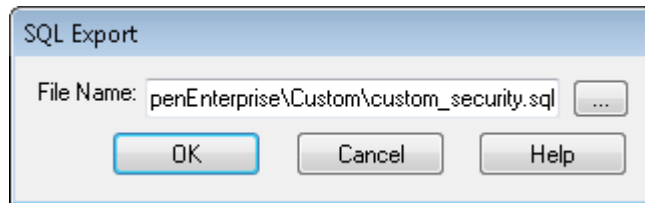


Option	Description
Remove All Links	Click to remove the selected link between any associated users or groups.
Cancel	Click to close the dialog; the system <b>does not</b> apply any changes to the database.
Help	Click to access the online help system for OpenEnterprise.

## 2.8 SQL Import-Export File Dialog

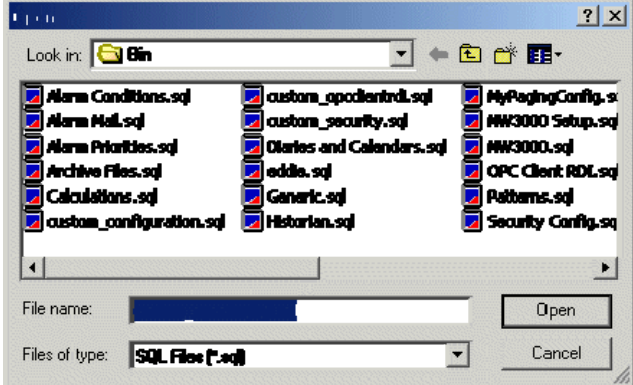
The SQL Export dialog enables you to override the default filename and location to which the system saves the SQL Export.

**Figure 2-71. SQL Export dialog**



Option	Description
File Name	<p>Displays the name and file location for the Export file. During exports, the system automatically selects this file and places it in the <i>File Name</i> field. You can manually enter a different location or file name or use the browse button to select another name and location.</p> <p>By default, the system names the Export file <i>custom_&lt;Component&gt;.SQL</i>, where <i>&lt;Component&gt;</i> indicates the OpenEnterprise configuration component from which you initiate the Export. The system writes the file to the standard OpenEnterprise export file directory. The Status file has a default name of <i>custom_&lt;Component&gt;.txt</i>.</p> <p><b>Note:</b> If a file already exists in the directory with the specified filename, then you should rename the existing file to append old to its name, that is <i>custom_opcclientrdi.sql.old</i>.</p>



Option	Description
Browse Button	Click to display a standard Windows File Open dialog. Use it to select a file for import, export, or Saving Import Status.
	
OK	Click to begin the selected action. The system closes the dialog when the action completes.
Cancel	Click to cancel the selected action and close the dialog.
Help	Click to display the online help system for OpenEnterprise.

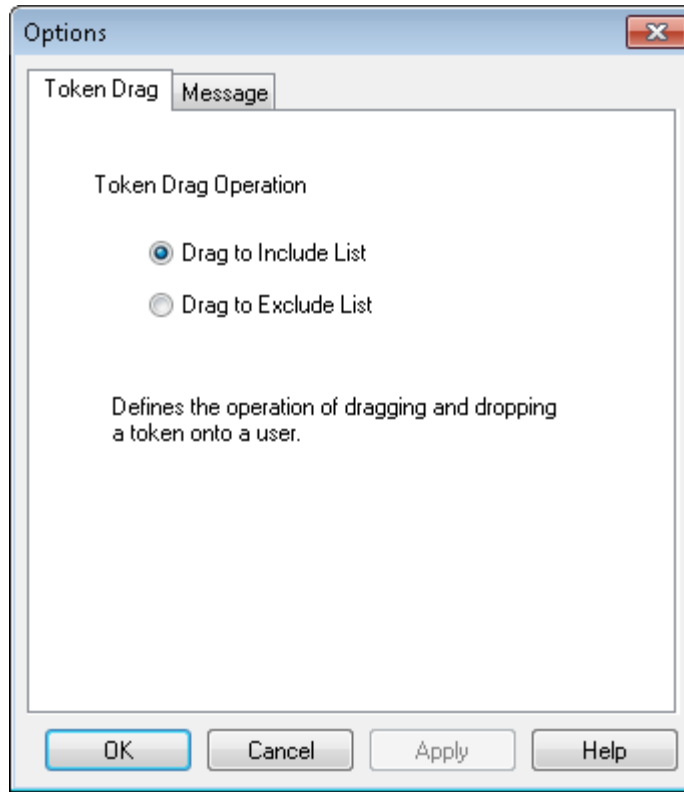
## 2.9 Options Dialog

Use this dialog to control how the system manages token and message functionality in the Security Configuration tool.

### 2.9.1 Options Dialog: Token Drag Tab

This tab enables a **system administrator** to configure the way that token drag and drop functionality works within the Security Configuration tool.

Figure 2-72. Options dialog: Token Drag tab



Option	Description
Drag to Include List	Adds a token or token group selected from the right pane and dragged and dropped onto a user or user group within the left pane to the <b>Included</b> List for the user or user group.
Drag to Exclude List	Adds a token or token group selected from the right pane and dragged and dropped onto a user or user group within the left pane to the <b>Excluded</b> List for the user or user group.

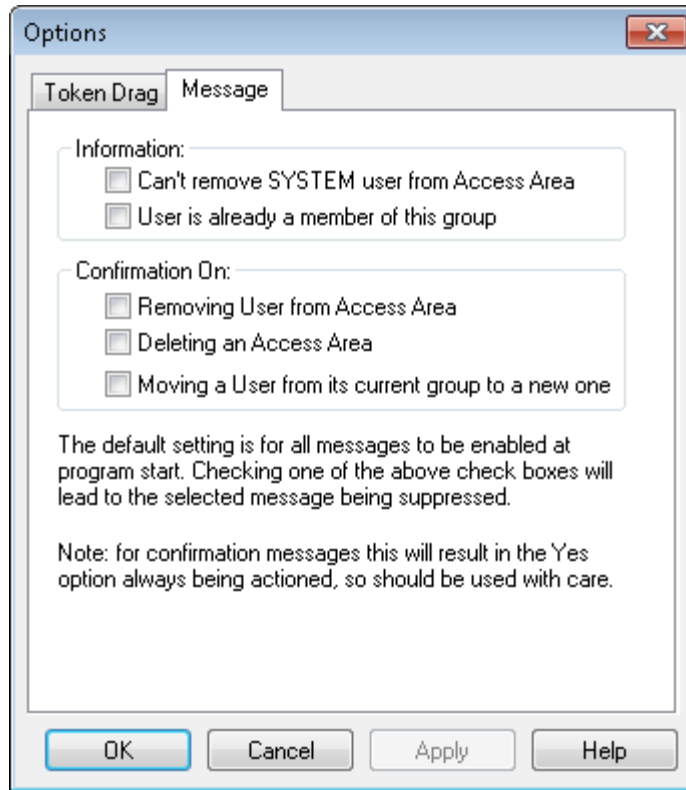
## 2.9.2 Options Dialog: Message Tab

This tab allows a **system administrator** to suppress system information and confirmation messages. You may find it useful to suppress information/confirmation messages during multi-selection moves.

### Note

At program start, the system resets these (that is, de-selects) options so that all messages are seen.

**Figure 2-73. Options dialog: Message tab**



Option	Description
Can't Remove SYSTEM User from Access Area	Controls whether the system displays an informational message when you attempt to remove the SYSTEM user from an access area (by default, a SYSTEM user must always be in every access area). Select this option to suppress this message.
User is already a member of this group	Controls whether the system displays an informational message when you attempt to drag-and-drop a user into a group with which they are already associated. Select this option to suppress this message.
Removing User from Access Area	Controls whether the system displays a confirmation message when you remove a user from an access area. Select this option to suppress this message.
Deleting an Access Area	Controls whether the system displays a confirmation message when you delete an access area. Select this option to suppress this message.
Moving a User from its current group to a new one	Controls whether the system displays a confirmation message when you move a user from its current user Group to a new user Group. Select this option to suppress this message.



## 3 Using the Security Configuration Tool

The Security Configuration tool allows OpenEnterprise System Administrators to create, modify, and delete security-related objects such as Users, groups, tokens and access areas. OpenEnterprise System Administrators can also grant or deny tokens and access areas to Users and groups, thus providing a comprehensive and integrated security configuration.

### 3.1 Managing Security Objects

Security objects are **groups** you define based on the types of users (such as Dispatchers, Engineers, Operators, Guests, etc.) you believe will use the system and **Users** (specific Ids PUBLIC or SYSTEM). You also need to determine the OpenEnterprise component – workstation or server – to which these groups have access privileges.

#### 3.1.1 Creating a New User

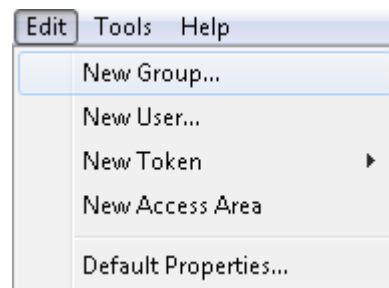
For further information, refer to section 2.1.2.2, *Creating a New User*.

#### 3.1.2 Creating New User Groups

You can create a new group using any of the following methods:

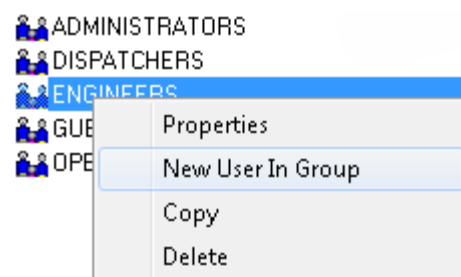
- Select **Edit > New Group** from the Security Configuration tool's menu bar:

**Figure 3-1. New Token option, Edit menu**



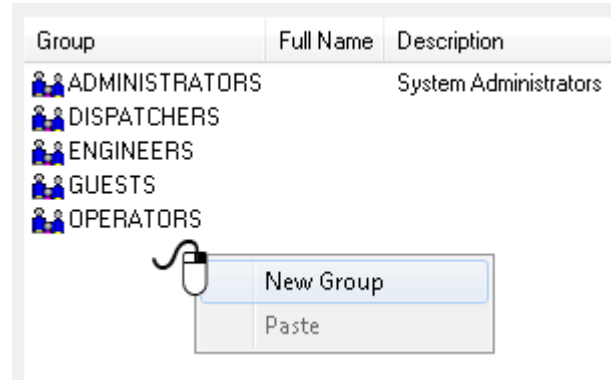
- Right-click a user group and select **New User In Group** from the context menu:

**Figure 3-2. New User in Group menu option**



- Select a groups node, right-click in the List pane, and select **New Group** from the context menu:

**Figure 3-3. New Group context menu option**

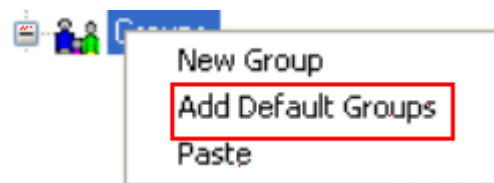


Once you select the **New Group** menu option, the List page displays all the currently configured groups, inserting a new blank entry at the top of the list. Enter a valid unique name and press the **Enter** key. The system displays the Groups Properties dialog. Use it to define further configuration details.

### 3.1.3 Adding Default Groups

To add a Default Group, right-click the Groups icon and select **Add Default Groups** from the context menu:

**Figure 3-4. Add Default Groups context menu option**

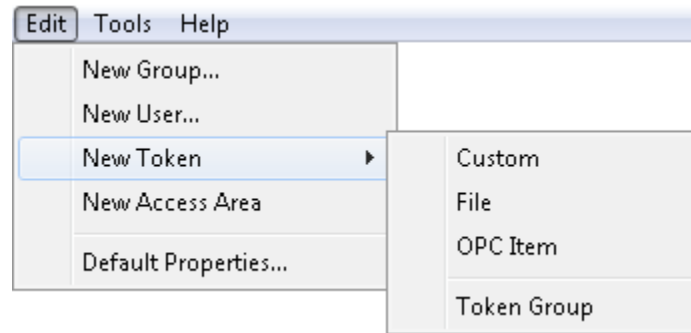


### 3.1.4 Creating New Token Groups

You can create a new token group using any of the following methods:

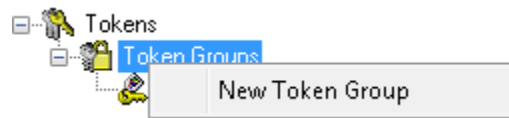
- Select the **Edit > New Token > Token Group** from the Security Configuration tool's menu bar:

**Figure 3-5. New Token menu option**



- Expand the Tree pane, right-click the Token Groups icon, and select **New Token Group** from the context menu:

**Figure 3-6. New Token Group context menu option**



Once you select this menu item, the List pane displays all the currently configured token groups, inserting a new blank entry at the top of the list. Enter a valid unique name and press the **Enter** key. The system displays the Token Group Properties dialog. Use it to define further configuration details.

**Note**

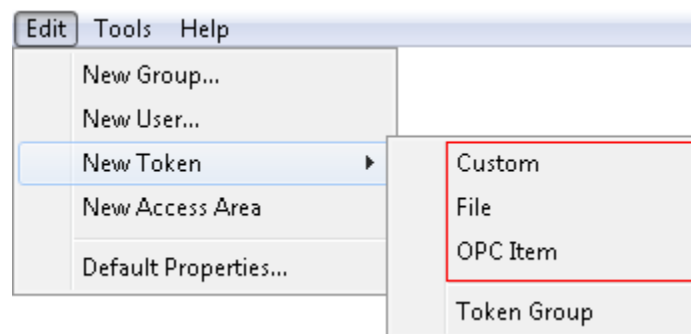
Once you enter the new token group name you cannot change it.

### 3.1.5 Creating Custom, File and OPC Item Tokens

You can create new custom tokens, file tokens, and OPC item tokens using one of the following methods:

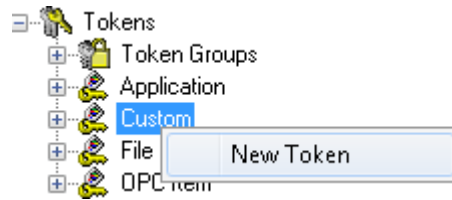
- Select **Edit > New Token** from the Security Configuration tool's menu bar. Then select the desired option (Custom, File, or OPE Item) from the sub-menu.

**Figure 3-7. New Token menu options**



- Right-click a token icon from the Tree pane and select **New Token** from the context menu.

**Figure 3-8. New Token context menu option**



Once you select this menu item, the List pane displays all the currently configured token groups of the type you have chosen, inserting a new blank entry at the top of the list. Enter a valid, unique, case-sensitive name and press the **Enter** key. The system displays the Token Group Properties dialog. Use it to define further configuration details.

### Note

Once you enter the new token name you cannot change it.

## 3.1.6 Creating New Application Tokens

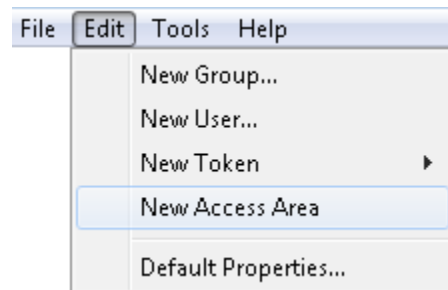
You **cannot** create a new application token using the Security Configuration tool. For an explanation of application tokens, refer to the *All Application Tokens* topic in the OpenEnterprise online help file.

## 3.1.7 Creating New Access Areas

You can create a new access area using any of the following methods:

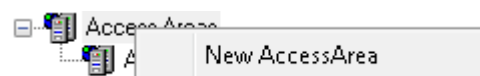
- Select **Edit > New Access Area** from the Security Configuration tool's menu bar.

**Figure 3-9. New Access Area menu option**



- Right-click the Access Area node on the Tree pane and select **New Access Area** from the context menu.

**Figure 3-10. New Access Area context menu**





Once you select New Access Area, the List pane displays all the currently configured access areas, inserting a new blank entry at the top of the list. Enter a valid, unique, case-sensitive name and press the **Enter** key. The system displays the Access Area Properties dialog. Use it to define further configuration details.

## 3.2 Modifying Security Objects

Use these procedures to modify security objects.

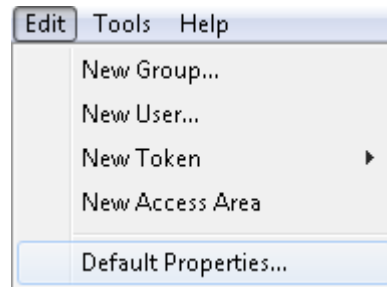
### 3.2.1 Modifying Default Group Settings

You can modify the Default Group's security settings using the following methods:

- Select **Edit > Default Properties** from the Securing Configuration tool's menu bar.

---

**Figure 3-11. Default Properties menu option**



- Right-click the Default Group icon on the Tree pane and select Properties from the context menu.

---

**Figure 3-12. Properties context menu option**



When you select either of these options, the system displays the Default Properties dialog. Use it to define further configuration details.

---

#### Note

A good practice is to include only a bare minimum of necessary tokens in the Default Group, since any tokens you include and do not exclude in the Default Group cannot subsequently be excluded from any other group or user.

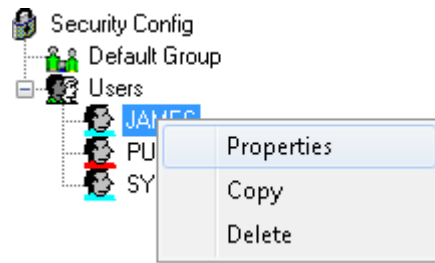
---

### 3.2.2 Modifying User Account Settings

You can modify a user's Security settings using the following methods:

- Right click a user's icon in the Tree pane and select **Properties** from the context menu.

**Figure 3-13. Properties context menu option**



- Double-click a user's icon in the Tree pane.

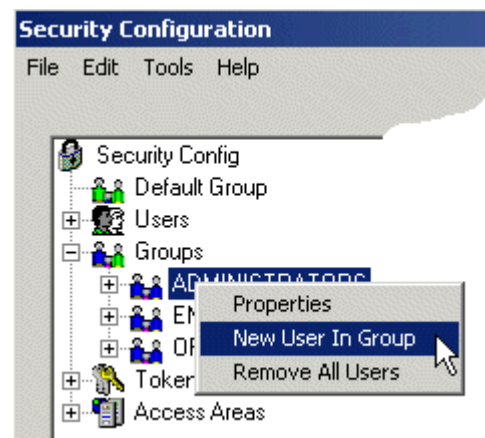
When you use either of these options, the system displays the User Properties dialog. Use it to define further security settings.

## 3.2.3 Adding a New User to a Group

You can add a new user to a user group using one of the following methods:

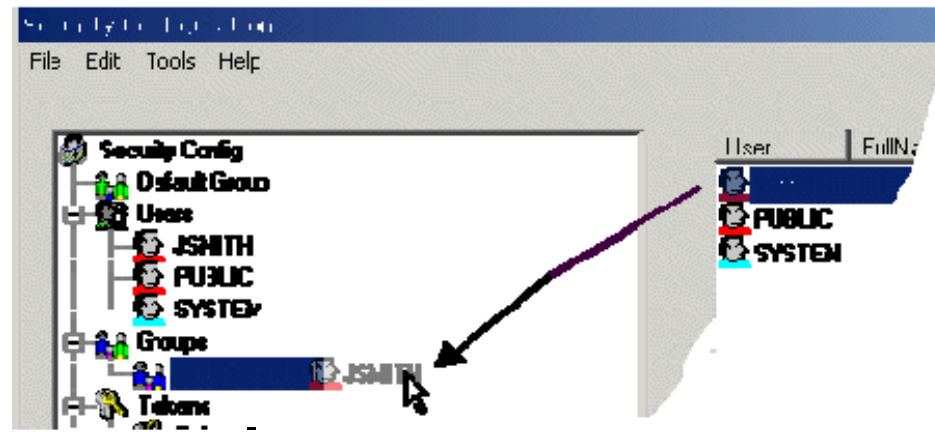
- Right-click the group to which you want to add the new user and select **New User in Group** from the context menu.

**Figure 3-14. New User In Group menu option**



- Drag and drop the user from the List pane to a user group in the Tree pane.

**Figure 3-15. Drag and drop User to the Tree**

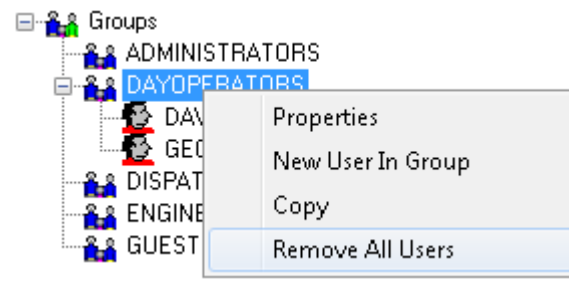


### 3.2.4 Removing All Users from a Group

To remove all Users from a group:

1. Right-click the group from which you want to remove all Users and select **Remove All Users** from the context menu.

**Figure 3-16. Remove All Users menu option**



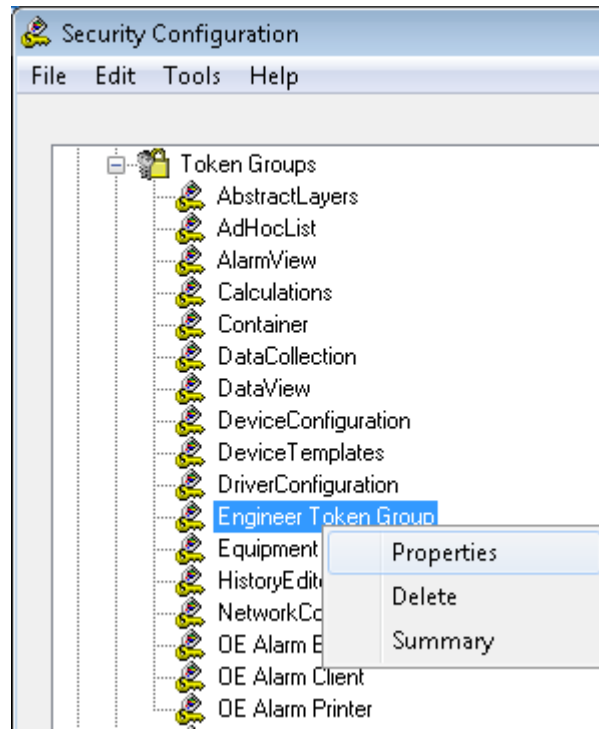
2. Once you click **Remove All Users**, the system displays a warning dialog asking you to verify the action. Click **Yes** to proceed with the deletion or **No** to cancel the process.

### 3.2.5 Modifying Token Groups

You can modify token groups using the following methods:

- Right-click a token group and select **Properties** from the context menu.

**Figure 3-17. Properties context menu option**



- Double-click a token group.

When you use either of these options, the system displays the Token Group Properties dialog. Use it to define further security settings.

**Note:** OpenEnterprise automatically manages settings for application token groups. You cannot change these values.

## 3.2.6 Linking Tokens with a Token Group

The system provides two ways you can link tokens with a token group.

- Use the Token Group's Properties dialog.
- Select a token from the List pane and drag and drop it onto the token group in the Tree pane.

## 3.2.7 Linking Tokens or Token Groups with Users or Groups

The system provides two ways you can link tokens or token groups with Users or groups

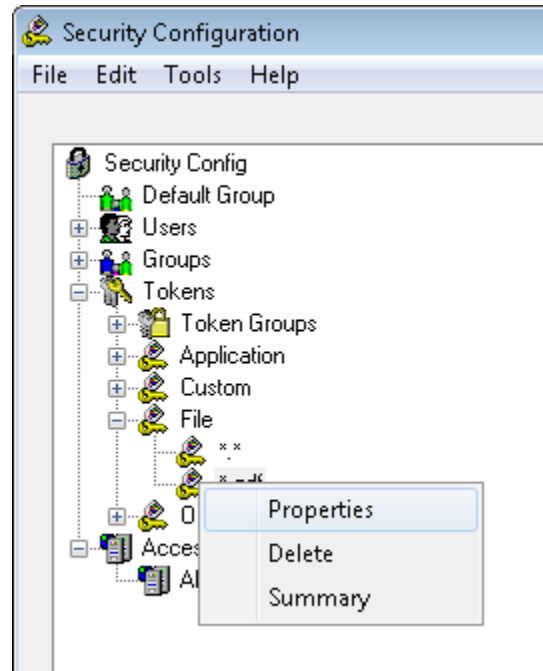
- Use the User or Group Properties dialog.
- Select a token from the List pane and drag and drop it onto the user or group in the Tree pane

## 3.2.8 Modifying Custom, File and OPC Item Tokens

There are two ways to modify Custom, File or OPC Item tokens.

- Right-click on a Custom, File, or OPC Item token and select **Properties** from the context menu.

**Figure 3-18. Token Properties context menu option**



- Double-click any Custom, File, or OPC Item Token

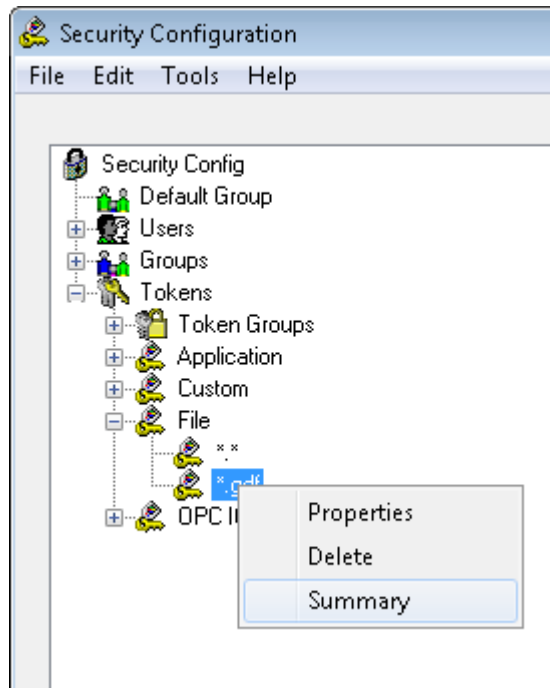
The system displays the Token Properties dialog. Use it to change the description for the selected token.

**Note:** You can only modify the descriptions or access area for these types of tokens.

## 3.2.9 Viewing and Breaking Token Links

When you place a token group into the Include or Exclude token list for a user or group, the token group “has a link” to that the user or group. You can view and remove these links using the Token Summary dialog, which you access by selecting **Summary** on a token context menu.

**Figure 3-19. Summary Token menu option**

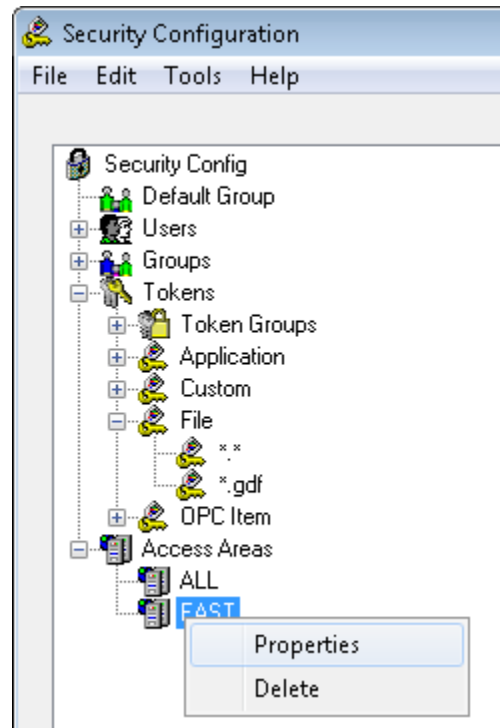


## 3.2.10 Modifying Access Areas

The system provides two ways to modify access areas.

- Right-click an access area and select **Properties** from the context menu.

Figure 3-20. Properties context menu option



- Double-click any access area.

The system displays the Access Area Properties dialog. Use it to modify the description for the selected access area.

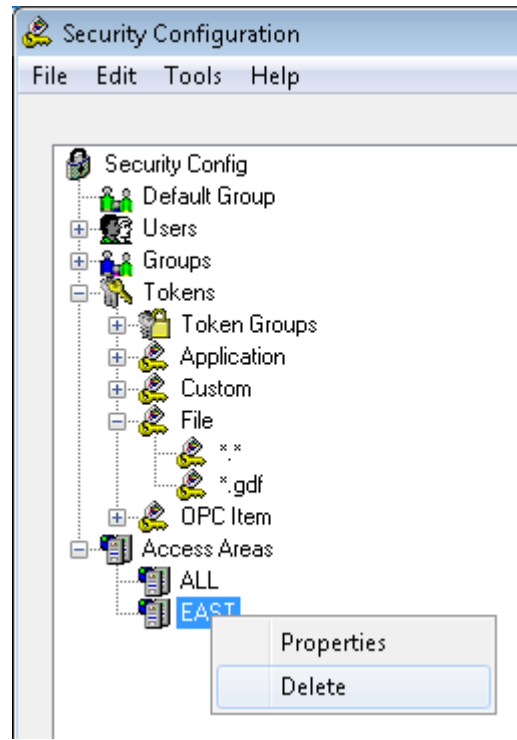
**Note:** You can **modify** only the description.

### 3.2.11 Deleting Security Objects

To delete a User, group, token or access area:

1. Right-click the object and select **Delete** from the context menu.

**Figure 3-21. Delete context menu option**



**Note:** You cannot delete the default OpenEnterprise System Administrator (SYSTEM); any application token group; any application token; any token associated with a User, group, or token group; or any access area associated with a user or group. -

2. Once you click **Delete**, the system displays a warning dialog asking you to verify the action. Click **Yes** to proceed with the deletion or **No** to cancel the process.

## 3.3 Logging into the Container for the First Time

With OpenEnterprise version 3x, the default SYSTEM and PUBLIC user password is blank (NULL). During your initial logon to the Container on the server, the system prompts you to change the password.

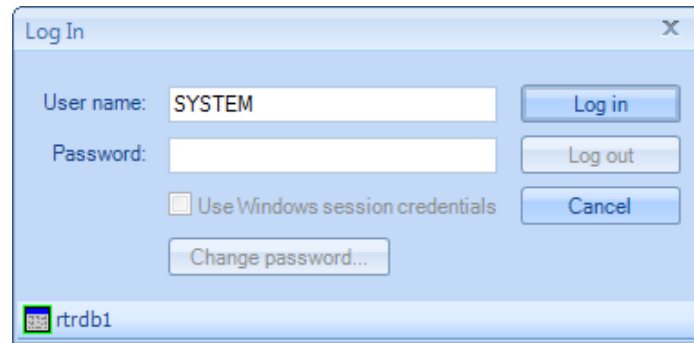
**Note:** The default database build sets the user's *mustChangePassword* attribute to **TRUE**.

The sequence of events for the first-time login is:

1. Install the OpenEnterprise Server (this creates and starts the OpenEnterprise session).
2. Open the Container to configure OpenEnterprise. The system displays the Log In dialog.

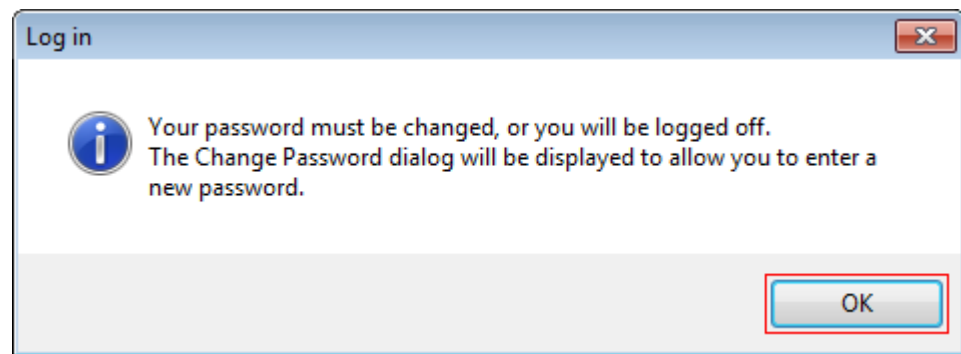


**Figure 3-22. Log In dialog**



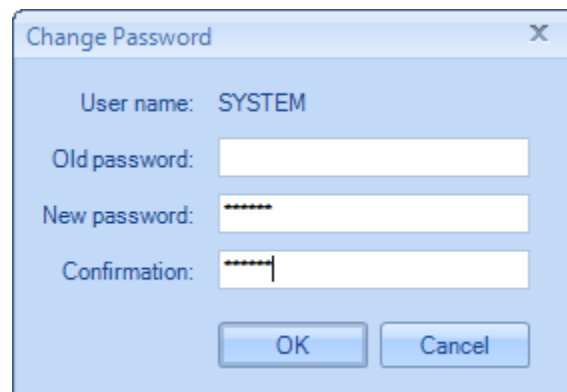
3. Log in as **SYSTEM** and click **Log in** (do not enter a password).
4. The system prompts you to change the password (this is a standard feature of OpenEnterprise).

**Figure 3-23. Log In password prompt**



5. Click **OK**. The system displays the Change Password dialog.

**Figure 3-24. Change Password dialog**

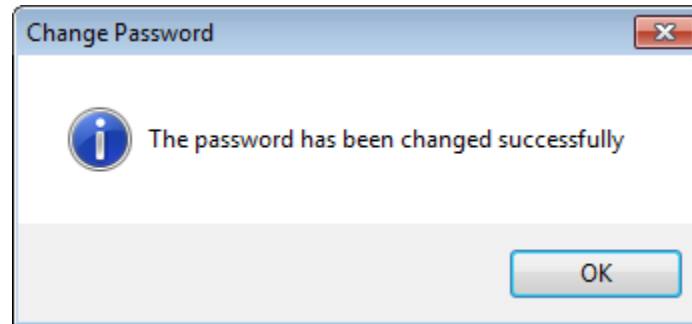


6. Enter the password for the selected user in the New Password field, and enter it again in the Confirmation field. Click **OK**.

**Note:** Leave the **Old password** field blank; it is **null** for the **first** login.

Provided the passwords match, the system displays a confirmation message.

**Figure 3-25. Changed password confirmation dialog**



Click **OK**. The initial OpenEnterprise logon begins.

## 3.4 Changing the SYSTEM User Password

### CAUTION

**Do not** change the SYSTEM password from a standalone workstation. **Always** change the SYSTEM password on the OpenEnterprise server.

As soon as possible, you must change the password for the SYSTEM user, first on the OpenEnterprise server than then on any associated servers. In quick succession, update the computers in a OpenEnterprise system in the following order:

1. OpenEnterprise Server(s)
  - a) SingleBox Solution and Standalone Server
  - b) Redundant System
2. Remote Communication Controller(s)
3. Reporting and Messaging Server(s)

The following sections detail the procedures to follow to change the SYSTEM user password for each of the following possible configurations:

- SingleBox Solution and Standalone Server
- Redundant System
- Remote Communication Controller
- Reporting or Messaging Server
- Standalone Workstation

### 3.4.1 On a SingleBox Solution and Standalone Server

To change the SYSTEM user password on a SingleBox solution or a standalone server

1. Start the OpenEnterprise Container.
2. Logon as SYSTEM user.
3. Select **Security > Change password** option
4. Enter the old password, new password, and confirm the new password. Click **OK**.

The Security Manager updates the SYSTEM user password. There is no need to restart the OpenEnterprise Session.

### 3.4.2 On a Redundant System

To change the SYSTEM user password on a redundant system:

1. Start the OpenEnterprise Container on the current master server.
2. Logon as SYSTEM user.
3. Select **Security > Change password** option
4. Enter the old password, new password, and confirm the new password. Click **OK**. The Security Manager updates the database and the OpenEnterprise.ini file.
5. Copy the OpenEnterprise.ini file (located at *C:\ProgramData\Emerson\OpenEnterprise\Application Data\OpenEnterprise.ini*) to the standby server.

**Note:** There is no need to perform a failover or restart the redundant session

### 3.4.3 On a Remote Communication Controller

To change the SYSTEM user password on a remote communication controller:

On the Remote Communication Controller computer, run the RemotePasswordUpdate application and enter the new password.

**Note:** The system stores the RemotePasswordUpdate executable file at *C:\Program Files\Emerson\OpenEnterprise\Bin\RemotePasswordUpdate.exe*.

### 3.4.4 On a Reporting or Messaging Server

To change the SYSTEM user password on a Reporting or Messaging Server:

1. On the Reporting or Messaging Server computer, run the RemotePasswordUpdate application and enter the new password.

**Note:** The system stores the RemotePasswordUpdate executable file at *C:\Program Files\Emerson\OpenEnterprise\Bin\RemotePasswordUpdate.exe*.

## 3.4.5 On a Standalone Workstation

 **CAUTION**

**Do not** change the SYSTEM password from a standalone workstation. **Always** change the SYSTEM password on the OpenEnterprise server.

---

## 4 Security Group Privileges Editor

The Security Group Privileges Editor (which you access by selecting Security Group Privileges from the Administrative Tools pane) enables Administrative users to set table or view privileges for user groups.

Table and View privileges consist of:

- **None**  
Users who belong to the group cannot view or change any of the data in the table or view.
- **RO (Read-Only)**  
Users who belong to the group can view the data in the table or view, but cannot change it.
- **RW (Read-Write)**  
Users who belong to the group can view and change the data within the table or view, including modifying, inserting, and deleting objects.

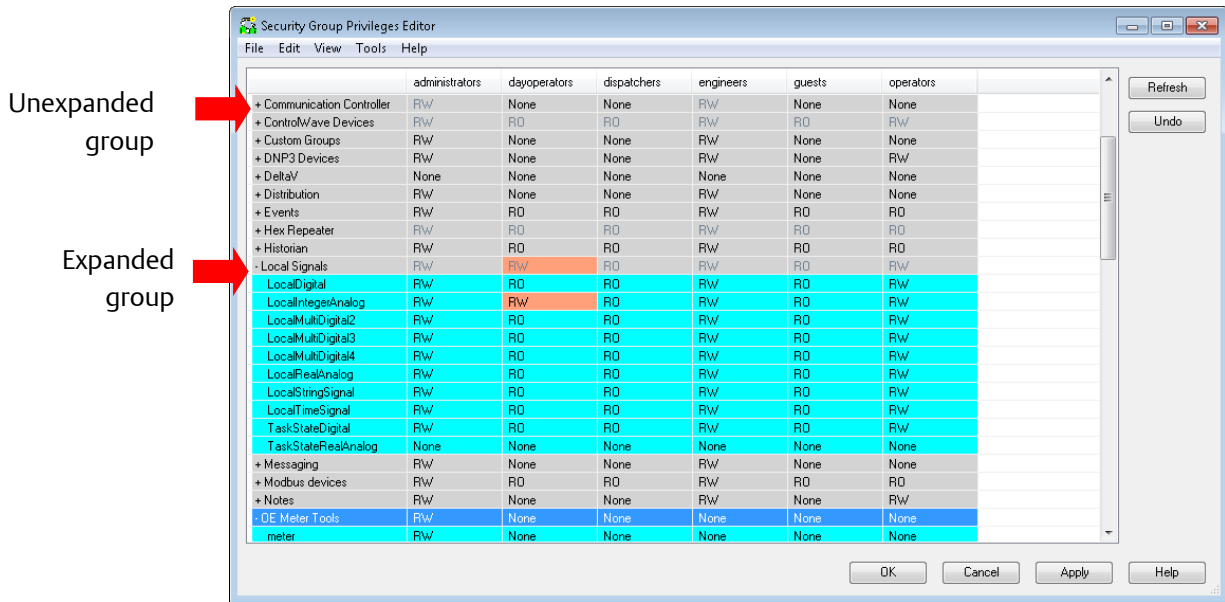
Once you define table and view privileges for each user group, you assign each user to the appropriate group. The user then has the database privileges required to do their job.

It is important to remember that only views contain access area security, such that a user can only view objects within a table that belong to the access areas assigned to them. Giving a user **RW** or **RO** privileges on the corresponding table gives that user access to **all** objects within the table.

### 4.1 Main Dialog

The Security Group Privileges Editor enables Administrative users to set table or view privileges for user groups. The Main dialog consists of a grid of vertical table groups and horizontal user groups (horizontal). The system groups tables and views into functional areas for greater clarity (see *Figure 4-1*).

Figure 4-1. Security Group Privileges Editor



Option	Description
OK	Click to close the Security Group Privileges Editor. Before closing, the system submits any configuration changes you have made to the database and displays the SQL Execution dialog. Click <b>Close</b> ; the system both closes the SQL Execution dialog and the Security Group Privileges Editor.
Cancel	Click to close the dialog. The system discards any configuration changes you may have made but not applied.
Apply	Click to submit any configuration changes to the database. The system displays the SQL Batches dialog until the system has submitted all SQL batches to the database. When the system closes the SQL Batches dialog it redisplay the Main dialog. You can continue with any configurations. The system returns any pink cells (indicating changes) to the default color (gray for table/view groups and light blue for tables and views).
Refresh	Click to refresh the whole grid display on the Main Dialog. The system returns all changed cells to the <b>value</b> they had when the Security Group Privileges Editor last read the database and to their default colors (gray for table/view groups and light blue for tables or views). Click <b>Refresh</b> when you want to get rid of <b>all</b> changes and start over again. To undo the last few changes, click <b>Undo</b> .

Option	Description
Undo	Click to undo changes made on the grid in reverse order one at a time. For instance, if you make three separate changes, then decide to keep only the first change, click this button two times.
Help	Click to open the OpenEnterprise online help file at a topic related to this page. Click <b>F1</b> to access context sensitive help for this dialog.

### 4.1.1 Groups

To simplify the display, the system groups the more important table and views together according to functionality. It colors a group grey and places a plus sign (+) to the left of a group when the group is compressed. When you click the plus sign to expand the group, it changes to a minus sign (-) and the component tables and views appear in light blue under the group (see *Figure 4-1*).

### 4.1.2 Tables and Views

As noted, the system displays tables and views with a light blue background, groups them according to functionality, and slightly indents them to visually mark them. Since you cannot expand tables and views, they have neither plus signs nor minus signs.

You can usually identify tables by the presence of an underline in their names (*realanalog\_table* or *dvi\_device*). Names for views have no underline (i.e. *realanalog*), except for the users table. It is important to grant privileges on the views **only** for non-administrative users, since the views contain the accessarea security that restricts the viewing of objects according to accessarea.

### 4.1.3 Assigning Privileges

When you select a cell that defines a privilege for a user group, the system displays a drop-down list.

**Figure 4-2. Security Group Privileges Editor privilege drop-down**

	administrators	dispatchers	engineers
+ Access Areas	RW	RO	None
+ Alarm Conditions	RW	None	RO
+ Alarm Configuration	RW	None	RW

You have the option of assigning no privileges (None), read-only privileges (RO), or read-write privileges (RW) for that table or view to the user group.

If you assign privileges to a table group, the system assigns those privileges to **all** the tables and views under the group.

## 4.1.4 Changed Privileges

When you change privileges during a session with the Security Group Privileges editor, the system modifies the cell with the changed privilege by changing its background color to pink: **RW**. This visual clue allows you to easily see what changed during the session, and adjust it if not required by clicking **Undo** or **Refresh**.

If a table or view within a group is changed, the group cell changes color also to indicate that one of the tables or views under it has changed.

## 4.1.5 User Groups

The system places user groups as columns across the top of the Editor dialog. If you have not created any user groups when you attempt to open the Editor, the system displays a warning message that no user groups have been configured and does not open the Editor.

### Default User Groups

The default user groups are included with the product, or they can be created at a later stage using either the Security Configuration tool or the SQL Client.

Group	Description
Administrators	Require unrestricted access to all OpenEnterprise functionality.
Engineers	Require configuration access to all system features except those related to controlling security privileges of other users.
Operators	Require the ability to change set points, acknowledge alarms, and perform basic Workstation configuration but no Server configuration.
Dispatchers	Require read-only access to all operational and process data and the ability to acknowledge alarms. Dispatchers are not required to change set points.
Guests	Require only read-only access. They can view data but cannot acknowledge alarms or change set points.

## 4.2 Main Dialog Menu

The Main Menu consists of File, Edit, View, Security and Help options.

---

**Figure 4-3. Security Group Privileges Editor main menu**

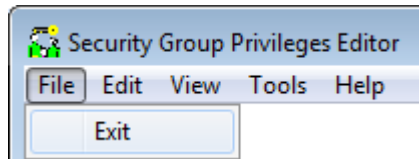




## 4.2.1 File

The File menu only has one option: **Exit**. Selecting this exits the Security Group Privileges Editor. The system discards any unapplied changes you may have made to the grid.

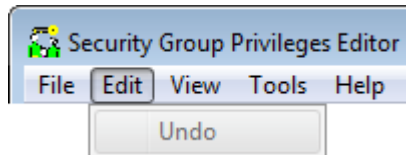
**Figure 4-4. Security Group Privileges Editor – File menu**



## 4.2.2 Edit

The Edit menu has only one option: **Undo**. The system does not activate this option until you make a change on the grid. The option acts in the same way as the **Undo** button: selecting it undoes the **last** change made. Like the Undo button, this option can undo several previous changes in reverse chronological order.

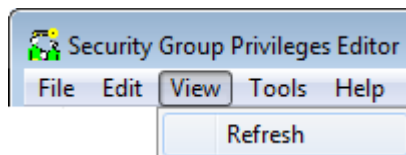
**Figure 4-5. Security Group Privileges Editor – Edit menu**



## 4.2.3 View

The View menu has one option: **Refresh**. Select it to undo all changes that you have made on the grid (provided you have not clicked **Apply** or **OK**). In this way it acts just like the Refresh button.

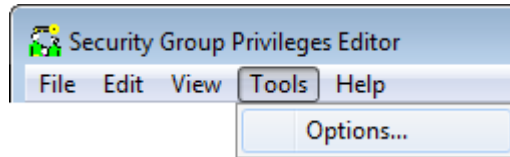
**Figure 4-6. Security Group Privileges Editor – View menu**



## 4.2.4 Tools

The Tools menu has one option: **Options**. Select this option to display the SQL Batches dialog, which enables you to configure SQL statements in variously sized batches. This can be useful to reduce strain on the database when making large changes.

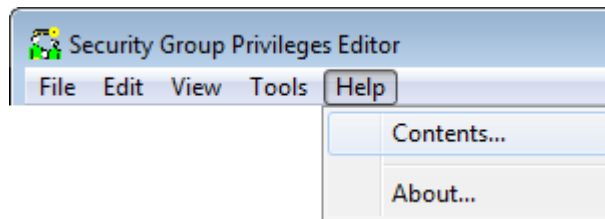
**Figure 4-7. Security Group Privileges Editor – Tools menu**



## 4.2.5 Help Menu

The Help menu has two options: **Contents** and **About**. Select **Contents** to open the OpenEnterprise online help system. Select **About** to open the About dialog, which provides contact information and information about the version and build of OpenEnterprise that you are using.

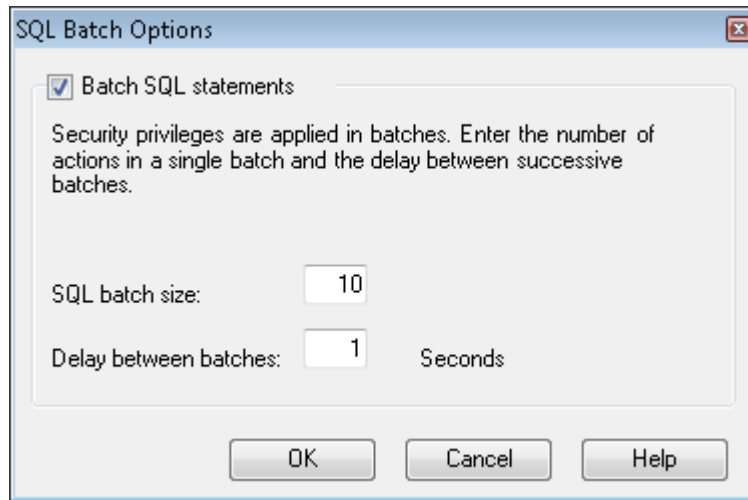
**Figure 4-8. Security Group Privileges Editor – Help menu**



## 4.2.6 SQL Batches Dialog

Select **Options** on the Tools menu to display the SQL Batches dialog. Use the SQL Batches dialog to configure how the Security Group Privileges Editor runs the SQL statements required for making changes in the database. By default, the system sends security privilege updates in batches. Each batch is 10 statements, and the delay between batches is 1 second.

**Figure 4-9. SQL Batch Options dialog**

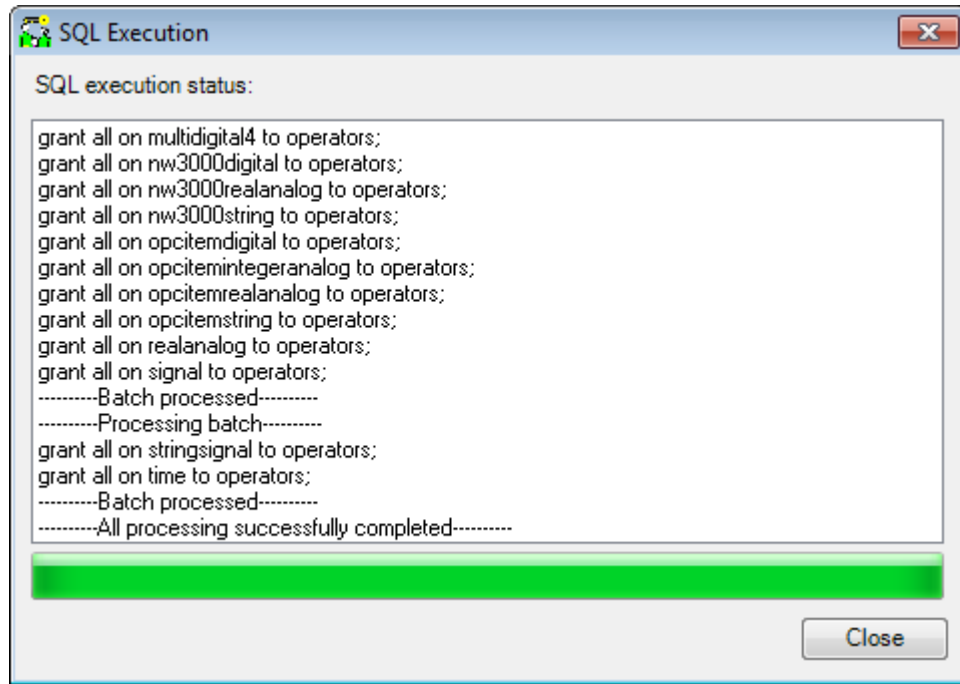


Option	Description
Toggle Batch Operation	Enables or disables the use of batched. Select this option to <b>enable</b> batches (the <b>default</b> ). Changing table security privileges can be a database intensive operation, which is why batch operation is enabled by default.
SQL Batch Size	Defines the number of SQL statements to perform per batch. The <b>default</b> setting is <b>10</b> . The smaller this number, the less strain you place on the database, but the entire operation may take longer.
Delay Between Batches	Sets the delay between batch processing in seconds. The <b>default</b> setting is <b>1</b> second. Set this field to a high value to ease the strain on the database.
OK	Click to close the dialog. The system saves any batch configuration changes.
Cancel	Click to close the dialog. The system discards any configuration changes you have made.
Help	Click to open the OpenEnterprise online help file at a topic related to this page. Click <b>F1</b> to access context sensitive help for this dialog.

## 4.2.7 SQL Execution Dialog

The SQL Execution dialog displays the SQL commands that the Security Group Privileges Editor submits to the database, based on any changes you make on the grid. The SQL Execution dialog informs you of any batches that failed.

Figure 4-10. SQL Execution Dialog



Option	Description
Batch Processing Pane	Informs you of the system’s progress in making the changes to user group privileges based on the changes made on the grid of the Main Dialog. If the system encounters an error, it displays a message explaining the error and asks if you want to continue with the rest of the updates.
Batch Progress Bar	Displays the system’s progress (and turns blue) as it writes the SQL statements to the database progresses. During this process, you can cancel the process by clicking <b>Cancel</b> . When the bar reaches its full length, the configuration changes are complete, and the system changes the <b>Cancel</b> button to a <b>Close</b> button.
Cancel/Close	Enables you to stop the process of writing Group Privileges to the database. As the process proceeds, you can cancel it by clicking <b>Cancel</b> . Once the process completes, the system changes the <b>Cancel</b> button to a <b>Close</b> button. Click <b>Close</b> to close the SQL Execution Dialog.



*[This page is intentionally left blank]*

## Appendix A. Glossary

### A

ACCOL	ACCOL™ is an acronym for <b>A</b> dvanced <b>C</b> ommunications and <b>C</b> ontrol- <b>O</b> riented <b>L</b> anguage, the library of function blocks used in ControlWave Designer to program ControlWave and Bristol33xx devices.
Access Area	Every device, plant area and signal in the OpenEnterprise database belongs to an access area. Access Area security controls what objects within a table can be viewed by the User. Users must be granted the access area of an object in order to view it in the HMI. Access area security is configured using the Security Configuration tool.
Active Query	Type of query the OpenEnterprise database supports that reports changes in data back to the client as those changes occur (without polling) . This mechanism is very fast and efficient.
AMS Device Manager	An Emerson software component which allows interaction with HART devices in the RAS RTU network. The Device Manager uses the RAS host system interface (HIS) to display device hierarchy and HART device data using the static HART device description information (stored in DD files) and to communicate with HART devices.
API	<b>A</b> pplication <b>P</b> rogramming <b>I</b> nterface, the collection of protocols and associated tools used to build software applications.
Archive File Manager	A server-based software tool that enables you to manage the process of moving archive files online and offline.
Archive File Configuration tool	A software tool that enables you to quickly configure archive files.

### B

Background Query	A background query is used to get specific values back from the database. You can configure calculations and workflows to run (“trigger”) when a database value changes. Background queries can also pre-query data (usually non-signal data) to be used in calculations.
Baud Rate	Unit of signaling speed derived from the number of events per second (normally bits per second). However if each event has more than one bit associated with it the baud rate and bits per second are not equal.
BSAP	<b>B</b> ristol <b>S</b> ynchronous/ <b>A</b> synchronous <b>C</b> ommunication <b>P</b> rotocol; the protocol OpenEnterprise uses to communicate with ControlWave RTUs.

### C

Calendar	A yearly time template.
CC	<b>C</b> ommunications <b>C</b> ontroller. A suite of software components that provides port sharing and protocol sharing for OpenEnterprise applications when

## C

	communicating with RTUs.
CL	Control Language; a scripting language contained within the Polyhedra database.
CPU	Central Processing Unit.
CRC	Cyclical Redundancy Check error checking.
CW	ControlWave

## D

DA	Data Access
Data Bits	Sets the number (typically 8) of data bits contained in an asynchronous byte, or character.
Data Cache	A “data cache” is a term for all the values held in memory that have been queried by background queries.
DD	<b>Device Descriptor.</b> A DD for a HART-enabled field device provides AMS with all the parameters and capabilities of that device, as provided by the manufacturer, including the device icon that OpenEnterprise displays on the device tree graphic.
Deadband	A value that defines an inactive zone above the low limits and below the high limits. The deadband prevents a value (such as an alarm) from being set and cleared continuously when the input value oscillates around the specified limit. Defining a deadband also prevents the logs or data storage locations from being over-filled with non-significant data.
Device	A device in the OpenEnterprise database that maps to a physical RTU.
Device Template	A device in the OpenEnterprise database that can be used to create (“clone”) a new device.
Diagnostic Logging	If enabled, this allows logging of communications to and from wired HART® and <i>WirelessHART</i> ® devices.
Diary	A time frame that may act as a “container” for a pattern. The diary has an assigned beginning and ending time. The Scheduler (which must be running in order for scheduled diaries to work) automatically starts the diary at the specified time. You can configure a diary to repeat continuously, to run for a specified number of times, or run just once.
DNP3	DNP3 is a robust protocol used in process control systems such as OpenEnterprise. Providing communication between control equipment and data acquisition devices, DNP3 was originally developed for use in electric and water utility SCADA systems.

## E

EFM	Electronic Flow Metering or Measurement
-----	---



## F

FF	Foundation Fieldbus
Field device	An RTU which has been added to the OpenEnterprise database...
Field Tools™	A software product from Remote Automation Solutions. Technicians at the wellhead use Field Tools to connect with RTUs and HART transmitters in order to set up, tune, and perform field maintenance work for the SCADA network. Field Tools interfaces with the AMS HART Device Configurator (a limited release of AMS Device Manager that accesses device menus and icons, and launches the AMS Device Manager device screens from an external tool). Field Tools also provides an interface to the RAS network of HART devices.
FloBoss 107	A microprocessor-based device that provides flow calculations, remote monitoring, and remote control. A FloBoss is a type of ROC.

## H

HART®	Highway Addressable Remote Transducer.
HART/IP	“HART over IP”: a method to transport HART communications to an IP address that is running a HART server.
HCF	HART Communications Foundation, the standards development and support organization for the HART communication protocol.
HDA	Historical Data Access
Historian module	A software component that creates historical data.
HMI	Human Machine Interface. Basically, the data that is presented to the control room operator from the processing plant.
HSI	Host System Interface. Specific software that allows AMS Device Manager to communicate with the OpenEnterprise system.

## I

IBP	Internet Bristol Protocol over UDP
ICMP	Internet Control Message Protocol
IEC 62591	Standard from the International Electrotechnical Commission (IEC) that specifies an interoperable self-organizing mesh technology in which field devices form wireless networks that dynamically mitigate obstacles in the process environment. The Remote Automation Solutions’ IEC62591 Interface module provides ROC, FloBoss, and ControlWave Micro devices with this functionality.

## L

Lists	Collections of ACCOL signals. Each signal list is assigned a number from 1 to 255. Signals within the signal list are referenced by their position in the list. Each list can contain any mixture of analog, analog alarm, logical, logical alarm, or string
-------	--

## L

	signals.
List view	Part of the HMI that displays list content.
Local Alarm	Local alarms can be raised depending on numerical or digital attribute values in the database. <b>Note:</b> String and Date/Time attributes cannot generate alarms.

## M

MIS	<b>Management Information System.</b> A computer system, usually based on a mainframe or minicomputer, that provides management personnel with up-to-date information (such as sales and inventory) on an organisation's performance. MIS output information in a form that is useable by managers at all organizational levels (strategic, tactical, and operational).
Modbus	A popular device communications protocol developed by Gould Modicon.
MSD	Signal address. A two-byte numerical address for a signal within a ControlWave RTU. Also referred to as PDD.

## N

Network Configuration Utility	The component of the AMS Device Manager software designed to maintain all parameters you can change for an OpenEnterprise network including communication settings.
nw3000	The Network3000 range of RTUs for which the BSAP RDI was first developed.
.NET	Microsoft technology that abstracts coding away from the operating system and provides a library of objects for use within an application. Also takes care of memory de-allocation. .NET is the technology of choice for OpenEnterprise Version 3.x applications

## O

Open Enterprise	<b>OpenEnterprise™</b> , the SCADA application from Emerson Process Management Remote Automation Solution.
OpenEnterprise Language Pack	A file that contains the translations for a particular language for a given build of OpenEnterprise. This can be installed via the Translation Manager.
OESTore	The application file store for Workstation views and other related files. OESTore is a substituted directory created during the installation of an OE Workstation. OpenEnterprise maps the folder <i>C:\ProgramData\Emerson\OpenEnterprise\OESTore</i> to the drive letter O. (This is the default location but can be changed using the SettingsEditor).
OPC	<b>Object linking and embedding for Process Control</b> applications; a set of seven open standards for connectivity and interoperability of industrial automation and the enterprise systems.

**P**

Pattern	Templates that OpenEnterprise uses to change the value of an analog or digital signal over a period of time.
PI	Suite of applications including Enterprise Historian, Asset Framework, Calculation Engine, Notification and Visualization manufactured by OSISoft Inc.
Polling	The act of collecting data from an RTU. This can occur either manually or automatically.
Product Translations	Translations required for customer-specific strings (such as the name of a pump or a well).
Project Translations	Translations required for customer-specific strings (such as the name of a pump or a well).
Protocol	A set of standards that enables communication or file transfers between two computers. Protocol parameters include baud rate, parity, data bits, stop bit, and the type of duplex.
Protocol Bridge Device	A HART device (such as the HART Multiplexer or 1420 Smart wireless gateway) that has other devices connected to it either wired or wirelessly.

**R**

RAS	<b>Remote Automation Solutions</b> , a business unit of Emerson Process Management, focused on serving the oil and gas industry.
RBE	<b>Report By Exception</b>
RCC	Remote Comm Controller, a machine running the Remote Comm Manager which allows the OpenEnterprise client server to manage the machine's devices and communications.
RDB	<b>Remote Database Access</b>
RDI	<b>Remote Device Interface</b> ; a program that communicates with the control program in the device to obtain data.
Redundant device pair	The ControlWave/Bristol 33xx redundant control systems use communications redundancy and dual CPUs and power supplies. This redundant system monitors primary and hot standby CPUs, automatically detects failures, and triggers a switchover from the primary CPU to the hot standby CPU. The process also switches all communication channels and automatically transfers data, alarms, and historical information.
ROC	Remote Operations Controller, a microprocessor-based unit that provides remote monitoring and control.
ROCLINK 800	Microsoft® Windows®-based software used to configure functionality in ROC, DL8000, or FloBoss devices.
rtrdb1	The default database DATSERVICE name for the OpenEnterprise database.
RTU	<b>Remote Terminal Unit</b> . A device which interfaces objects in the physical world to a SCADA system by transmitting telemetry data to the system and/or altering the state of connected objects based on control messages received from the system.

### S

SCADA	Supervisory Control And Data Acquisition; a type of industrial control system (ICS). Industrial control systems are computer-controlled systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICS systems by being large-scale processes that can include multiple sites and large distances.
Sessions	
Signals	The data points placed in or collected from a device.

### T

Template	In OpenEnterprise, a physical device which is used as a pattern to simplify the process of adding new physical devices to a network. You apply the template – and its associated data configurations – to the new device to quickly configure it. Additionally, you can configure the new device to reflect any changes you may make to the template device.
TLP	Type (of point), Logical (or point) number, and Parameter number. You reference data in the ROC800 or FloBoss by type, location or logical, and parameter (TLP). Type refers to the number of the point type. The location or logical number is a value based on physical input or output. A parameter is a numeric value assigned to each piece of data contained in a given point.
Tokens	Tokens determine workstation security. Specific Human Machine Interface (HMI) functionality is allowed or denied through tokens. Tokens are required for file access, OPC write access, built in application context menus and custom menus. Token security is configured using the Security Configuration tool.

### U

Unicode	Computing industry standard for the consistent encoding, representation, and handling of text expressed in most of the world's writing systems. Storage of each character is stored in more than one byte and therefore characters from languages other than English are available. However, the wider characters mean that Unicode text needs to be treated differently in code from ASCII.
Update mask	A configuration tool that identifies specific portions of a device's configuration to address when updates occur. A mask can prevent or facilitate updates.
UTC	Coordinated Universal Time (UTC), a worldwide civil time standard.

### W

WHA	WirelessHART® Adapter
Wizard	A series of software screens that guides you through a specific task.

## Appendix B Application Tokens

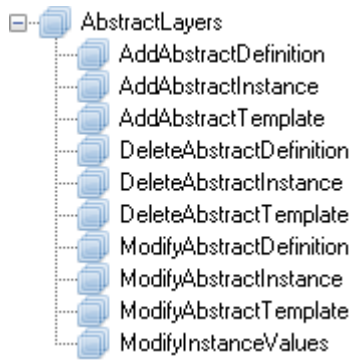
As noted in Chapter 2, tokens provide a way you can include or exclude access for applications and system functionality for a User ID. This appendix is a reference list of all OpenEnterprise tokens and includes:

- Abstract Layers Tokens (Asset Modeling)
- AdHoc List Tokens (Custom Groups)
- Alarm View Tokens
- Alarm Banner Tokens
- Calculations Tokens
- Container Tokens
- Data Collection Tokens
- DataView Tokens (currently reserved)
- Device Configuration (HART) Tokens
- Device Template Tokens
- Driver Configuration Tokens (currently reserved)
- Equipment Tokens (currently reserved)
- Graphics View Tokens
- History Editor Tokens
- Network Configuration Tokens
- Notes View Tokens
- OE Alarm Client Tokens
- OEDesktop Tokens
- Report Selector Tokens
- Secure Desktop Tokens
- Session Manager Tokens
- Sites Tokens
- SQL View Tokens
- Trend View Tokens
- Workflows Tokens

## 1. Abstract Layers Tokens

Abstract Layers tokens provide access to functional options within the Asset Modeling pane.

**Figure B-1. Abstract Layers Tokens**

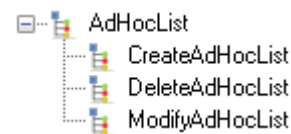


Token	Description
AddAbstractDefinition	Adds a new abstract Definition
AddAbstractInstance	Adds a new abstract Instance
AddAbstractTemplate	Adds a new abstract Template
DeleteAbstractDefinition	Deletes an abstract Definition
DeleteAbstractInstance	Deletes an abstract Instance
DeleteAbstractTemplate	Deletes an abstract Template
ModifyAbstractDefinition	Modifies an abstract Definition
ModifyAbstractInstance	Modifies an abstract Instance
ModifyAbstractTemplate	Modifies an abstract Template
Modify InstanceValues	Modifies instance values.

## 2. AdHoc List Tokens

AdHocList tokens provide access to functional options within the Groups pane's Custom Groups section.

**Figure B-2. AdHocList Tokens**

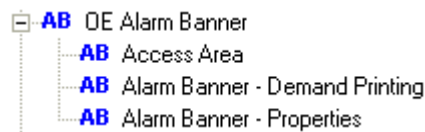


Token	Description
CreateAdHocList	Creates a new AdHoc List
DeleteAdHocList	Deletes an AdHocList
ModifyAdHocList	Modifies an AdHocList

### 3. Alarm Banner Tokens

These application tokens are available for the Alarm Banner.

**Figure B-3. Alarm Banner Tokens**



Token	Description
Access Area	Accesses the menu item that provides a filter on the Alarm Banner based on access area.
Alarm Banner - Demand Printing	Prints the contents or a selection of the contents of any OEDesktop window containing an Alarm Banner file.
Alarm Banner - Properties	Accesses the Properties menu to display the Alarm Banner's Property Pages in Configure mode.

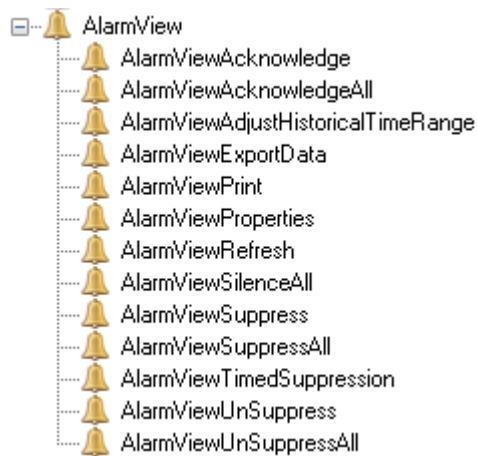
### 4. Alarm View Tokens

Exclusion of any token means the item does not appear on the Alarm View's context menu when the User or members of the User Group log into OpenEnterprise.

**Note**

The Alarm View panel is available as standard in the lower right of the Container and from the Alarms menu.

**Figure B-4. Alarm View Tokens**



Token	Description
AlarmViewAcknowledge	Acknowledges selected alarms by accessing the Acknowledge menu item on the Alarm View's context menu
AlarmViewAcknowledgeAll	Acknowledges all alarms with a single click of the mouse
AlarmViewAdjustHistoricalTimeRange	Adjusts the time range, when the Alarm View is configured for historical usage, such as an event log. This token permits the shortening of the time for which the Alarm View returns event data.
AlarmViewExportData	Exports information from the Alarm View to the Windows clipboard for pasting into other applications. By holding the Shift key at the same time, the data can be directly pasted into a MS Excel spreadsheet.
AlarmViewPrint	Prints all or a selection of alarms from the Alarm View pane.
AlarmViewProperties	Accesses the Property pages of the Alarm View in Runtime mode and permits configuration changes.
AlarmViewRefresh	Refreshes the data being displayed by the Alarm View. If the Alarm View is configured for Historical (such as events) display, then a new query is initiated
AlarmViewSilenceAll	Silences all current alarms that are set to sound. As new alarms come in, they begin to sound.
AlarmViewSuppress	Suppresses selected alarms. This means that the alarm is still in the Alarm Summary, but it does not appear within the Alarm View because a filter is applied based on whether the alarm has its Suppressed attribute set to true.

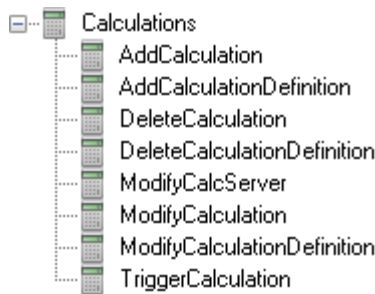


Token	Description
AlarmViewSuppressAll	Suppresses all alarms.
AlarmViewTimedSuppression	Suppresses an alarm for a specified period of time. Timed suppression may be subject to a maximum period, which may be defined on the Suppression Page of the Alarm View's configuration pages.
AlarmViewUnsuppress	Immediately un-suppresses a previously suppressed alarm.
AlarmViewUnsuppressAll	Immediately un-suppresses all previously suppressed alarms.

## 5. Calculations Tokens

Calculations tokens provide access to functional options within the Calculations pane.

**Figure B-5. Calculations Tokens**

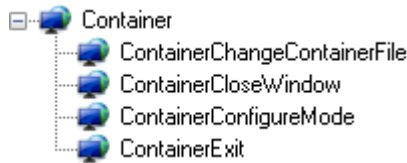


Token	Description
AddCalculation	Adds a new Calculation
AddCalculationDefinition	Adds a new Calculation Formula or Background Query
DeleteCalculation	Deletes a Calculation
DeleteCalculationDefinition	Deletes a Calculation Formula or Background Query
ModifyCalcServer	Modifies a Calculation Server
ModifyCalculation	Modifies a Calculation
ModifyCalculationDefinition	Modifies a Calculation Formula or Background Query
TriggerCalculation	Triggers a Calculation

## 6. Container Tokens

These application tokens belong to the OpenEnterprise Container.

**Figure B-6. Container Tokens**

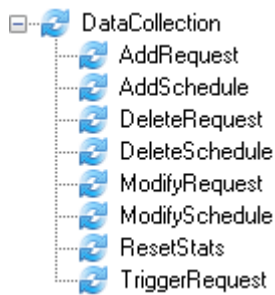


Token	Description
ContainerChangeContainerFile	Changes the OpenEnterprise Container file.
ContainerCloseWindow	Closes any child window within the Container
ContainerConfigureMode	Enters the Container's Configure mode.
ContainerExit	Exits the Container application.

## 7. Data Collection Tokens

These application tokens belong to the OpenEnterprise Container Network Communications pane Collections tree and the Device Templates pane Schedules tree.

**Figure B-7. Data Collection Tokens**

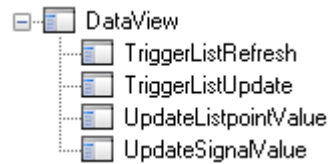


Token	Description
AddRequest	Adds a Request.
AddSchedule	Adds a Schedule.
DeleteRequest	Deletes a Request.
DeleteSchedule	Deletes a Schedule
ModifyRequest	Modifies a Request.
ModifySchedule	Modifies a Schedule.
ResetStatistics	Resets the statistics from the Network Communication's pane Statistics views.
TriggerRequest	Triggers a Request or a Read.

## 8. DataView Tokens

These tokens are reserved for future use.

**Figure B-8. DataView Tokens**



Token	Description
TriggerListRefresh	Reserved for future use
TriggerListUpdate	Reserved for future use
TriggerListpointValue	Reserved for future use
UpdateSignalValue	Reserved for future use

## 9. Device Configuration Tokens - HART

These application tokens belong to the HART Pass-Through application.

**Figure B-9. HART Pass-Through Tokens**

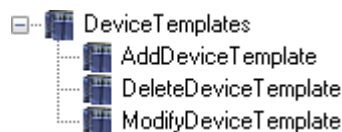


Token	Description
AddDD	Adds a HART Device Descriptor file.
LaunchDeviceScreen	Launches the HART Device Configurator.
ScanHART	Scans a HART device.

## 10. Device Templates Tokens

These application tokens belong to the OpenEnterprise Container Device Templates pane.

**Figure B-10. Device Templates Tokens**

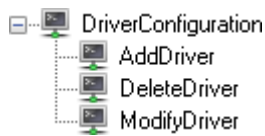


Token	Description
AddDeviceTemplate	Adds a device template.
DeleteDeviceTemplate	Deletes a device template.
ModifyDeviceTemplate	Modifies a device template.

## 11. Driver Configuration Tokens

These tokens are reserved for future use.

**Figure B-11. Driver Configuration Tokens**

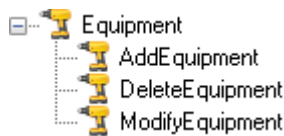


Token	Description
AddDriver	Reserved for future use
DeleteDriver	Reserved for future use
ModifyDriver	Reserved for future use

## 12. Equipment Tokens

These tokens are reserved for future use.

**Figure B-12. Equipment Tokens**



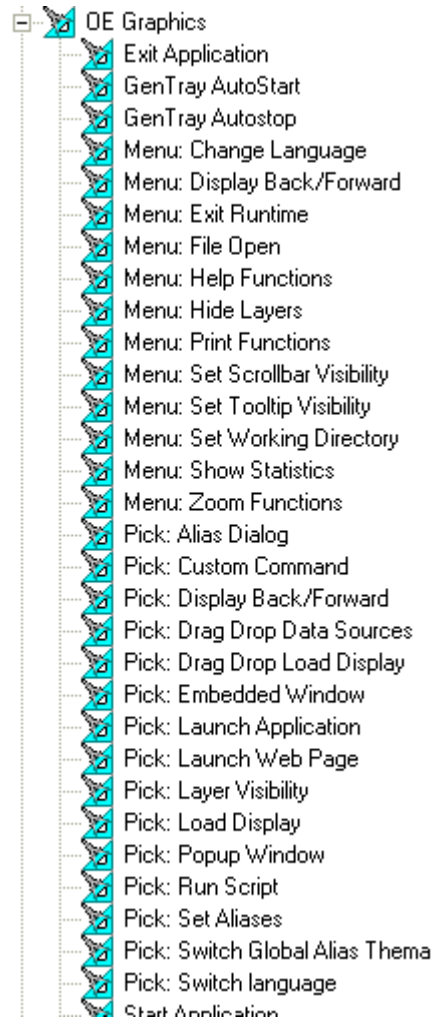
Token	Description
AddEquipment	Reserved for future use
DeleteEquipment	Reserved for future use
ModifyEquipment	Reserved for future use

## 13. Graphics View Tokens

Some of the Graphics View Menu Tokens (prefaced **Menu:**) only affect the Graphics application when it is runs outside of the OEDesktop environment, and so are not relevant to OpenEnterprise. Other Menu tokens affect the menu items that appear under the View menu of

the OEDesktop when a Graphics display window is selected within the OEDesktop. The Pick tokens (prefaced **Pick:**) affect the User's access to OpenEnterprise Graphics Pick type objects during Runtime mode.

**Figure B-13. OE Graphics Tokens**



Token	Description
Exit Application	Exits the Graphics application, but the User must have the OEDesktop Create or Close Window Token to be able to close a window displaying a Graphics file within OEDesktop.
GenTray AutoStart	Auto-starts the Graphics View application with the GenTray utility. This token is only relevant when starting the OpenEnterprise Graphics View application <b>outside</b> of the OEDesktop environment.
GenTray AutoStop	Auto-stops the Graphics application with the GenTray utility when it is running <b>outside</b> of the OEDesktop environment.

Token	Description
Menu: Change Language	Changes the language of the Graphics application. <b>Note:</b> Do not assign this token to routine (non-system administrator) users of the OpenEnterprise application.
Menu: Display Back/Forward	Enables backwards or forwards movement through a series of configured displays. <b>Note:</b> Since display navigation is best achieved through use of the OEMenus, it is not recommended to use this method.
Menu: Exit Runtime	Switches the display into Configure mode when running the Graphics application <b>outside</b> of the OEDesktop environment. When running <b>within</b> the OEDesktop environment, the OEDesktop's Configure Mode Token enables Users to switch all Views into Configure mode.
Menu: File Open	Accesses the Graphics View File/Open menu item. It is not relevant if the OEDesktop File/Open menu item is available.
Menu: Help Functions	Accesses the context-sensitive Graphics View help.
Menu: Hide Layers	Accesses the Graphics View Hide Layers menu item.
Menu: Print Functions	Accesses the Graphics View Print menu functions when the Graphics application runs <b>outside</b> of the OpenEnterprise Desktop. When running <b>within</b> the OpenEnterprise Desktop the OEDesktop File Menu has an option to print any selected View window. The OEDesktop File menu is displayed by default, but can be hidden from the Menu tab of the OE Desktop's Property pages (accessed from the <b>Desktop&gt;Customize</b> menu item)
Menu: Set Scrollbar Visibility	Accesses the Graphics View <b>Set Scrollbar Visibility</b> menu item.
Menu: Set Tooltip Visibility	Enables the User to access the Graphics View <b>Set Tooltip Visibility</b> menu item.
Menu: Set Working Directory	Accesses the Graphics View <b>Set Working Directory</b> menu item.
Menu: Show Statistics	Accesses the Graphics View <b>Show Statistics</b> menu item, which gives display statistics.
Menu: Zoom Functions	Accesses the Graphics View Zoom menu items.
Pick: Alias Dialog	Accesses a Pick action object which displays the Alias Dialog (for editing aliases).
Pick: Custom Command	Accesses any Graphics View Pick action object

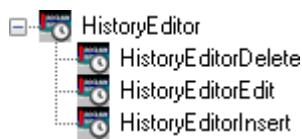
Token	Description
	that uses a Custom Command. From an OE perspective, this is the most important of the Pick commands. The Custom Command provides access to OEMenus and the OEMenus editor interface.
Pick: Display Back/Forward	Accesses any Graphics Pick action object that uses the Display Back/Forward commands.
Pick: Drag Drop Data Sources	Accesses any Graphics View Pick action object that uses the Drag Drop Data Sources functionality.
Pick: Drag Drop Load Display	Accesses any Graphics View Pick action object that uses the Drag Drop Load Display functionality.
Pick: Embedded Window	Accesses any Graphics View Pick action object that uses the Embedded Window functionality.
Pick: Launch Application	Accesses any Graphics View Pick action object that uses the Launch Application functionality.
Pick: Layer Visibility	Accesses any Graphics View Pick action object that uses the Layer Visibility functionality.
Pick: Load Display	Accesses any Graphics View Pick action object that uses the Load Display functionality
Pick: Popup Window	Accesses any Graphics View Pick action object that uses the Popup Window functionality.
Pick: Run Script	Accesses any Graphics View Pick action object that uses the Run Script functionality
Pick: Set Aliases	Accesses any Graphics View Pick action object that uses the Set Aliases functionality.
Pick: Switch Language	Accesses any Graphics View Pick action object that uses the Switch Language functionality
Start Application	Accesses the Graphics View Start Application functionality.
Tab Load Display	Accesses the Graphics View Tab Load Display functionality.
Graphics View File Token: Layers	The rest of the security tokens listed on this page belong to the Application Token category, but there is also a special File type security Token that applies <b>only</b> to the Graphics View component of OE, so it is mentioned here. To enable security on layers within Graphics displays, add a File Token with the format: <code>&lt;Filename&gt; &lt;Layername&gt;</code> Then include this File Token in the Security configuration for any users who should have access to that layer. For example, if you have a display called <i>PumpRoom.gdf</i> and a layer that is named

Token	Description
	<i>SecretLayer</i> , you would create a new File Token (see the online help topic <i>Creating Custom, File and OPC Item Tokens</i> ) with the name: - <i>PumpRoom.gdf SecretLayer</i>

## 14. History Editor Tokens

These application tokens belong to the ROC History Editor.

**Figure B-14. History Editor Tokens**

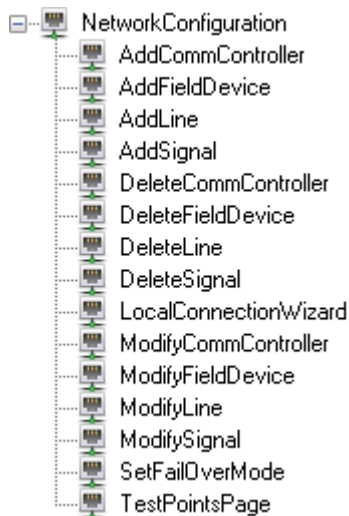


Token	Description
HistoryEditorDelete	Deletes ROC history data
HistoryEditorEdit	Edits ROC history data
HistoryEditorInsert	Inserts ROC history data

## 15. Network Configuration Tokens

These tokens provide access to Network Configuration functional options.

**Figure B-15. Network Configuration Tokens**



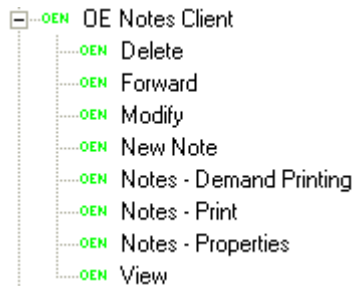


Token	Description
AddCommController	Adds a Comm Controller
AddFieldDevice	Adds a new field device
AddLine	Adds a communications line
AddSignal	Adds a signal to the database
DeleteCommController	Deletes a Comm Controller
DeleteFieldDevice	Deletes a field device
DeleteSignal	Deletes a signal from the database
LocalConnectionWizard	Activates the Local Connection wizard
ModifyCommController	Modifies a Comm Controller
ModifyFieldDevice	Modifies a field device
ModifyLine	Modifies a communications line.
ModifySignal	Modifies a signal
SetFailOverMode	Sets the failover mode
TestPointsPage	Accesses the test points.

## 16. Notes View Tokens

These application tokens are available for the Notes View component.

**Figure B-16. OE Notes View Tokens**



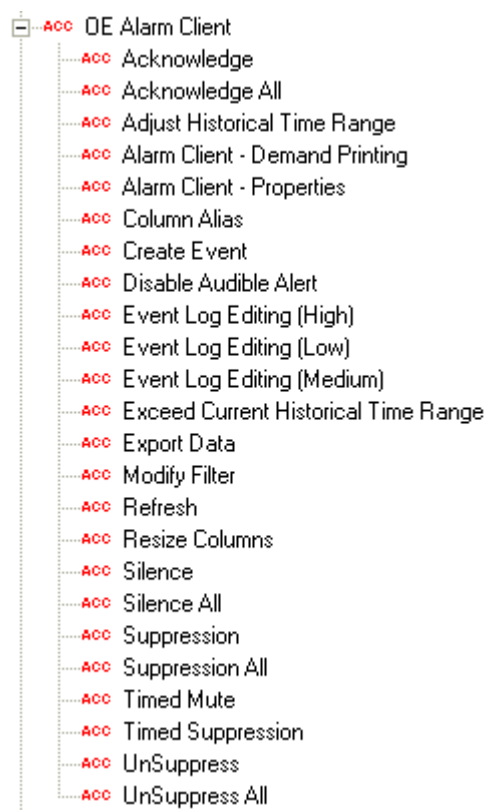
Token	Description
Delete	Deletes a selected Note.
Forward	Forwards Notes.
Modify	Modifies Notes.
New Note	Creates Notes.
Notes - Demand Printing	Prints the contents of the Notes window.
Notes - Print	Prints a selected Note.
Notes - Properties	Accesses the Property Pages of the Note View when in Configuration mode.

Token	Description
View	Views individual Notes that are displayed within the Notes View window

## 17. OE Alarm Client Tokens

Exclusion of any token means the item does not appear on the OE Alarm Client's context menu when the User or members of the User Group are logged into OpenEnterprise.

Figure B-17. OE Alarm Client Tokens



Token	Description
Acknowledge	Acknowledges selected alarms by accessing the Acknowledge menu item on the Alarm Client's context menu.
Acknowledge All	Acknowledges all alarms with a single click of the mouse.
Adjust Historical Time Range	Adjusts the time range (when the Alarm Client is configured for historical usage, as with an event log) by shortening the time for which the Alarm Client returns event data.
Alarm Client Demand Printing	Prints all or a selection of alarms from the Alarm

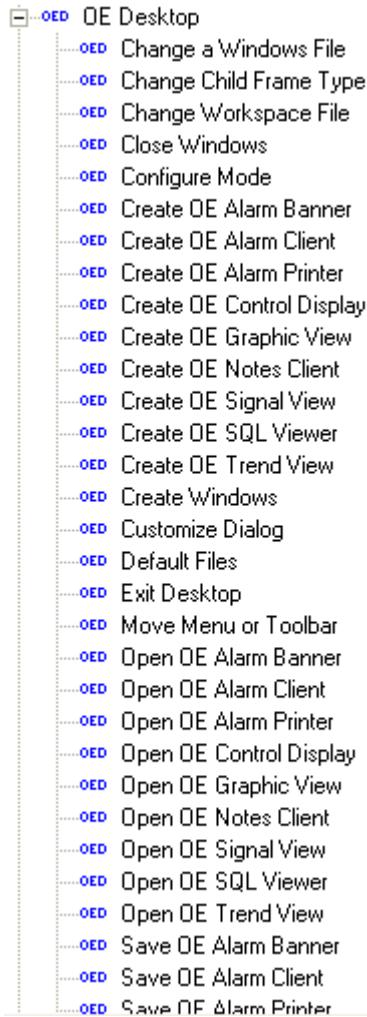
Token	Description
	Client window.
Alarm Client Properties	Accesses the Property pages of the Alarm Client in Runtime mode and make configuration changes.
Column Alias	Specifies aliases for the column headings within the Alarm Client. Right-clicking on a column heading displays a text box, in which you enter the name of the alias. The alias then replaces the real column name.
Create Event	Creates a new event within the Event Log. You select a current event and change the wording of certain attributes. OpenEnterprise then creates a copy of the current event with the new wording and inserts it as a new event into the Event History table.
Disable Audio Alert	Disables the audible alert on the Sound page of the Alarm Client Property pages. <b>Note:</b> If assigned this token, you must <b>also</b> be given the Alarm Client Properties token.
Event Log Editing (High)	Lists the Event Log fields that you can change when creating an event. The exact fields that can be updated are set in the OpenEnterprise Settings file. To view the fields that are available, open the Settings Editor and go to the Tasks\Event Viewer>Edit Permissions key.
Event Log Editing (Medium)	Permits the changing of certain attributes (description, alarmtext, devicename, base, extension, helptext, and operatortext) when creating an event.
Event Log Editing (Low)	Edits the description attribute of the selected 'copy' event when creating a new event.
Exceed Current Historical Time Range	Exceeds the currently set Historical Time Range on an Alarm Client configured for Historical (that is, event) viewing.
Export Data	Exports information from the Alarm Client to the Windows clipboard for pasting into other applications. By holding the Shift key at the same time, the data can be directly pasted into an Excel spreadsheet.
Modify Filter	Modifies filters applied to the Alarm Client. Without it the <b>Modify</b> button on the Filter Page of the Alarm Client Property Pages is disabled. <b>Note:</b> If assigned this token, you must have been previously assigned the Alarm Client - Properties token to use this one.

Token	Description
Refresh	Refreshes the data the Alarm Client displays. <b>Note:</b> If the Alarm Client is configured for Historical (that is, events) display, this token initiates a new query.
Resize Columns	Resizes the columns of the Alarm Client.
Silence	Silences a selected alarm if it is set to create a sound.
Silence All	Silences all current alarms that are set to sound. As new alarms come in, they begin to sound.
Suppression	Suppresses selected alarms. While the alarm is still in the Alarm Summary, it does not appear within the Alarm Client because a filter is applied based on whether the alarm has its Suppressed attribute set to true.
Suppression All	Suppresses all alarms.
Timed Mute	Applies a timed suppression of alarm annunciation.
Timed Suppression	Suppresses an alarm for a specified period of time. Timed suppression may be subject to a maximum period, which may be defined on the Suppression Page of the Alarm Client's configuration pages.
Unsuppress	Immediately un-suppresses a previously suppressed alarm.
Unsuppress All	Immediately un-suppresses all previously suppressed alarms.

## 18. OEDesktop Tokens

These application tokens belong to the OEDesktop.

**Figure B-18. OEDesktop Tokens**



Token	Description
Change a Windows File	Changes the file within an open window in the OEDesktop. For example, if a window displaying a trend file was open in the OEDesktop, you could only open a different trend file into the same window if you have the Change a Windows File Token
Change Child Frame Type	Changes the window type of window within the OEDesktop; right-click on its Title Bar and access the window type context menu.
Change Workspace File	Changes the OEDesktop file.

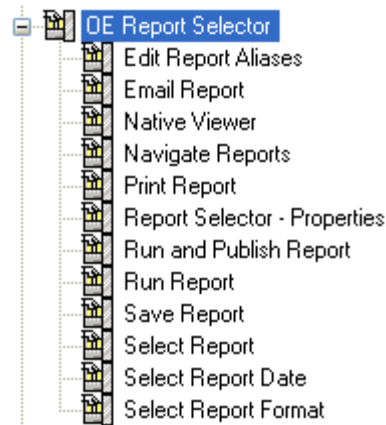
Token	Description
Configure Mode	Accesses Configure mode for the OEDesktop or any View Component within the OEDesktop.
Create Alarm Banner	Creates a new Banner Alarm using the OEDesktop's New menu item.
Create Alarm Client	Creates a new Alarm View using the OEDesktop's New menu item.
Create Alarm Printer	Creates a new Alarm Printer View using the OEDesktop's New menu item.
Create OEControl Display	Creates a new OEControl Display using the OEDesktop's New menu item.
Create Graphic View	Creates a new Graphic View using the OEDesktop's New menu item.
Create Notes View	Creates a new Notes View using the OEDesktop's New menu item.
Create Signal View	Creates a new Signal View using the OEDesktop's New menu item.
Create SQL Viewer	Creates a new SQL View using the OEDesktop's New menu item.
Create Trend View	Creates a new Trend View using the OEDesktop's New menu item.
Create or Close Window	Creates a new window within the OEDesktop or closes any child window within the OEDesktop.
Customize Dialog	Accesses the OEDesktop's File Customize menu option to configure the OEDesktop.
Exit Desktop	Exits the OEDesktop application
Move Menu or Toolbar	Changes the position of the OEDesktop Menu bar and/or Toolbar.
Open Alarm Banner	Opens a previously saved Alarm Banner file into the OEDesktop.
Open Alarm Client	Opens a previously saved Alarm View file into the OEDesktop.
Open Alarm Printer	Opens a previously saved Alarm Printer file into the OEDesktop.
Open Control Display	Opens a previously saved OEControl Display file into the OEDesktop.
Open Graphic View	Opens a previously saved OEGraphic View file into the OEDesktop.
Open Notes Client	Opens a previously saved Notes View file into the OEDesktop.
Open Signal View	Opens a previously saved Signal View file into the OEDesktop.
Open SQL Viewer	Opens a previously saved SQL View file into the OEDesktop.

Token	Description
Open Trend View	Opens a previously saved Trend View file into the OEDesktop.
Save Alarm Banner	Saves a configured Alarm Banner file from within the OEDesktop.
Save Alarm Client	Saves a configured Alarm Client file from within the OEDesktop.
Save Alarm Printer	Saves a configured Alarm Printer file from within the OEDesktop.
Save OEControl Display	Saves a configured OEControl Display file from within the OEDesktop.
Save Graphic View	Saves a configured Graphic View file from within the OEDesktop.
Save Notes Client	Saves a configured Notes View file from within the OEDesktop.
Save Signal View	Saves a configured Signal View file from within the OEDesktop.
Save SQL Viewer	Saves a configured SQL View file from within the OEDesktop.
Save Trend View	Saves a configured Trend View file from within the OEDesktop.
Toggle Status Bar	Hides or shows the Status bar for the OEDesktop and its child windows.
Toggle Toolbar	Hides or shows the OEDesktop Toolbar.

## 19. Report Selector Tokens

Report Selector tokens provide access to functional options within the Report Selector View.

**Figure B-19. Report Selector Tokens**

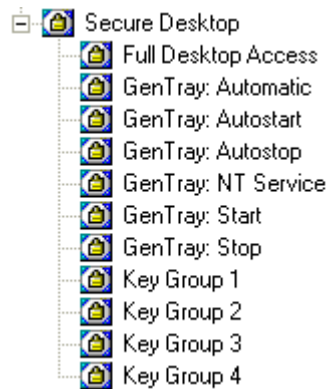


Token	Description
Edit Report Aliases	Edits the alias values for the report.
Email Report	Emails the report.
Native Viewer	Opens the report in its native viewer.
Navigate Reports	Enables the User to navigate reports using the next/previous buttons.
Print Report	Prints a report.
Report Selector – Properties	Configures the report selector.
Run and Publish Report	Runs and publishes a report.
Run Report	Runs a report.
Save Report	Saves a report to a different location.
Select Report	Selects a report from a drop-down list.
Select Report Date	Selects a date for the report.
Select Report Format	Selects a report format from a drop-down list.

## 20. Secure Desktop Tokens

Secure Desktop tokens provide or deny access to the Windows Desktop for a user.

**Figure B-20. Secure Desktop Tokens**



Token	Description
-------	-------------



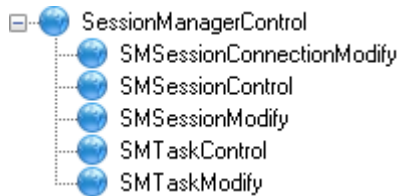
Token	Description
Full Desktop Access	<p>Accesses all the normal Windows Desktop features, including the System keys (such as Ctrl-Alt-Delete, the Windows key to activate the Start button, the System Tray, etc.) if the token is in the user's Include list.</p> <p>A user not having this token or having it in their Exclude list cannot access normal Windows Desktop functionality. They can use the Ctrl-Alt-Delete key combination to bring up the <i>Windows Security</i> dialog, but all buttons on it except for <b>Cancel</b> are disabled.</p>
Gentray: Automatic	<p>Controls whether users can select the option to make Secure Desktop an Automatic Windows service from the Gentray icon on the Windows System bar when logged into OpenEnterprise.</p> <p><b>Note:</b> This option is available <b>only</b> if the Secure Desktop has already been designated as a Windows service.</p>
Gentray: Autostart	<p>Controls whether users can select the option to make Secure Desktop start automatically when logging into OpenEnterprise. This option is available from the Gentray icon on the Windows System bar when logged into OpenEnterprise.</p>
Gentray: Autostop	<p>Controls whether users can select the option to make Secure Desktop automatically stop when a user logs out of OpenEnterprise. This option is available from the Gentray icon on the Windows System bar when logged into OpenEnterprise.</p>
Gentray: NT Service	<p>Controls whether users can select the option to make Secure Desktop a Windows service from the Gentray icon on the Windows System bar when logged into OpenEnterprise.</p>
Gentray: Start	<p>Controls whether users can start Secure Desktop from the Gentray icon on the Windows System bar when logged into OpenEnterprise.</p>
Gentray: Stop	<p>Controls whether users can stop Secure Desktop from the Gentray icon on the Windows System bar when logged into OpenEnterprise.</p>
Keygroup 1	<p>Permits use of the keyboard keys specified in this Keygroup when logged into OpenEnterprise.</p> <p><b>Note:</b> Any user not having this token cannot access these keys.</p>
Keygroup 2	<p>Permits use of the keyboard keys specified in this Keygroup when logged into OpenEnterprise.</p> <p><b>Note:</b> Any user not having this token cannot access these keys.</p>

Token	Description
Keygroup 3	Permits use of the keyboard keys specified in this Keygroup when logged into OpenEnterprise. <b>Note:</b> Any user not having this token cannot access these keys.
Keygroup 4	Permits use of the keyboard keys specified in this Keygroup when logged into OpenEnterprise. <b>Note:</b> Any user not having this token cannot access these keys.

## 21. Session Manager Tokens

Session Manager tokens provide access to functional options within the Sessions pane.

**Figure B-21. Session Manager Tokens**

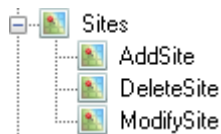


Token	Description
SMSessionConnectionModify	Modifies a Session connection.
SMSessionControl	Accesses the Session context menus.
SMSessionModify	Modifies a Session.
SMTaskControl	Accesses the Task context menus.
SMTaskModify	Modifies tasks.

## 22. Sites Tokens

Sites tokens provide access to functional options within the Groups pane’s Sites tree.

**Figure B-22. Sites Tokens**



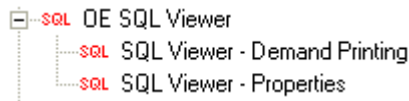
Token	Description
AddSite	Adds a Site

Token	Description
DeleteSite	Deletes a Site
ModifySite	Modifies a Site

## 23. SQL View Tokens

These application tokens are available for the SQL View component.

**Figure B-23. SQL View Tokens**

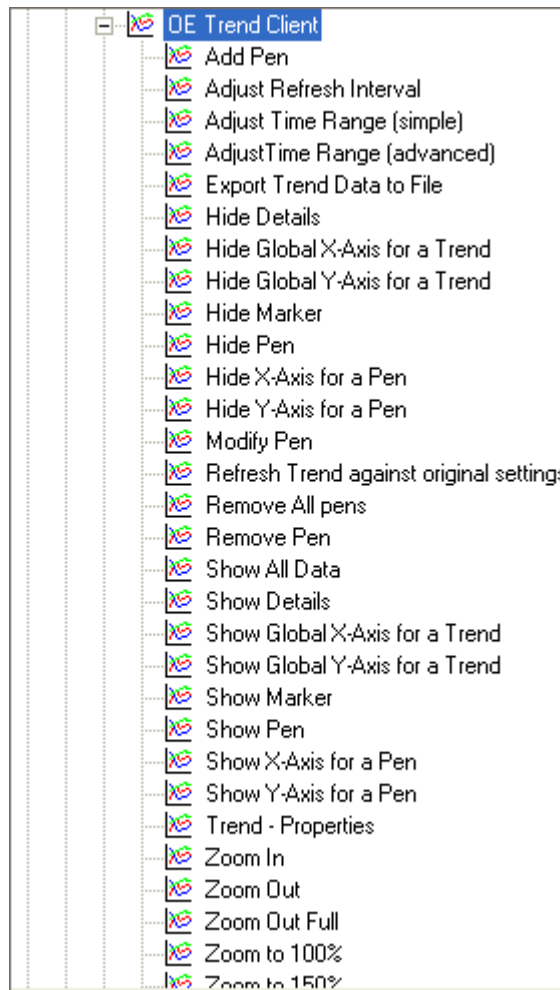


Token	Description
SQL Viewer - Demand Printing	Prints the contents or a selection of the contents of any OEDesktop window containing an SQL Viewer file
SQL Viewer - Properties	Accesses the Properties menu to display the SQL Viewer Property Pages in Configure mode

## 24. Trend View Tokens

The system uses all the following tokens in runtime mode unless otherwise stated.

Figure B-24. Trend View Tokens



Token	Description
Add Pen	Adds a new Pen to a Trend View.
Adjust Refresh Interval	Changes the refresh rate of the Trend View.
Adjust Time Range (Simple)	Adjusts the Start Time and the Range of the Trend View window (allowing the trend to retrieve more or less data) via a runtime context menu item.
Adjust Time Range (Advanced)	Accesses the Advanced button on the Trend View's Data Page, used to change the Data Collection Interval, Number of Samples per Pen, and Maximum Pages of Data for the trend. <b>Note:</b> This feature is used <b>only</b> in Configure

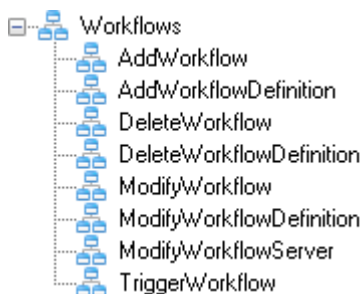
Token	Description
	mode.
Export Trend Data to File	Exports the current Trend View data to an Excel spreadsheet file, a CSV file, or to export the window as a BMP or JPG graphics file.
Hide Details	Hides the Pen Details window via a content menu item. By default, the Pen Details window appears at the bottom of the Trend View window.
Hide Global X-Axis for a Trend	Hides the Trend's Global X-axis via a context menu.
Hide Global Y-Axis	Hides the Trend's Global Y-axis via a context menu .
Hide Marker	Hides the Trend's Marker bar.
Hide Pen	Hides any Pen selected from the Trend Details pane.
Hide X-Axis for Pen	Hides a Pen's individual X-axis.
Hide Y-Axis for Pen	Hides a Pen's individual Y-axis.
Modify Pen	Permits limited Pen modification while in Runtime mode.
Refresh Trend Against Original Settings	Refreshes a Trend using the original settings of the trend.
Remove All Pens	Removes all Pens from the trend.
Remove Pen	Removes a Pen selected in the Details pane.
Show All Data	Controls the Show All Data context menu item, available from the Trend Graph pane. The Show All Data menu item displays all data for a Trend that has Trend optimization configured. Unless the user has this token, the option does not appear on the context menu. For more information on Trend optimization refer to the Trend documentation.
Show Details	Shows the Details window after it has been hidden.
Show Global X-Axis for a Trend	Shows a hidden Global X-axis.
Show Global Y-Axis for a Trend	Shows a hidden Global Y-axis.
Show Marker	Shows a hidden Trend Marker line.
Show Pen	Shows a hidden Pen.
Show X-Axis for a Pen	Shows the individual X-axis for a Pen selected using the Details pane
Show Y-Axis for a Pen	Shows the individual Y-axis for a Pen selected using the Details pane.
Trend - Properties	Accesses the Trend's Properties context menu in

Token	Description
	Configuration mode, permitting configuration of the Trend View.
Trend View - Demand Printing	Prints the contents of a Trend View window while it runs in the OEDesktop.
Zoom In	Zooms in by a margin of 50%.
Zoom Out	Zooms out by a margin of 50%.
Zoom Out Full	Zooms out to the original setting from any magnification.
Zoom to 100%	Zooms the Trend to its original setting.
Zoom to 150%	Sets the Trend's magnification to the indicated setting.
Zoom to 25%	Sets the Trend's magnification to the indicated setting.
Zoom to 250%	Sets the Trend's magnification to the indicated setting.
Zoom to 50%	Sets the Trend's magnification to the indicated setting.
Zoom to 75%	Sets the Trend's magnification to the indicated setting.
Zoom to Custom	Sets the Trend's magnification to a custom setting.
Zoom Undo	Restores the Trend's magnification to its previous setting.

## 25. Workflows Tokens

Workflows tokens provide access to functional options within the Action Engine pane.

**Figure B-25. Workflows Tokens**



Token	Description
AddWorkflow	Enables the User to add a new Workflow
AddWorkflowDefinition	Enables the User to add a new Workflow definition.

Token	Description
DeleteWorkflow	Enables the User to delete a Workflow.
DeleteWorkflowDefinition	Enables the User to delete a Workflow definition.
ModifyWorkflow	Enables the User to modify a Workflow.
ModifyWorkflowDefinition	Enables the User to modify a Calculation definition.
ModifyWorkflowServer	Enables the User to modify a Calculation Server.
TriggerWorkflow	Enables the User to trigger a Workflow.





# Index

Abstract Layers Tokens .....	112	Configure Mapping .....	49
Access Area node .....	43	Exclude .....	61, 62, 65, 67, 69
Access Area nodes .....	44	F1 .....	97, 101
Access Areas		Help .....	20, 50, 57, 58, 60, 61, 64, 66, 68, 70, 72, 73, 74, 75, 97, 101
Modifying .....	88	Include .....	60, 62, 64, 67, 69
Access Areas .....	59	OK20, 50, 57, 58, 59, 61, 63, 66, 68, 70, 75, 96, 101	
Active Database .....	19	OK73	
Active Directory .....	3	OK (Token Group Properties) .....	72
Adding		Refresh.....	96
Default Group .....	80	Remove .....	59, 60, 62, 65, 67, 69, 72
New User to User Group.....	84	Remove All Links .....	74
AdHoc List Tokens.....	112	Undo.....	97
Alarm Banner Tokens .....	113	Calculations Tokens .....	115
Alarm Client Tokens.....	124	Changed Privileges.....	98
Alarm View Tokens .....	113	Changing the SYSTEM password	
All Users in a Group		On a redundant system .....	93
Removing .....	85	On a remote Comm Controller .....	93
Application token icons.....	40	On a Reporting or Messaging server .....	93
Application Token tab.....	60	On a SingleBox and Standalone Server.....	92
Application tokens		On a Standalone Workstation.....	92, 94
Drag & drop .....	41	Container Tokens .....	115
Application Tokens .....	111	Creating .....	24, 25, 31
Assigning Privileges .....	97	New Access Areas.....	31, 44, 82
Associated Access Areas .....	59	New Application Tokens.....	82
Auto Log Out (Fixed Period) .....	57	New Token Groups.....	80
Auto Log Out (Inactivity).....	57	New User .....	24, 25, 79
Available Access Areas .....	59	New User Groups .....	23, 36, 79
Batch Processing Pane .....	102	Tokens .....	81
Batch Progress Bar .....	102	Creating New Token Groups.....	30
Breaking Token Links .....	87	Creating Tokens .....	29
Button		Current User.....	19
Add.....	59, 72	Custom Token tab.....	62
Apply .....	50, 57, 58, 60, 61, 64, 66, 68, 70, 96	Custom tokens	
Browse.....	50, 75	Modifying.....	87
Cancel ..20, 50, 57, 58, 59, 61, 64, 66, 68, 70, 75, 96,		Custom Tokens .....	41
101, 102		Data Collections Tokens .....	116
Cancel .....	73	DataView Tokens .....	117
Cancel .....	74	Days (expires in).....	55
Cancel (Token Group Properties) .....	72	Default Group	
Close .....	102		

Adding.....	80	Application tokens .....	41
Default Group node .....	33	Driver Configuration Tokens.....	118
Default Group Properties dialog .....	53	Equipment Tokens .....	118
Default Security Database.....	18	Expiry Warning.....	56
Default User Settings		Failed Log On Attempts.....	57
Modifying .....	83	Fallback Database .....	18
Delay Between Batches .....	101	Field	
Deleting		Access Area .....	48, 71, 73
Access Areas .....	89	Accessed.....	61, 63, 66, 68, 70
Groups.....	89	Account Disabled.....	49
Tokens.....	89	Account LockOut .....	49
Users .....	89	Active Database .....	19
Deleting Security Objects.....	89	Available Tokens .....	64, 67, 69, 71
Desktop Login-Logout File Precedence .....	51	Can't Remove System User from Access Area .....	77
Desktop Tokens .....	127	Change Password at Next Logon .....	48
Device Configuration (HART) Tokens .....	117	Configured Tokens.....	71
Device Templates Tokens .....	117	Connected .....	19
Dialog		Current User.....	19
Default Group Properties .....	53	Days Prior to Expiry.....	56
Group Name Entry .....	37	Deleting an Access Area .....	77
Log In.....	14	Description .....	48, 71
Login Mappings .....	51, 52	Description .....	73
Message Suppression.....	76	Drag to Exclude List.....	76
Modify Logon Credentials .....	53	Drag to Include List .....	76
OE Desktop Security Options .....	8	Exclude List .....	61, 63, 65, 67, 70
Options.....	75	Expires In.....	55
Options – Message tab.....	77	Expiry Warning.....	56
Options – Token Drag tab .....	76	File Name .....	74
Security Configuration .....	46	Full Name.....	47
Security Manager.....	17, 19	Grantor .....	49
SQL Export.....	74	Include List.....	61, 63, 65, 67, 70
SQL Export.....	74	Location.....	19
Token Drag.....	75	Lock Out Duration .....	57
Token Group Properties .....	70, 71	Log Out (Fixed Period).....	57
Token Properties.....	72	Log Out (Inactivity) .....	57
Token Properties.....	72	Login.....	49
Token Summary.....	73	Logout .....	50
Token Summary.....	73	Maximum Length (password).....	56
User Name Entry .....	34	Minimum Age (password) .....	56
User Properties .....	46	Minimum Length (password).....	56
User Properties Account .....	55	Moving a User from its current group to a new one	77
User Properties Summary .....	57	Number of Failed Log On Attempts .....	57
Windows Run.....	7	Parent Group.....	49
Workstation Login Client.....	14	Password.....	48
Drag & Drop		Refuse Login When Password Expires .....	56

Refuse Login When Password Expires (ODBC/SQLC)	
.....	56
Removing User from Access Area.....	77
Security Database.....	18
System Administrator.....	48
Test String.....	61, 63, 65, 68, 70
Token Group Name.....	71
Token Name.....	73
Token Type.....	71
User Cannot Change Password.....	48
User is already a member of this group.....	77
User Name.....	47
Verify Password.....	48
Fields	
Available Tokens.....	60, 62
Figures	
1-1. User and Group Hierarchy.....	4
1-2. Run dialog.....	7
1-3. Settings Editor - Program ID string.....	7
1-4. OE Desktop Security Options dialog.....	8
1-5. Token Groups node context menu.....	9
1-6. Token Security Hierarchy diagram.....	11
1-7. OE Security Overview.....	13
1-8. Workstation Login Client dialog.....	14
1-9. Log In dialog.....	14
1-10. Security Manager dialog.....	17
1-11. Settings Editor – Fallback databases.....	18
1-12. Security Manager Properties dialog.....	19
2-1. Security Configuration Tool interface.....	21
2-2. Security Configuration Tool menu bar.....	21
2-3. Security Configuration tool File menu.....	22
2-4. Security Configuration tool Edit menu.....	23
2-5. Security Configuration Tool File menu New	
Group option.....	23
2-6. Security Configuration Tool Edit menu New User	
In Group option.....	23
2-7. New Group context menu.....	24
2-8. Security Configuration tool Edit menu New User	
option.....	24
2-9. New User context menu.....	24
2-10. New User Floating context menu.....	25
2-11. Security Configuration dialog.....	25
2-12. New User with blank entry.....	25
2-13. Security Configuration tool Edit menu New	
User option.....	26
2-14. New User context menu.....	26
2-15. New User context menu.....	26
2-16. New User context menu.....	26
2-17. New User context menu.....	27
2-18. New User with blank entry.....	28
2-19. User Linked to Active Directory - User	
Properties.....	28
2-20. User Linked to Active Directory – Account Tab	
.....	29
2-21. Security Configuration tool Edit menu –New	
Token.....	30
2-22. Token node menu.....	30
2-23. Security Configuration tool Edit menu New	
Token menu.....	30
2-24. Token Group node.....	31
2-25. Security Configuration tool Edit menu New	
Access Area.....	31
2-26. Access Area node menu.....	31
2-27. Security Configuration tool Tools menu	
Options.....	32
2-28. Tree pane.....	33
2-29. Default Group node.....	33
2-30. Users node.....	34
2-31. User node menu – Paste Option.....	34
2-32. User Name Entry dialog.....	34
2-33. User node menu.....	35
2-34. Groups node menu.....	36
2-35. Security Configuration tool Edit menu New	
Group.....	36
2-36. Group node menu.....	36
2-37. New Group context menu.....	37
2-38. Group node menu –Paste option.....	37
2-39. Group Name Entry dialog.....	37
2-40. Group node menu.....	38
2-41. Expanded Tokens node.....	39
2-42. Token Groups node.....	39
2-43. Token Groups menu.....	39
2-44. Expanded Token Groups node.....	40
2-45. Application Tokens node.....	40
2-46. Selected Application Token type.....	41
2-47. Selected Custom Token node.....	42
2-48. Selected File Token node.....	43
2-49. Expanded OPC Item node.....	43
2-50. Access Areas node.....	44

2-51. Security Configuration tool Edit menu – New Access Area..... 44	3-22. Log In dialog.....91
2-52. New Access Area context menu ..... 44	3-23. Log In password prompt.....91
2-53. Selected Access Area ..... 45	3-24. Change Password dialog.....91
2-54. List pane (showing users) ..... 45	3-25. Change password confirmation dialog .....92
2-55. User Properties - tabs ..... 46	4-1. Security Group Privileges editor.....96
2-56. User Properties dialog ..... 47	4-2. Security Group Privileges Editor drop down ....97
2-57. Login Mappings dialog ..... 52	4-3. Security Group Privileges Editor main menu ...98
2-58. Modify Login Credentials dialog ..... 53	4-4. Security Group Privileges Editor – File menu ...99
2-59. Group Properties – Properties tab ..... 54	4-5. Security Group Privileges Editor – Edit menu ..99
2-60. Group Properties – Account tab ..... 55	4-6. Security Group Privileges Editor – View menu.99
2-61. User Properties – Summary tab ..... 58	4-7. Security Group Privileges Editor – Tools menu ..... 100
2-62. User Properties – Access Areas tab ..... 59	4-8. Security Group Privileges Editor – Help menu ..... 100
2-63. User Properties – Application Token tab..... 60	4-9. SQL Batch Options dialog ..... 101
2-64. User Properties – Custom Token tab ..... 62	4-10. SQL Execution dialog .....102
2-65. User Properties – File Token tab ..... 64	4-11. Error processing SQL dialog ..... 103
2-66. User Properties – OPC Item Token tab..... 66	4-12. SQL Execution dialog with errors ..... 103
2-67. User Properties – Token Group tab..... 69	B-1. Abstract Layers Tokens.....112
2-68. Token Group Properties dialog..... 71	B-2. AdHocList Tokens.....112
2-69. Token Properties dialog ..... 72	B-3. Alarm Banner Tokens ..... 113
2-70. Token Summary dialog ..... 73	B-4. Alarm View Tokens.....114
2-71. SQL Export dialog..... 74	B-5. Calculations Tokens.....115
2-72. Options dialog – Token Drag tab ..... 76	B-6. Container Tokens .....116
2-73. Options dialog – Message tab ..... 77	B-7. Data Collection Tokens.....116
3-1. New Token option, Edit menu ..... 79	B-8. DataView Tokens ..... 117
3-2. New User in Group menu option ..... 79	B-9. Pass-Through Tokens .....117
3-3. New Group context menu option ..... 80	B-10. Device Template Tokens ..... 117
3-4. Add Default Groups context menu option ..... 80	B-11. Driver Configuration Tokens.....118
3-5. New Token menu option..... 81	B-12. Equipment Tokens .....118
3-6. New Token Group context menu option..... 81	B-13. OE Graphics Tokens.....119
3-7. New Token menu option..... 81	B-14. History Editor Tokens ..... 122
3-8. New Token context menu option ..... 82	B-15. Network Configuration Tokens.....122
3-9. New Access Area menu option ..... 82	B-16. OE Notes View Tokens.....123
3-10. New Access Area context menu ..... 82	B-17. Alarm Client Tokens ..... 124
3-11. Default Properties menu option ..... 83	B-18. OEDesktop Tokens.....127
3-12. Properties context menu option..... 83	B-19. Report Selector Tokens ..... 129
3-13. Properties context menu option..... 84	B-20. Secure Desktop Tokens ..... 130
3-14. New User in Group menu option ..... 84	B-21. Session Manager Tokens .....132
3-15. Drag and drop User to the Tree ..... 85	B-22. Site Tokens.....132
3-16. Remove All User menu option ..... 85	B-23. SQL View Tokens .....133
3-17. Properties context menu option..... 86	B-24. Trend View Tokens.....134
3-18. Token Properties context menu option ..... 87	B-25. Workflows Tokens.....136
3-19. Summary Token menu option..... 88	File Precedence .....51
3-20. Properties context menu option..... 89	File Token tab.....64
3-21. Delete context menu option ..... 90	

File tokens .....	42	Modifying Custom tokens .....	87
Modifying .....	87	Modifying File tokens .....	87
Graphics View Tokens .....	119	Modifying OPC Item tokens.....	87
Group Configuration		Modifying Security Objects.....	83
Paste.....	37	Network Configuration Tokens.....	122
Group Name Entry dialog.....	37	New Access Areas.....	31
Group Nodes .....	38	Creating .....	31, 44, 82
Groups.....	2, 97	New Application Tokens	
Groups node .....	35	Creating .....	82
History Editor Tokens.....	122	New Token Groups	
Iconics Security Server .....	15	Creating .....	30, 80
Linking		New User	
Tokens.....	86	Creating .....	24, 25
Linking tokens or token groups with Users or groups		New User Groups .....	23, 36
.....	86	Creating .....	23, 36, 79
List Pane .....	45	New User to User Group	
Lock Out Duration.....	57	Adding .....	84
Logging into the container for the first time .....	90	Node	
Login Mappings dialog .....	51	Access Area .....	43
Managing Security Objects .....	79	Nodes	
Menu		Token.....	39
Edit.....	17, 99	Token Groups.....	39
Edit.....	22	Notes View Tokens.....	123
File.....	17, 22, 99	ODBC	
Group node .....	36, 38	Refuse Login When Password Expires .....	56
Groups node .....	36	OE Desktop Files.....	51
Help.....	17, 32, 100	OE Security Configuration Tool Overview .....	79
New Access Area context .....	44	OE Security Manager.....	13
New Group floating context .....	37	Online help system.....	1
Token Groups .....	39	OPC Item Token tab .....	66
Tools.....	31, 100	OPC Item Tokens.....	43
User node .....	35	OPC Items tokens	
View .....	17, 99	Modifying.....	87
Menu bar		Option	
Security Configuration .....	21	Hide on Minimise .....	20
Menu Option		Minimised .....	20
Exit .....	22	Show System Tray Icon.....	20
Export.....	22	Show Window .....	20
Message Suppression dialog .....	76	Options dialog.....	75
Modify Logon Credentials dialog .....	53	Overview.....	13
Modifying		OE Security.....	1
Access Areas .....	88	Password	
Default User Settings .....	83	SYSTEM.....	1
Token Groups .....	85	Password Expiry .....	55
User Account Settings.....	83	Paste Group Configuration .....	37

Paste User Configuration .....	34	Abstract Layers.....	112
Refuse Login When Password Expires (OE Components).....	56	AdHoc List.....	112
Removing		Alarm Banner .....	113
All Users in a Group .....	85	Alarm Client .....	124
Report Selector Tokens .....	129	Alarm View.....	113
Sec File.....	15	Calculations .....	115
Secure Desktop Tokens.....	130	Container .....	115
Security .....	1	Creating.....	29, 81
Tokens.....	3	Data Collection .....	116
Security Configuration dialogs .....	46	DataView .....	117
Security Configuration tool .....	1, 21	Desktop .....	127
Help menu.....	32	Device Configuration .....	118
Tools menu.....	31	Device Configuration (HART) .....	117
Security Configuration Tool .....	15	Device Templates.....	117
Security Group Privileges Editor .....	1, 15	Equipment .....	118
Security Group Privileges Overview .....	95	File .....	42
Security Objects		Graphics View .....	119
Deleting.....	89	History Editor .....	122
Managing .....	79	Linking .....	86
Modifying .....	83	Network Configuration.....	122
Session Manager Tokens.....	132	Notes View.....	123
SitesTokens .....	132	OPC Item .....	43
SQL Batch Size .....	101	Pattern Matching .....	9
SQL Batches Page.....	100	Report Selector .....	129
SQL Components.....	56	Secure Desktop.....	130
SQL Errors .....	103	Session Manager .....	132
SQL Export dialog.....	74	Sites.....	132
SQL View Tokens.....	133	SQL View.....	133
Summary list.....	58	Trend View.....	134
Table .....	97	Wildcards.....	9
Toggle Batch Operation .....	101	Workflow .....	136
Token Drag dialog.....	75	Tokens or token groups	
Token Group Icons.....	40	linking with Users or groups .....	86
Token Group Properties dialog.....	70	Tool	
Token Groups		OE Security Configuration Overview.....	79
Modifying .....	85	Security Configuration .....	1, 21
Token Groups Nodes.....	39	Security Configuration tool .....	15
Token links		Security Group Privileges Editor.....	1, 15
Breaking .....	87	Tree Pane .....	32
Viewing .....	87	Trend View Tokens .....	134
Token nodes .....	39	Unlocking a locked account.....	57
Token Properties dialog .....	72	User Account Settings	
Token Summary dialog .....	73	Modifying.....	83
Tokens.....	3, 111	User Configuration	
		Paste.....	34

User Configured Token Groups .....	40	User Properties Account tab .....	55
User Groups .....	98	User Properties Summary dialog .....	57
User Name Entry dialog .....	34	User Token Group tab .....	68
User node icons .....	34	Users .....	2
User Properties		Users node .....	33
Custom Token tab .....	62	View .....	97
File Token tab .....	64	Viewing Token Links .....	87
OPC Item Token tab .....	66	Workflows Tokens .....	136
User Token Group tab .....	68		

# Configuring OpenEnterprise Security

D301796X012

September 2017

---

For customer service and technical support,  
visit [www.EmersonProcess.com/Remote/Support](http://www.EmersonProcess.com/Remote/Support).

## Global Headquarters,

### North America, and Latin America:

Emerson Automation Solutions  
Remote Automation Solutions  
6005 Rogerdale Road  
Houston, TX 77072 U.S.A.  
T +1 281 879 2699 | F +1 281 988  
4445

[www.EmersonProcess.com/Remote](http://www.EmersonProcess.com/Remote)

### Europe:

Emerson Automation Solutions  
Remote Automation Solutions  
Unit 8, Waterfront Business Park  
Dudley Road, Brierley Hill  
Dudley UK DY5 1LX  
T +44 1384 487200 | F +44 1384  
487258

### Middle East/Africa:

Emerson Automation Solutions  
Remote Automation Solutions  
Emerson FZE  
P.O. Box 17033  
Jebel Ali Free Zone – South 2  
Dubai U.A.E.  
T +971 4 8118100 | F +971 4  
8865465

### Asia-Pacific:

Emerson Automation Solutions  
Remote Automation Solutions  
1 Pandan Crescent  
Singapore 128461  
T +65 6777 8211 | F +65 6777 0947

© 2014 -2017 Remote Automation Solutions, a business unit of Emerson Automation Solutions. All rights reserved.

This publication is for informational purposes only. While every effort has been made to ensure accuracy, this publication shall not be read to include any warranty or guarantee, express or implied, including as regards the products or services described or their use or applicability. Remote Automation Solutions (RAS) reserves the right to modify or improve the designs or specifications of its products at any time without notice. All sales are governed by RAS terms and conditions which are available upon request. RAS accepts no responsibility for proper selection, use or maintenance of any product, which remains solely with the purchaser and/or end-user.