

OpenEnterprise Security Configuration Reference Guide (V2.83)

Contents

1	Security Configuration Overview	1
1.1	Security Manager	1
1.2	Login Client	1
1.3	Security and Workstation Views	1
1.4	Security and the Toolbox	2
1.5	The Security Configuration Tool	2
1.6	Access to the Login Client.....	2
1.7	Security settings applied	2
2	Security Concepts	2
2.1	Users and Groups	2
2.1.1	Users	3
2.1.2	Groups	3
2.1.3	Default Group	3
2.1.4	User and Group Hierarchy.....	3
2.2	User and Group Hierarchy	3
2.3	Tokens	4
2.3.1	Application Tokens	4
2.3.2	File Tokens	4
2.3.3	OPC Item Token Types	4
2.3.4	Custom Tokens	5
2.3.4.1	Custom Token Examples	5
2.3.4.2	Disabling Custom Menus	5
2.3.4.3	Hiding Toolbox Components.....	5
2.3.4.4	Disabling Toolbox Table Mode	6
2.3.4.5	Limiting Toolbox Table Mode.....	6
2.3.4.5.1	Disable Inserting of Objects.....	6
2.3.4.5.2	Disable Modifying of Objects	6
2.3.4.5.3	Disable Deleting of Objects	6
2.3.4.6	Protecting Windows	6
2.3.5	Token Wildcards.....	7
2.3.6	Token Pattern Matching	7
2.3.6.1	Wildcards	7
2.3.6.2	File Tokens.....	8
2.3.7	Token Security Hierarchy	8
2.4	Access Areas	9
2.5	Database Privileges	9
3	Security Config Tool Interface.....	10
3.1	Menu Bar.....	10
3.1.1	File Menu	11
3.1.1.1	Export.....	11
3.1.1.2	Import	11
3.1.1.3	Exit	11
3.1.2	Edit Menu.....	12
3.1.2.1	Creating New User Groups.....	12
3.1.2.2	Creating a New User.....	13

3.1.2.3	Creating Custom, File and OPC Item Tokens	13
3.1.2.4	Creating New Token Groups	14
3.1.2.5	Creating New Access Areas	15
3.1.3	Tools Menu.....	16
3.1.4	Help Menu	16
3.2	The Tree Pane	16
3.2.1	The Tree Pane.....	16
3.2.2	Default Group Node.....	17
3.2.3	Users Node.....	17
3.2.3.1	Creating a New User.....	17
3.2.3.2	Paste User	18
3.2.4	User Nodes.....	19
3.2.4.1	Context Menu.....	19
3.2.4.2	Properties.....	19
3.2.4.3	Copy.....	19
3.2.4.4	Delete.....	19
3.2.4.5	Remove From Group	20
3.2.5	Groups Node	20
3.2.5.1	Creating New User Groups.....	20
3.2.5.2	Adding the Default Groups.....	21
3.2.5.3	Paste Group.....	21
3.2.6	Group Nodes	22
3.2.6.1	User Group Properties	22
3.2.6.2	Add New User to Group.....	22
3.2.6.3	Copy Group.....	22
3.2.6.4	Delete Group.....	22
3.2.7	Tokens Node	22
3.2.7.1	Token Groups Node.....	23
3.2.7.1.1	Token Group Nodes	23
3.2.7.1.1.1	User Configured Token Groups	24
3.2.7.2	Application Tokens Node	24
3.2.7.2.1	Application Token Component Types.....	24
3.2.7.2.2	Drag-dropping Application Tokens	25
3.2.7.3	Custom Tokens.....	25
3.2.7.4	File Tokens.....	25
3.2.7.5	OPC Item Tokens.....	26
3.2.8	Access Areas Node	27
3.2.8.1	Creating New Access Areas	27
3.2.9	Access Area Nodes	27
3.3	The List Pane	28
4	Security Config Tool Tasks.....	29
4.1	Creating Security Objects	30
4.1.1	New Users and Groups	30
4.1.1.1	Creating a New User.....	30
4.1.1.2	Creating New User Groups.....	31
4.1.1.3	Adding the Default Groups.....	31
4.1.2	New Tokens.....	32
4.1.2.1	Creating New Token Groups	32
4.1.2.2	Creating Custom, File and OPC Item Tokens	33

4.1.2.3	On Creating New Application Tokens	34
4.1.3	Creating New Access Areas	34
4.2	Modifying Security Objects	34
4.2.1	Modifying Users and Groups	34
4.2.1.1	Modifying Default Group Settings	34
4.2.1.2	Modifying User Account Settings	35
4.2.1.3	Adding a New User to a Group	35
4.2.1.4	Removing All Users from a Group	36
4.2.2	Modifying Tokens	36
4.2.2.1	Modifying Token Groups	36
4.2.2.2	Linking Tokens with a Token Group	37
4.2.2.3	Linking Tokens or Token Groups with Users or Groups	37
4.2.2.4	Modifying Custom, File and OPC Item Tokens	37
4.2.2.5	Viewing and Breaking Token Links	38
4.2.3	Modifying Access Areas	38
4.2.4	Deleting Security Objects	39
5	Security Configuration Dialogs	39
5.1	User Property Pages	40
5.1.1	The User Properties Page	40
5.1.1.1	User Name	41
5.1.1.2	Full Name	41
5.1.1.3	Description	41
5.1.1.4	Password	41
5.1.1.5	Verify Password	42
5.1.1.6	Access Area	42
5.1.1.7	Change Password at Next Logon	42
5.1.1.8	User Cannot Change Password	42
5.1.1.9	System Administrator	42
5.1.1.10	Account Disabled	42
5.1.1.11	Account Lockout	42
5.1.1.12	Grantor	43
5.1.1.13	Configure Group Privileges	43
5.1.1.14	Parent Group	43
5.1.1.15	OK Button	43
5.1.1.16	Cancel Button	43
5.1.1.17	Apply Button	43
5.1.1.18	Login Checkbox	43
5.1.1.19	OEDesktop Login - Logout File Precedence	43
5.1.1.20	Logout Checkbox	44
5.1.1.21	Logged in OEDesktop Filename	44
5.1.1.22	Logged out OEDesktop Filename	44
5.1.1.23	OED File Browse Button	44
5.1.2	User Group Properties Page	45
5.1.3	The User Account Page	45
5.1.3.1	Expires In	46
5.1.3.2	Expiry Warning	46
5.1.3.3	Refuse Login When Password Expires for OE Components	46
5.1.3.4	Refuse Login When Password Expires for ODBC or SQL Components	47
5.1.3.5	Password Length Section	47

5.1.3.6	Maximum Length.....	47
5.1.3.7	Minimum Length.....	47
5.1.3.8	Password Age Section.....	47
5.1.3.9	Minimum Age	47
5.1.3.10	Account Lockout	47
5.1.3.11	Lockout Duration.....	48
5.1.3.12	Number of Failed Logon Attempts Before Lockout.....	48
5.1.3.13	Auto Logout Section	48
5.1.3.14	Logout Fixed Period.....	48
5.1.3.15	Logout After Inactivity	48
5.1.3.16	Apply Logout Per Database Connection	48
5.1.4	The User Summary Page	48
5.1.4.1	Summary List	49
5.1.4.2	OK Button.....	49
5.1.4.3	Cancel Button.....	49
5.1.4.4	Apply Button.....	49
5.1.5	The User Access Areas Page	49
5.1.5.1	Available Access Areas	50
5.1.5.2	Add Access Area Button	50
5.1.5.3	Remove Access Area	50
5.1.5.4	Associated Access Areas	50
5.1.5.5	OK Button.....	50
5.1.5.6	Cancel Button.....	50
5.1.5.7	Apply Button.....	51
5.1.6	The User Application Token Page.....	51
5.1.6.1	Available Tokens.....	51
5.1.6.2	Include Button	51
5.1.6.3	Remove Button	51
5.1.6.4	Exclude Button.....	52
5.1.6.5	Test String.....	52
5.1.6.6	String Accessed	52
5.1.6.7	OK Button.....	52
5.1.6.8	Cancel Button.....	52
5.1.6.9	Apply Button.....	52
5.1.7	The User Custom Token Page.....	52
5.1.7.1	Available Tokens.....	53
5.1.7.2	Include Button	53
5.1.7.3	Remove Button	53
5.1.7.4	Exclude Button.....	53
5.1.7.5	Include List	53
5.1.7.6	Exclude List.....	54
5.1.7.7	Test String.....	54
5.1.7.8	Accessed Check Box	54
5.1.7.9	OK Button.....	54
5.1.7.10	Cancel Button	54
5.1.7.11	Apply Button.....	54
5.1.8	The User File Token Page.....	54
5.1.8.1	Available Tokens.....	55
5.1.8.2	Include Button	55
5.1.8.3	Remove Button	55

5.1.8.4	Exclude Button	55
5.1.8.5	Include List	55
5.1.8.6	Exclude List	56
5.1.8.7	Test String	56
5.1.8.8	Accessed Check Box	56
5.1.8.9	OK Button	56
5.1.8.10	Cancel Button	56
5.1.8.11	Apply Button	56
5.1.9	The User OPC Item Page	56
5.1.9.1	Available Tokens	57
5.1.9.2	Include Button	57
5.1.9.3	Remove Button	57
5.1.9.4	Exclude Button	57
5.1.9.5	Include List	57
5.1.9.6	Exclude List	58
5.1.9.7	Test String	58
5.1.9.8	Accessed Check Box	58
5.1.9.9	OK Button	58
5.1.9.10	Cancel Button	58
5.1.9.11	Apply Button	58
5.1.10	The User Token Group Page	58
5.1.10.1	Available Tokens	59
5.1.10.2	Include Button	59
5.1.10.3	Remove Button	59
5.1.10.4	Exclude Button	59
5.1.10.5	Include List	59
5.1.10.6	Exclude List	60
5.1.10.7	Test String	60
5.1.10.8	Accessed Check Box	60
5.1.10.9	OK Button	60
5.1.10.10	Cancel Button	60
5.1.10.11	Apply Button	60
5.2	Token Group Property Dialog	60
5.2.1	Token Group Name	61
5.2.2	Token Access Area	61
5.2.3	Token Group Description	61
5.2.4	Token Type Section	61
5.2.5	Available Tokens	61
5.2.6	Component Column	61
5.2.7	Configured Tokens List - Token Groups	62
5.2.8	Add Button	62
5.2.9	Remove Tokens Button	62
5.3	Token Properties Dialog	62
5.3.1	Token Name	62
5.3.2	Token Access Area	63
5.3.3	Token Description	63
5.3.4	OK Button	63
5.3.5	Cancel Button	63
5.4	Token Summary Dialog	63
5.4.1	Token Summary	63

5.4.2	Remove All Links Button	63
5.4.3	Token Summary Cancel Button.....	64
5.5	SQL Import-Export File Dialog	64
5.5.1	File Name	64
5.5.2	File Browse Button	64
5.5.3	OK Button	65
5.5.4	Cancel Button	65
5.6	File Import Dialog	65
5.6.1	Import Button	65
5.6.1.1	Import Warning.....	65
5.6.2	Save to File Button	66
5.6.3	Status Pane	66
5.6.4	Status Message	66
5.6.5	Close Button	66
5.6.6	Help Button	66
5.7	Options Dialog.....	66
5.7.1	Token Drag to Include List.....	67
5.7.2	Token Drag Exclude	67
5.7.3	Options Dialog - Messages Tab	67
5.7.3.1	Removing SYSTEM User from Access Area	68
5.7.3.2	Already a Member of this Group	68
5.7.3.3	Removing User from Access Area.....	68
5.7.3.4	Deletion of Access Area.....	68
5.7.3.5	Moving User from Current Group.....	68
5.7.4	Options Dialog - Password Tab.....	69
5.7.4.1	Password Visible.....	70
5.7.4.2	Enabling the Password Tab	70
6	Application Tokens Reference	70
6.1	Alarm View Tokens	70
6.1.1	Acknowledge	71
6.1.2	Acknowledge All	71
6.1.3	Adjust Historical Time Range	71
6.1.4	Alarm Client Demand Printing	71
6.1.5	Alarm Client Properties.....	71
6.1.6	Column Alias.....	71
6.1.7	Create Event.....	72
6.1.8	Disable Audio Alert	72
6.1.9	Event Log Editing (High).....	72
6.1.10	Event Log Editing (Medium).....	72
6.1.11	Event Log Editing (Low)	72
6.1.12	Exceed Current Historical Time Range.....	72
6.1.13	Export Data	72
6.1.14	Modify Filter.....	72
6.1.15	Refresh.....	72
6.1.16	Resize Columns	72
6.1.17	Silence.....	72
6.1.18	Silence All.....	73
6.1.19	Suppression	73
6.1.20	Suppression All	73

6.1.21	Timed Mute	73
6.1.22	Timed Suppression	73
6.1.23	Unsuppress	73
6.1.24	Unsuppress All	73
6.2	Trend View Tokens	73
6.2.1	Add Pen	74
6.2.2	Adjust Refresh Interval	74
6.2.3	Adjust Time Range (Simple).....	74
6.2.4	Adjust Time Range (Advanced).....	74
6.2.5	Export Trend Data to File	74
6.2.6	Hide Details	75
6.2.7	Hide Global X-Axis for a Trend.....	75
6.2.8	Hide Global Y-Axis	75
6.2.9	Hide Marker	75
6.2.10	Hide Pen.....	75
6.2.11	Hide X-Axis for Pen	75
6.2.12	Hide Y-Axis for Pen	75
6.2.13	Modify Pen	75
6.2.14	Refresh Trend Against Original Settings.....	75
6.2.15	Remove All Pens.....	75
6.2.16	Remove Pen.....	75
6.2.17	Show All Data.....	75
6.2.18	Show Details	75
6.2.19	Show Global X-Axis for a Trend.....	75
6.2.20	Show Global Y-Axis for a Trend.....	76
6.2.21	Show Marker	76
6.2.22	Show Pen	76
6.2.23	Show X-Axis for a Pen	76
6.2.24	Show Y-Axis for a Pen	76
6.2.25	Trend - Properties	76
6.2.26	Trend View - Demand Printing.....	76
6.2.27	Zoom In	76
6.2.28	Zoom Out	76
6.2.29	Zoom Out Full.....	76
6.2.30	Zoom to 100%.....	76
6.2.31	Zoom to 150%.....	76
6.2.32	Zoom to 25%	76
6.2.33	Zoom to 250%.....	76
6.2.34	Zoom to 50%	77
6.2.35	Zoom to 75%.....	77
6.2.36	Zoom to Custom.....	77
6.2.37	Zoom Undo.....	77
6.3	OEDesktop Tokens	77
6.3.1	Change a Windows File.....	78
6.3.2	Change Child Frame Type	78
6.3.3	Change Workspace File	78
6.3.4	Configure Mode	78
6.3.5	Create Alarm Banner.....	78
6.3.6	Create Alarm Client	78
6.3.7	Create Alarm Printer.....	78

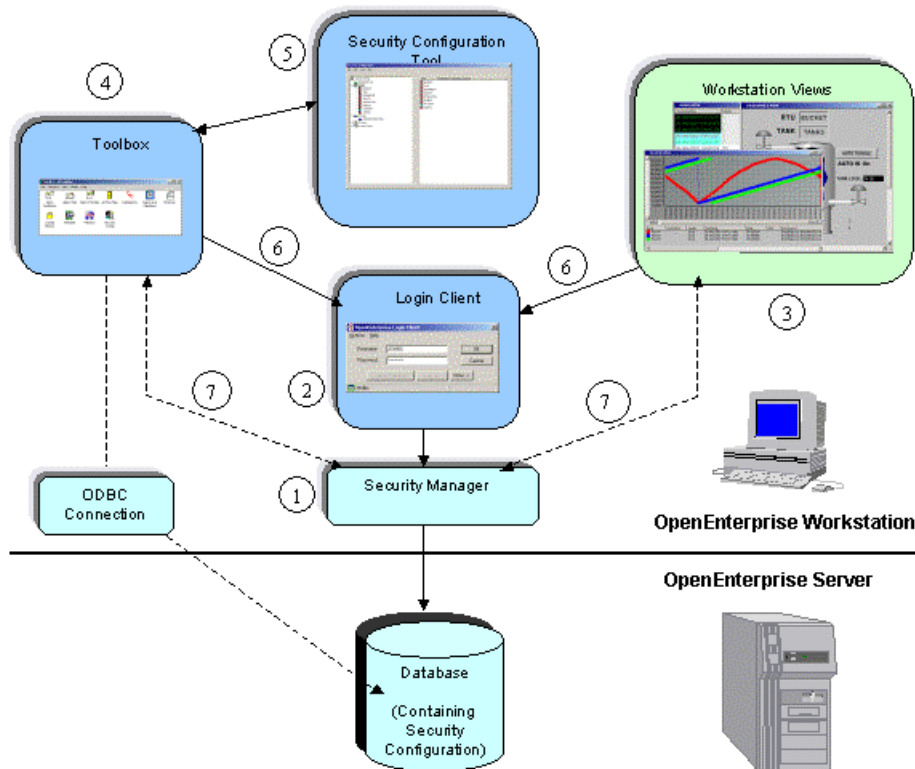
6.3.8	Create OEControl Display	78
6.3.9	Create Graphic View	78
6.3.10	Create Notes View	78
6.3.11	Create Signal View	78
6.3.12	Create SQL Viewer	78
6.3.13	Create Trend View	79
6.3.14	Create or Close Window	79
6.3.15	Customize Dialog	79
6.3.16	Exit Desktop	79
6.3.17	Move Menu or Toolbar	79
6.3.18	Open Alarm Banner	79
6.3.19	Open Alarm Client	79
6.3.20	Open Alarm Printer	79
6.3.21	Open Control Display	79
6.3.22	Open Graphic View	79
6.3.23	Open Notes Client	79
6.3.24	Open Signal View	79
6.3.25	Open SQL Viewer	79
6.3.26	Open Trend View	79
6.3.27	Save Alarm Banner	80
6.3.28	Save Alarm Client	80
6.3.29	Save Alarm Printer	80
6.3.30	Save OEControl Display	80
6.3.31	Save Graphic View	80
6.3.32	Save Notes Client	80
6.3.33	Save Signal View	80
6.3.34	Save SQL Viewer	80
6.3.35	Save Trend View	80
6.3.36	Toggle Status Bar	80
6.3.37	Toggle Toolbar	80
6.4	Signal View Tokens	80
6.4.1	Close Detail Windows	81
6.4.2	Security Level 1 - 6	81
6.4.3	Signal View - Demand Printing	81
6.4.4	Signal View - Properties	81
6.5	Notes View Tokens	81
6.5.1	Delete	81
6.5.2	Forward	81
6.5.3	Modify	81
6.5.4	New Note	81
6.5.5	Notes - Demand Printing	81
6.5.6	Notes - Print	81
6.5.7	Notes - Properties	81
6.5.8	View	82
6.6	Graphics View Tokens	82
6.6.1	Exit Application	82
6.6.2	GenTray AutoStart	82
6.6.3	GenTray AutoStop	83
6.6.4	Menu: Change Language	83
6.6.5	Menu: Display Back/Forward	83

6.6.6	Menu: Exit Runtime	83
6.6.7	Menu: File Open	83
6.6.8	Menu: Help Functions.....	83
6.6.9	Menu: Hide Layers	83
6.6.10	Menu: Print Functions	83
6.6.11	Menu: Set Scrollbar Visibility.....	83
6.6.12	Menu: Set Tooltip Visibility	83
6.6.13	Menu: Set Working Directory	83
6.6.14	Menu: Show Statistics.....	83
6.6.15	Menu: Zoom Functions	84
6.6.16	Pick: Alias Dialog	84
6.6.17	Pick: Custom Command	84
6.6.18	Pick: Display Back/Forward	84
6.6.19	Pick: Drag Drop Data Sources.....	84
6.6.20	Pick: Drag Drop Load Display.....	84
6.6.21	Pick: Embedded Window	84
6.6.22	Pick: Launch Application	84
6.6.23	Pick: Layer Visibility	84
6.6.24	Pick: Load Display.....	84
6.6.25	Pick: Popup Window	84
6.6.26	Pick: Run Script.....	84
6.6.27	Pick: Set Aliases	85
6.6.28	Pick: Switch Language.....	85
6.6.29	Start Application	85
6.6.30	Tab Load Display	85
6.6.31	Graphics View File Token: Layers	85
6.7	SQL View Tokens	85
6.7.1	SQL Viewer - Demand Printing	85
6.7.2	SQL Viewer - Properties.....	85
6.8	Alarm Banner Tokens	85
6.8.1	Access Area.....	86
6.8.2	Alarm Banner - Demand Printing.....	86
6.8.3	Alarm Banner - Properties	86
6.9	Secure Desktop Tokens.....	86
6.9.1	Full Desktop Access	86
6.9.2	Gentray: Automatic.....	86
6.9.3	Gentray: Autostart	87
6.9.4	Gentray: Autostop.....	87
6.9.5	Gentray: NT Service	87
6.9.6	Gentray: Start	87
6.9.7	Gentray: Stop	87
6.9.8	Keygroup 1	87
6.9.9	Keygroup 2	87
6.9.10	Keygroup 3.....	87
6.9.11	Keygroup 4.....	87
6.10	Report Selector Tokens.....	87
6.10.1	Edit Report Aliases.....	88
6.10.2	Email Report.....	88
6.10.3	Native Viewer	88
6.10.4	Navigate Reports	88

6.10.5	Print Report	88
6.10.6	Report Selector - Properties.....	88
6.10.7	Run and Publish Report	88
6.10.8	Run Report.....	88
6.10.9	Save Report	88
6.10.10	Select Report	88
6.10.11	Select Report Date.....	88
6.10.12	Select Report Format.....	89
7	Index	90

1 Security Configuration Overview

This diagram reveals how Security is implemented between the OpenEnterprise Server and Workstation.



1.1 Security Manager

The Security Manager is a server component, which runs in the background on the Workstation. The Security Manager acquires User Account details for the currently logged in User from the Database and performs Database transactions to generate journal messages. It also informs Workstation View components of the logged in User's security Token privileges, such as Application, File, OPC Item and Custom Tokens.

1.2 Login Client

The Login Client is used to enable a User at an OpenEnterprise Workstation to log on to the database. The Login Client connects to the Security Manager, and the Security Manager requests the log in from the database. The User can also change their password via the Login Client.

1.3 Security and Workstation Views

All Workstation View components are sourced with Application Token information directly from the OpenEnterprise Security Manager. The functionality available to the User when using these components is controlled by what Application Tokens have been assigned to that User.

1.4 Security and the Toolbox

To access the Toolbox editors, Users must login using the Login Client, which can be invoked from the Security menu of the Toolbox. Once the user is logged in, Workstation security ensures that Users are only able to see the editors in the Toolbox window for which they have the necessary String Token access. The Toolbox also makes a connection with the database via ODBC to provide its Table mode functionality.

1.5 The Security Configuration Tool

The Security Configuration tool is one of the OpenEnterprise configuration editors that are accessed from the Toolbox. Only Administrative users may access the Security Configuration tool. If changes are made using the Security Configuration tool, the Toolbox executes the transaction and writes this transaction to the 'Security Config.SQL' file, which is located in the Toolbox default folder location.

1.6 Access to the Login Client

Access to the Login Client is provided from the Security menu of the OEDesktop or the Toolbox. Once a user is logged in via the Login Client, all aspects of Workstation Security are applied through the Security Manager.

1.7 Security settings applied

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

2 Security Concepts

Security configuration applies to - Users and User Groups. It is important to understand how Users and User Groups relate to each other in OpenEnterprise.

Security is applied to Users and User Groups in three main ways:-

1. 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.
2. Access Areas - 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.
3. Database Privileges. Database privilege security grants access to whole tables or views within the OpenEnterprise Database. Without this, a User can neither see, nor manipulate the data within the Database. Database privileges are configured using a different tool from the toolbox - the security group privileges editor. Each User inherits Database privileges from their parent User Group.

2.1 Users and Groups

There are important differences between Users, created Groups and the Default Group. Users and Groups are stored in the Users table. In the Database, Users and Groups are treated like different types of Users. The following is a definition of all three security object types.

2.1.1 Users

A User is an individual who is able to log on to the OpenEnterprise application from an OpenEnterprise Workstation to view and update data. In the Database, a real user is given a type number of 0 (zero).

2.1.2 Groups

A Group is essentially a collection of Users 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. Each User may be allocated to one other Group in addition to the Default Group. All Users belong to the Default Group, and may belong to one other Group created by an Administrative User. In the Database, a Group created by an Administrative User is given a type number of 1.

2.1.3 Default Group

All Users including Administrative Users automatically belong to the Default Group. All Users automatically inherit the security settings of the Default Group. Users cannot be removed from this Group. In the Database, the Default Group is given a type number of 2.

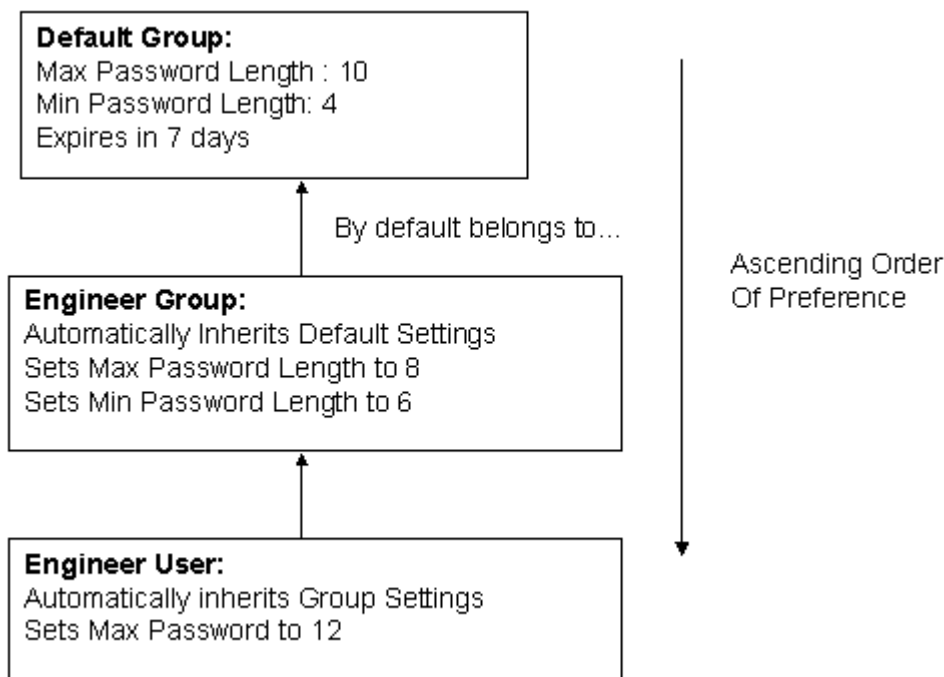
2.1.4 User and Group Hierarchy

User and Group Security Hierarchy - this hierarchy determines how account settings will be inherited on a User and Group level.

2.2 User and Group Hierarchy

Security account options may be configured at any one of the three levels: Default; Group; User. When a User or Group is first created they inherit the security account settings of the Default Group. If a User is included in a Group, then it inherits the Group's account settings. A Group may change some settings to suit particular requirements. These will override the Default Group settings. Likewise, a User may override its Group (if it belongs to a Group) as well as its Default Group settings.

To summarize with a diagram:



In the example shown the Group's settings for Passwords are: Max Length: 8; Min Length: 6; Expiry: 7days. The User's settings are Max Length: 12; Min Length: 6; Expiry: 7 days. Note: If a User only belongs to the Default Group, the middle Group level would not apply.

2.3 Tokens

Users can be granted or denied access to Workstation functionality by inserting Tokens into the User's Include or Exclude Token list. This is done using the User or User Group's Application, Custom, File and OPC Item Token Tabs. Templates can be set-up for all Tokens by creating a new Token Group within the Security Configuration tool . These Token Group templates can then be assigned to Users and User Groups through their Token Group Property Tab. Individual Users can still be granted extra privileges by using their Application Tokens Tab.

1. Application Tokens - used to disable View functions (such as changing to Configure Mode).
2. Custom Tokens - used to disable Custom Menus, or to 'protect' named windows from being closed.
3. File Tokens - used to control User access to View files on the Workstation.
4. OPC Item Tokens - used to control write access to process points on OpenEnterprise Graphic displays.
5. Token Groups - used as templates to grant or deny access to a range of View component functions to Users or User groups.

2.3.1 Application Tokens

These define actions that a User may perform within an OpenEnterprise Component. They cannot be created or edited by an Administrative User, although they can be assigned or denied individually to Users or Groups. They represent functions available from menu items within the component application, such as the "Acknowledge All" context menu available within the Alarm View component.

It may be desirable to remove this option from the Alarm View for some Users. This is done by adding this Token to the User's Excluded list of Application Tokens. Each OpenEnterprise Component has its own set of Application Tokens.

2.3.2 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, a File Token could be created with the name *.GDF. If the Token were then to be placed in a User's Excluded Token list, the User would not be able to load any Graphics View files into the OEDesktop (since Graphics files have an extension of *.GDF)

2.3.3 OPC Item Token Types

OPC (Object Linking and Embedding for Process Control) Tokens are strings that allow or deny write access to OPC points displayed on the Workstation. The String may represent part or all of the OPC string. When using a part of the OPC string, asterisks must be used as wildcards.

For example, an OPC Token is created with the name *RTU1* (note the asterisk wildcards at each end of the string), representing the name of an RTU. If no OPC Tokens are given to the Default User, then all other Users or Groups need to have the OPC Token for that RTU actively granted to them to be able to write to signals belonging to it from a data entry point on a Graphics View display.

If the Token were then placed in a User's Included OPC Token list, the User would find that they would now be able to change the value of any data entry process points on OpenEnterprise Graphics displays which reference RTU1. Note that:-

- Although a User is not able write to a data entry OPC point without the necessary OPC Token , it can still be viewed, but it is greyed out and cannot be selected.
- OPC Tokens do not affect writes made through the OEMenus Message Bus using the OEData Server

2.3.4 Custom Tokens

Custom Tokens are strings that can be security protected via Tokens. Here are some examples of how Custom Tokens can be used to provide Workstation security.

2.3.4.1 Custom Token Examples

Disabling Custom Menus

Hiding Toolbox Components

Disabling Toolbox Table Mode

Limiting Toolbox Table Mode

Protecting Windows in OEDesktop

2.3.4.2 Disabling Custom Menus

OpenEnterprise Custom Menus may be disabled for a User by inserting a string that matches the name of the Custom Menu into the Custom Token Exclude list for that User.

2.3.4.3 Hiding Toolbox Components

Configuration tools within the Toolbox may be hidden on a per User or User Group basis by inserting the Editor's Program ID into the Excluded list on the Custom page of the User Properties dialog for a User or User Group.

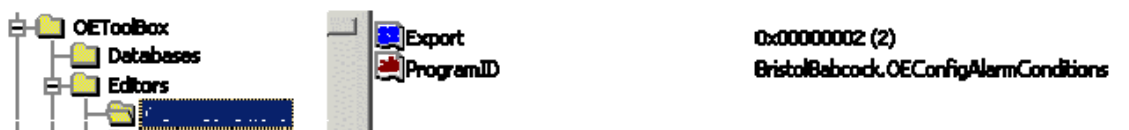
To find the Program ID of an editor, find the key of that editor under the following key :-

HKLM\SOFTWARE\

BristolBabcock\OpenEnterprise\Tasks\OEToolBox\Editors\<Editor>

On each Editor's key will be a string value named *ProgramID*. This string should be inserted into the Exclude list for the User or Group for which this editor should be excluded.

Example:



String = BristolBabcock.OEConfigAlarmConditions

Inserting this string into the Custom Token Exclude list for a User or Group would suppress this Tool from appearing in the Toolbox window when that User or a member of that Group is logged onto a Workstation.

Note: An Editor can also be removed from the Toolbox on a per Workstation basis by first removing its key from under the Editors key, if present, and then removing its Program ID from the list of editors found in the *Editor* string value on the Editors key, if present.

2.3.4.4 Disabling Toolbox Table Mode

The Custom Token that controls this feature is `OEConfig_Table_Mode`. If this string is inserted into a User's Custom Token Exclude list, the User is not able to access the Toolbox's Table mode, since the menu item is disabled.

2.3.4.5 Limiting Toolbox Table Mode

Once in table mode, a User may add, modify or delete objects by right clicking on a table and selecting a context menu. Any of these context menu items may be disabled in the following ways.

2.3.4.5.1 Disable Inserting of Objects

If the string "`OEConfig_Insert_Items`" is placed in the User's Excluded list, the User will be unable to add items to the database using the Toolbox in Table mode.

2.3.4.5.2 Disable Modifying of Objects

If the string "`OEConfig_Modify_Items`" is placed in the User's Excluded list, the User will be unable to add items to the database using the Toolbox in Table mode.

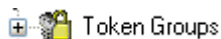
2.3.4.5.3 Disable Deleting of Objects

If the string "`OEConfig_Delete_Items`" is placed in the User's Excluded list, the User will be unable to add items to the database using the Toolbox in Table mode.

2.3.4.6 Protecting Windows

Users can be stopped from closing protected windows within the OEDesktop environment. To do this, the Window name must first be included in the Protected Windows list on the Windows tab of the OEDesktop Security Options dialog. This list is accessed from the OEDesktop Security/Configure menu.

Then, to complete the security configuration, the name of the protected window must be entered into the User's Custom Token Exclude list. This list is accessed using the OESecurity Config Tool.



The Token Groups node has a context menu which enables the user to create new Token Groups. See the Creating New Token Groups topic for more information.

When the Token Groups Node is expanded, it exposes the Token Group Type nodes. For more information on Token Group Nodes see the Token Group Nodes topic.

Token Groups are collections of Tokens, which may form a Template of Tokens to be associated with a User or User Group. User generated Token Groups may consist of a combination of any of the four types of tokens.

There are also several special Application Token Groups that are maintained independently of the Administrative User and are grouped by their Component name. They are the Alarm Banner, Alarm Client, Alarm Printer, OEDesktop, Graphics, Notes Client, Signal View, SQL Viewer and Trend View Token Groups. These Token Groups cannot be edited.

2.3.5 Token Wildcards

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

2.3.6 Token Pattern Matching

At runtime, the Include/Exclude lists are string compared as follows for each active User and Group until access is denied.

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 is performed.

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

2.3.6.1 Wildcards

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

2.3.6.2 File Tokens

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

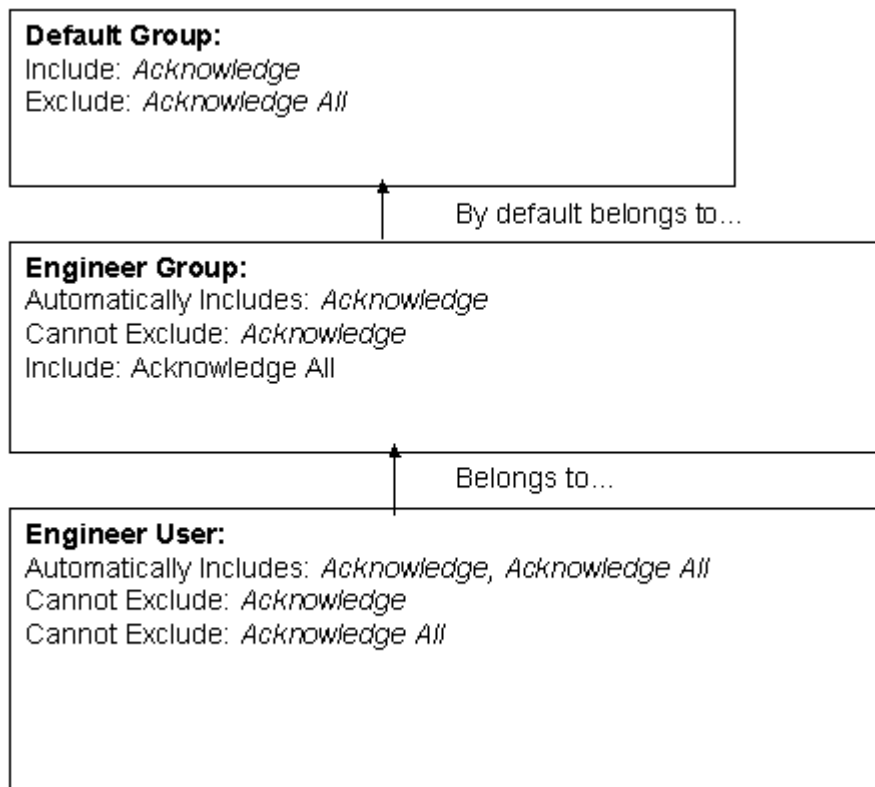
- The pattern matching is done on the file extension, separate from the file name to match the DOS wildcard semantics. For example the wildcard string to indicate all files is "*. *"
- A match is considered to have occurred if both the file name and extension match the given pattern.
- File names entered without a path are considered a match no matter what directory they are in.

2.3.7 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: -

1. Everyone inherits from the Default Group. Users belonging to another Group also inherit settings from that Group.
2. What is Included at one level cannot be Excluded at a different level.

This may be illustrated with a diagram: -



2.4 Access Areas

Each object has an Access Area with which it is associated. In the AccessArea table, each User is granted or denied the appropriate Access Areas for their operational needs. The User can only access objects belonging to the Access Areas which they have been granted.

This is implemented through the creation of database views when the User logs on to 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 only include objects that the logged in User has access to according to the AccessArea table. To complete the implementation, all the Workstation View components (e.g. Trend View, Alarm View etc.) are configured to retrieve objects from the database views, rather than the tables.

2.5 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. Access to this Editor can be gained from the User Properties Dialog, or from the Toolbox.

The User Groups have to be created first before the Security Privileges Editor can do its work. The Database Project Builder creates the following Groups, which have been found to cater for most functional requirements: -

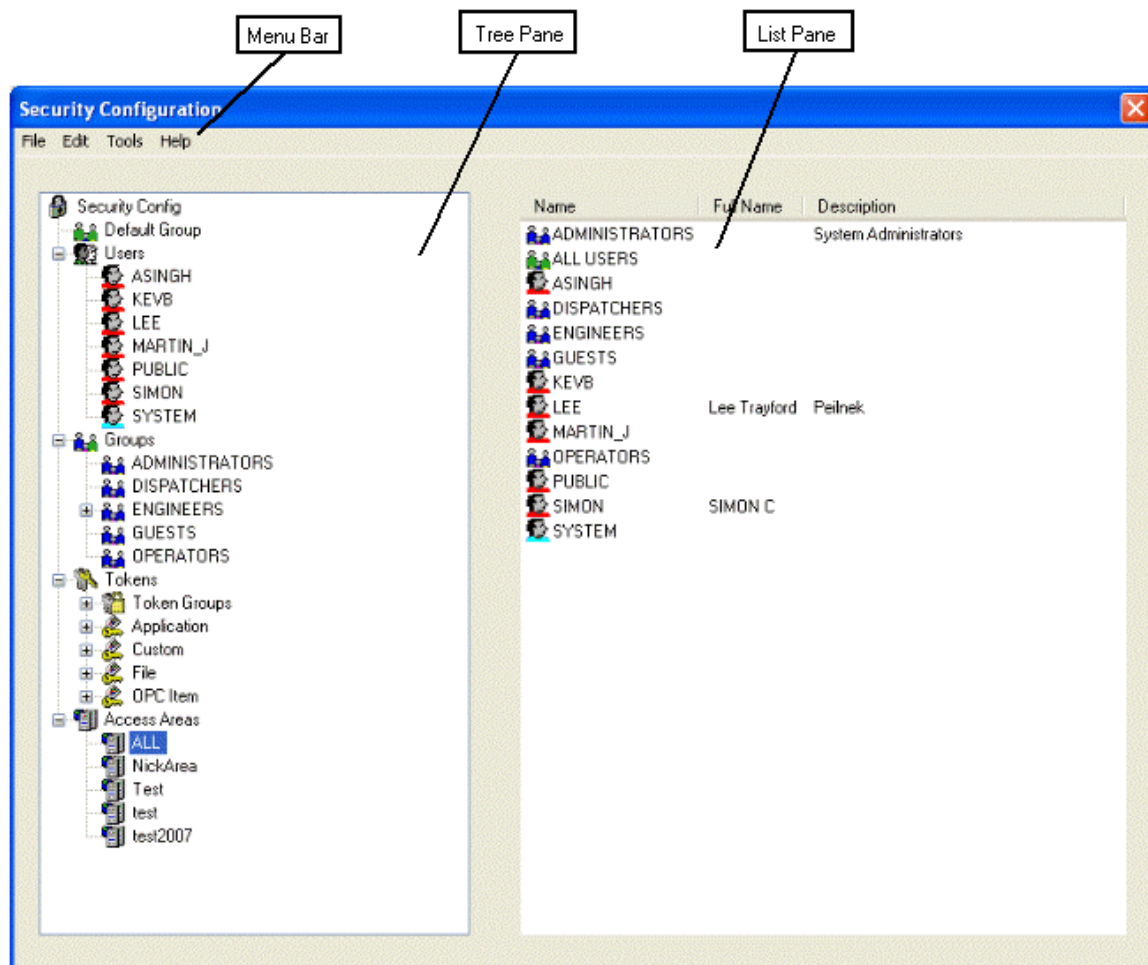
1. Administrators - have unrestricted access to all OpenEnterprise functionality.
2. Engineers - need configuration access to all system features except those related to controlling security privileges of other users.
3. Operators - are expected to be able to change set points, acknowledge alarms and perform basic Workstation configuration but no Server configuration.

4. Dispatchers - require read-only access to all operational and process data and the ability to acknowledge alarms. They are not required to change set points.
5. Guests - require read-only access to all operational and process data and the ability to acknowledge alarms. They are not required to change set points.

Then, Users must be assigned to the appropriate User Group to inherit the correct privileges for their required level of access.

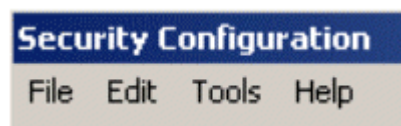
3 Security Config Tool Interface

This is the Security Configuration tool interface. It enables the Administrative User to configure all aspects of OpenEnterprise security.



3.1 Menu Bar

The Security Configuration tool Menu Bar provides access to all of its functions.



3.1.1 File Menu

This menu contains Import, Export and Exit options .



3.1.1.1 Export

The Export option enables you to save the current database Security Configuration to an SQL script file, which can be used to restore your Security settings at a later date.

When the Export option from the File drop down menu is selected, you will be presented with the SQL Import-Export File Dialog. This enables you to use the default SQL Export file, or to specify another file.

When the Export is completed, you will be informed by this message.



You must select the **[Close]** button to dismiss this dialog.

3.1.1.2 Import

The Import option enables you to import a previously saved (Exported) SQL script file into the database to restore your Security settings.

When you select the Import option from the File drop down menu, you will be presented with the SQL Import-Export File Dialog. This will enable you to accept the default Import filename, or to specify another file.

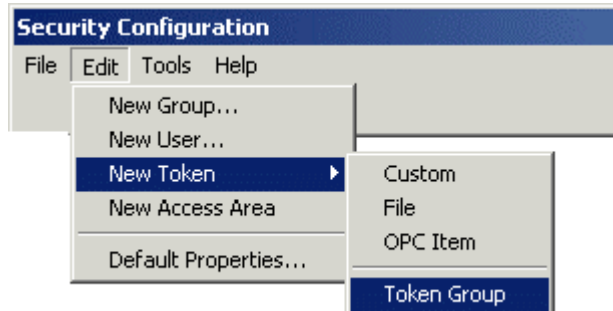
Once you click the **[OK]** button on the SQL Import dialog, the File Import dialog will be displayed, which initiates and monitors the Import process.

3.1.1.3 Exit

This option exits the Security Configuration tool, returning the focus back to the Toolbox window.

3.1.2 Edit Menu

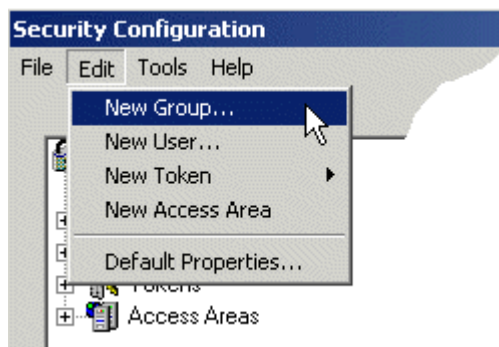
Items under this menu enable the Administrative User to create new Groups, Users, Tokens, Token Groups and Access Areas. There is also an option to edit settings for the Default Group.



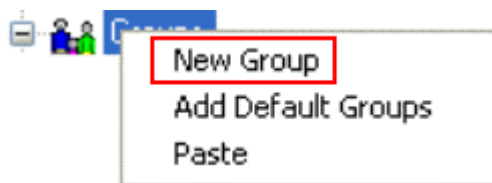
3.1.2.1 Creating New User Groups

A new Group may be created by any of the following methods:

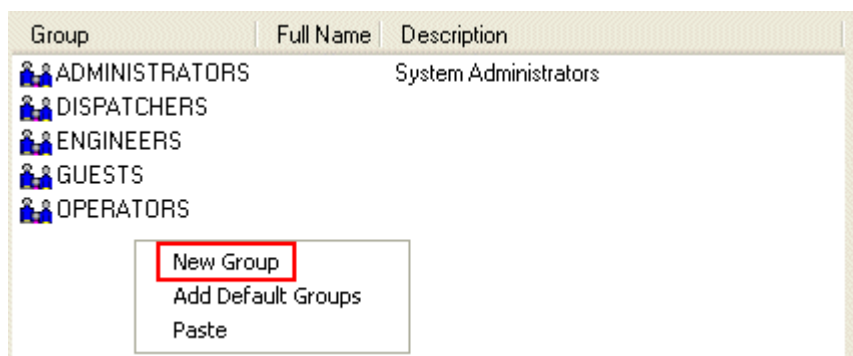
- Using the **Edit-New Group** menu item from the Security Configuration Tool menu bar.



- Using the **New Group** menu item from the Tree Pane:



- Using the floating **New Group** context menu from the List Pane when the **Groups** node is selected in the Tree Pane.

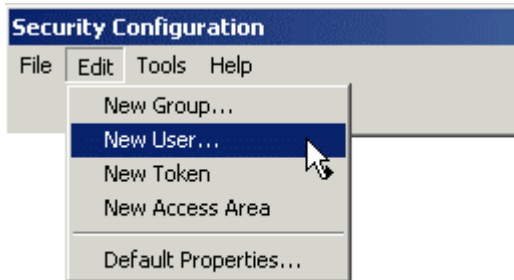


Entering of the name, and display of the Group Properties dialog is very similar in operation to creating a new User, except that the List pane displays configured Groups.

3.1.2.2 Creating a New User

A new User may be created by any of the following methods:

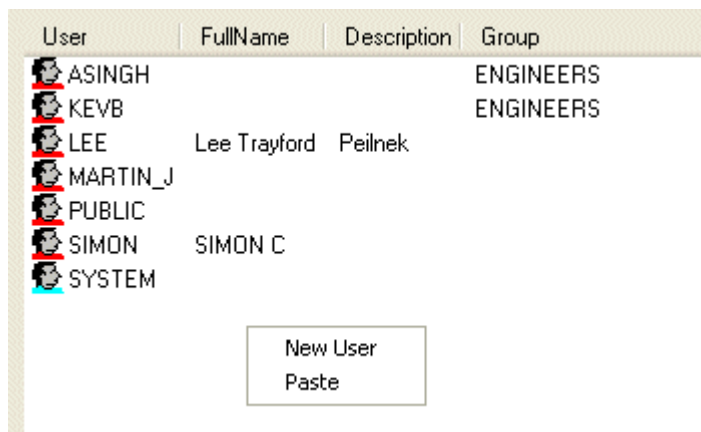
- Using the **Edit-New User** menu item from the Security Configuration Tool menu bar.



- Using the **New User** context menu from the Users icon in the Tree Pane.



- New User** floating context menu from the List Pane with Users icon selected in Tree Pane.



Once the New User menu item has been selected, the List Pane will automatically display all the currently configured Users. A new entry with a blank name field is inserted at the top of the list.

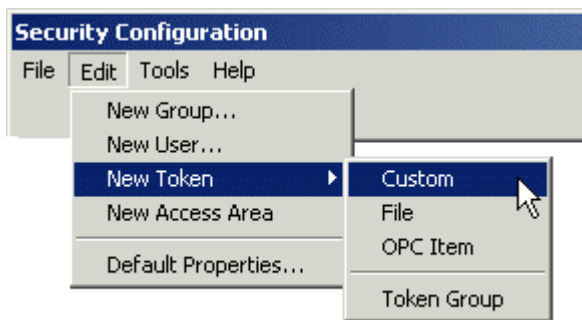
A valid name should be entered, and the Enter key selected. This will invoke the User Properties dialog, which will allow more detailed editing of the User.

Note: Once the new User name has been entered, it is not possible to edit it at a later time.

3.1.2.3 Creating Custom, File and OPC Item Tokens

Custom Tokens, File Tokens and OPC Item Tokens are created in the same way:

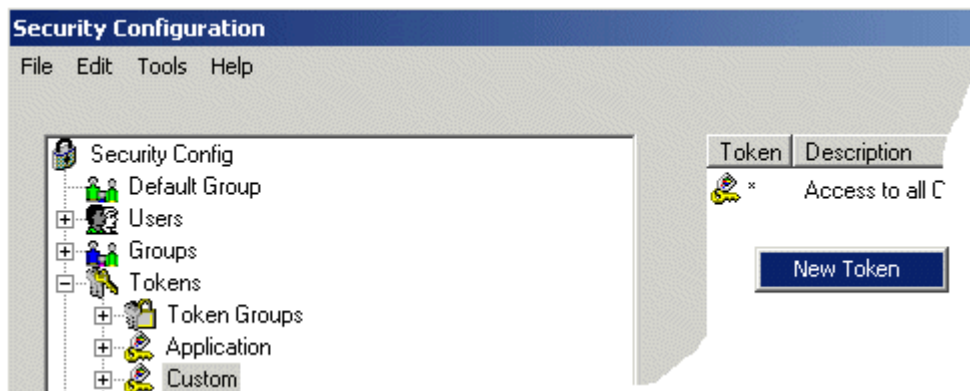
- Select the **Edit>New Token** menu item from the Security Tool menu bar. Then select the desired option from the list (e.g. Custom, File or OPE Item).



- Select **New Token** menu item from the expanded Tree Pane.



- Select the floating **New Token** context menu from the List Pane when the Custom, File or OPC Item node is selected in the Tree Pane.

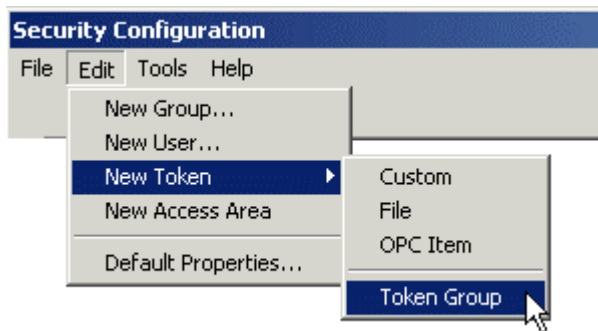


Once this menu item has been selected, editing may proceed in a similar way as described in the section Adding a New Token Group. The name should be unique among other Custom Tokens, and is case-sensitive. Once the name has successfully been entered, the Custom Token Properties dialog will be displayed. **Note:** it is not possible to edit the Token name once it has been entered.

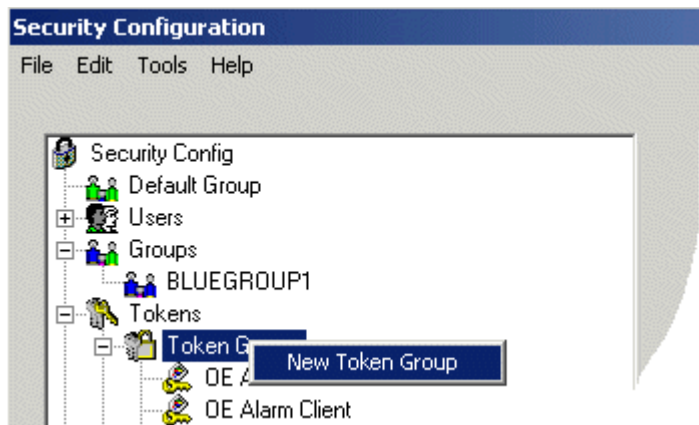
3.1.2.4 Creating New Token Groups

A new Token Group may be created by any of the following methods:

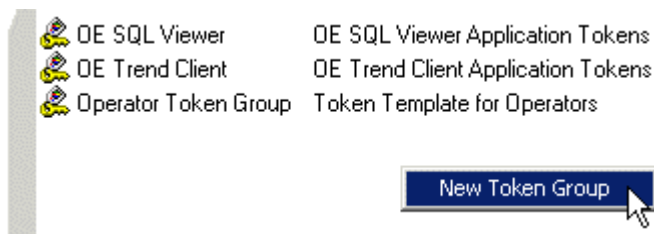
- Selecting the **Edit>New Token>New Token Group** menu item from the Security Tool menu bar.



- Selecting the **New Token Group** menu item from the expanded Tree Pane:



- Selecting the floating **New Token Group** context menu from the List Pane whilst the Token Group icon is selected in the Tree Pane:



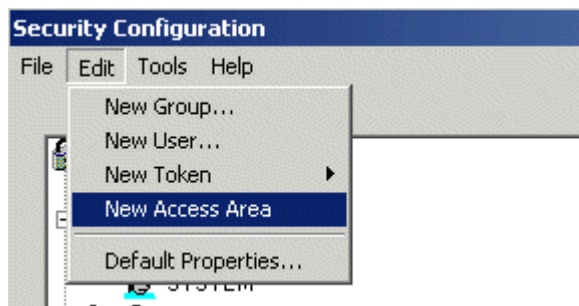
Once this menu item has been selected, the List Pane will automatically display all the currently configured Token Groups. A new entry with a blank name field is inserted at the top of the list. A valid, unique name should be entered, and the Enter key selected. This will invoke the Token Group Properties dialog, which will allow more detailed editing.

Note: once the new name has been entered, it is not possible to edit the name at a later time.

3.1.2.5 Creating New Access Areas

A new Access Area may be entered either by

- Selecting the **Edit>New Access Area** menu option from the Security Configuration Tool menu bar



- By selecting the **New AccessArea** context menu option from the Access Areas node.



Selecting either of these options will result in prompting for an Access Area name in the right hand list and, upon successfully entering a unique name, the Access Area Properties dialog will be displayed.

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

3.1.3 Tools Menu

This menu provides access to the Options dialog which enables the User to configure how certain functions within the Security Configuration tool behave.



3.1.4 Help Menu

Selection of the **Help** option displays this help file. Selection of the **About...** option displays information about the OpenEnterprise version, build number and contact details.

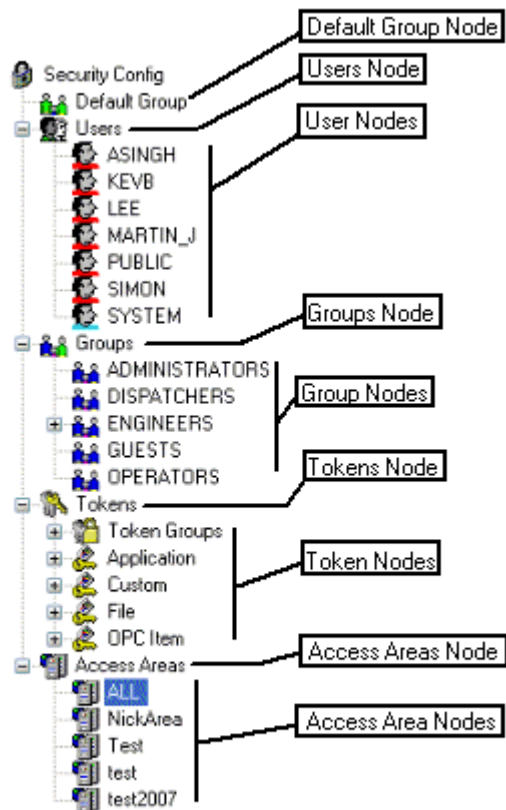
3.2 The Tree Pane

3.2.1 The Tree Pane

The Tree Pane provides an overview of the current configuration by means of a tree structure.

The tree consists of a number of object type nodes (Users, Groups, Tokens and Access Areas), which display configured Security objects of that type underneath.

Most object type nodes have a context menu, activated with a right mouse click, which enables a new object of that type to be created under the node.



All configured object elements in the Tree Pane have a context menu, providing access to the Property Pages for that object, as well as other options, depending on the type of object selected.

3.2.2 Default Group Node

The Default Group node has one context menu option. This opens the property pages 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.



3.2.3 Users Node

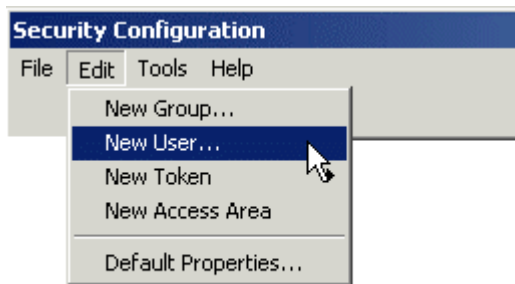
The users node has a context menu that provides two options.



3.2.3.1 Creating a New User

A new User may be created by any of the following methods:

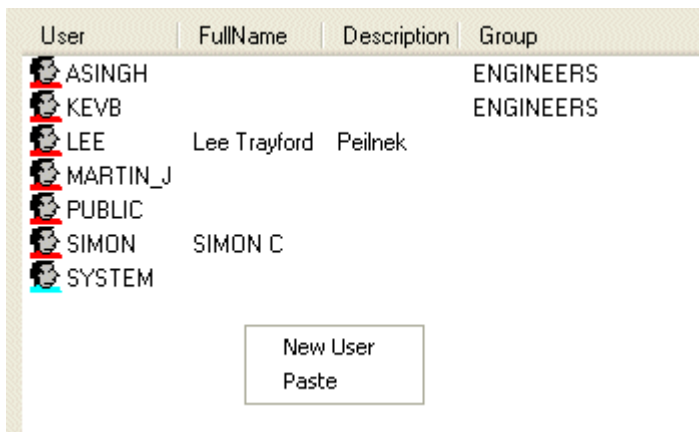
- Using the **Edit-New User** menu item from the Security Configuration Tool menu bar.



- Using the **New User** context menu from the Users icon in the Tree Pane.



- New User** floating context menu from the List Pane with Users icon selected in Tree Pane.



Once the New User menu item has been selected, the List Pane will automatically display all the currently configured Users. A new entry with a blank name field is inserted at the top of the list.

A valid name should be entered, and the Enter key selected. This will invoke the User Properties dialog, which will allow more detailed editing of the User.

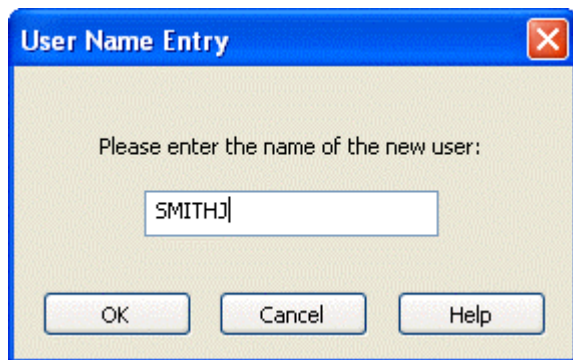
Note: Once the new User name has been entered, it is not possible to edit it at a later time.

3.2.3.2 Paste User

The Paste option, when selected from the Users icon begins the process of pasting a previously copied user's security configuration details to a new user. If no user has been copied, the Paste option is disabled.





Before the new user is created, the User Name Entry dialog appears, prompting for a name for the new user. The name must be unique. When the [OK] button is selected, the new user is added, complete with all of the security configuration of the copied user.



3.2.4 User Nodes

Individual User nodes indicate the administration level of the User. They may be either:

Red  Standard, non-administrative User

Blue  Administrative User

Only Administrative Users are able to configure security within Open Enterprise. Only an Administrative User may grant Users administrative rights. The SYSTEM User is an Administrative User by default.

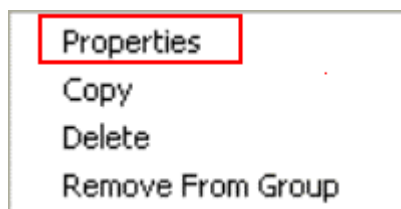
3.2.4.1 Context Menu

A context menu is available when the user right clicks on any user in the list.



3.2.4.2 Properties

Opens the Property pages for the selected user. See the User Property Pages topic for more information.

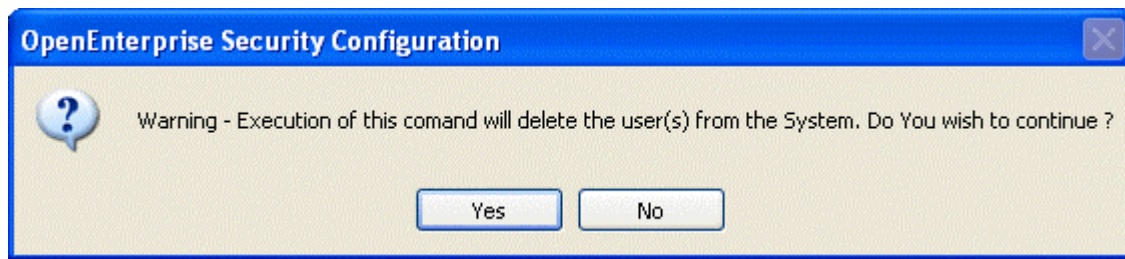


3.2.4.3 Copy

Copies the selected user's configuration details ready for pasting the same configuration to a new user.

3.2.4.4 Delete

Deletes the selected user. A warning message will appear before deleting the user.

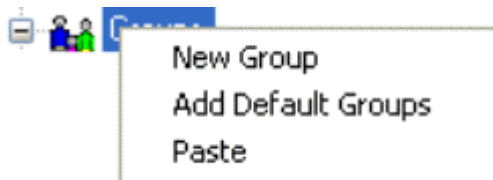


3.2.4.5 Remove From Group

Removes the selected user from the User Group that it is under, but does not delete the user.

3.2.5 Groups Node

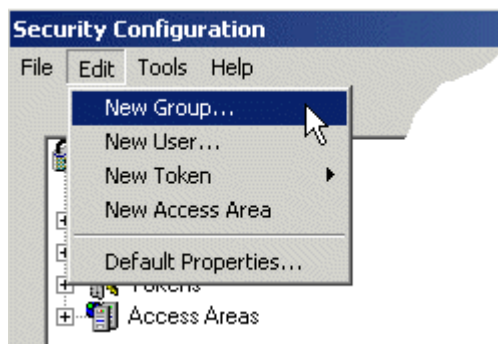
The Groups node has a context menu that provides three options.



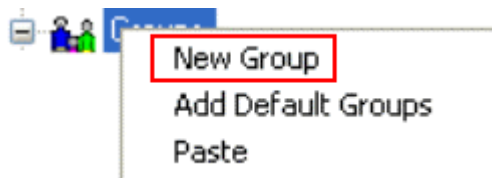
3.2.5.1 Creating New User Groups

A new Group may be created by any of the following methods:

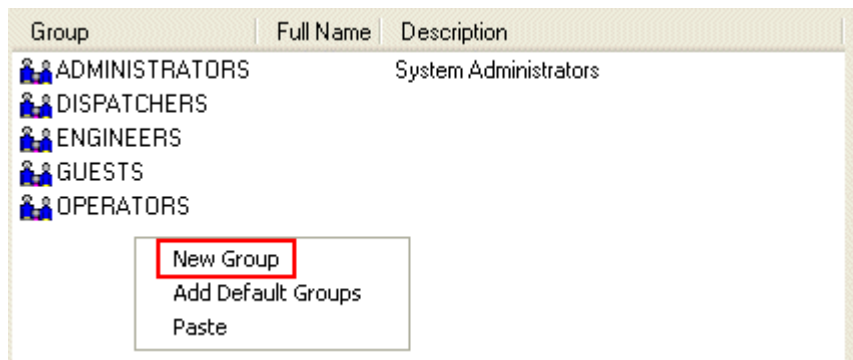
- Using the **Edit-New Group** menu item from the Security Configuration Tool menu bar.



- Using the **New Group** menu item from the Tree Pane:



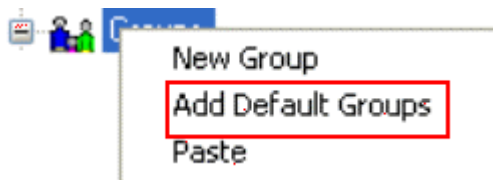
- Using the floating **New Group** context menu from the List Pane when the **Groups** node is selected in the Tree Pane.



Entering of 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.

3.2.5.2 Adding the Default Groups

If they were not created when the OpenEnterprise database was built, the Default OpenEnterprise Groups may be added from the Security Configuration tool by selecting the *Add Default Groups* option from the context menu off the main Groups icon.



3.2.5.3 Paste Group


The Paste option, when selected from a the Groups icon begins the process of pasting a previously copied user group's security configuration details to a new user group. If no user group has been copied, the Paste option is disabled.

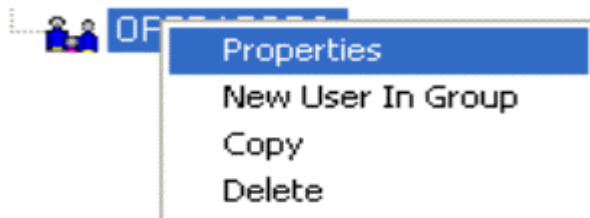


Before the new user group is created, the Group Name Entry dialog appears, prompting for a name for the new user group. The name must be unique. When the [OK] button is selected, the new user group is added, complete with all of the security configuration of the copied user group.



3.2.6 Group Nodes

Groups created by the Administrative User have a Blue icon . All Administrative User created Groups will appear with a blue icon. Each Group node has a context menu that provides four options.



Expansion of the Groups branch displays the configured individual Group names and icons. Selection of this node results in the configured Groups being listed in the List Pane, together with any associated Full Name and description.

3.2.6.1 User Group Properties

This option opens the selected User Group's property pages for editing. See the User Group Properties Dialog topic for further help on this dialog.

3.2.6.2 Add New User to Group

This option enables a new user to be created and added to the selected User Group. See the Creating a New User topic for further help on this process.

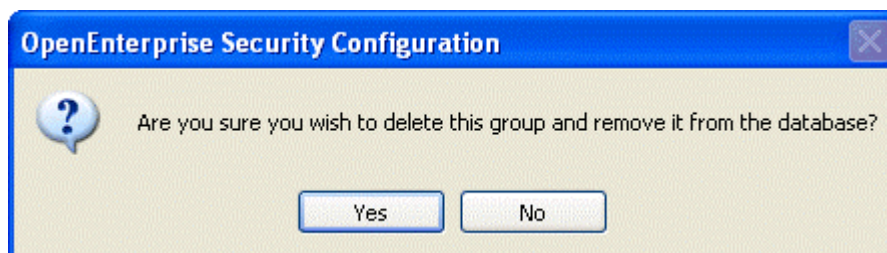
3.2.6.3 Copy Group

This option enables a User Group's configuration to be copied and then pasted from the Groups Node.

Note: the users in the copied User Group are not copied. It is the security configuration only that is copied.

3.2.6.4 Delete Group

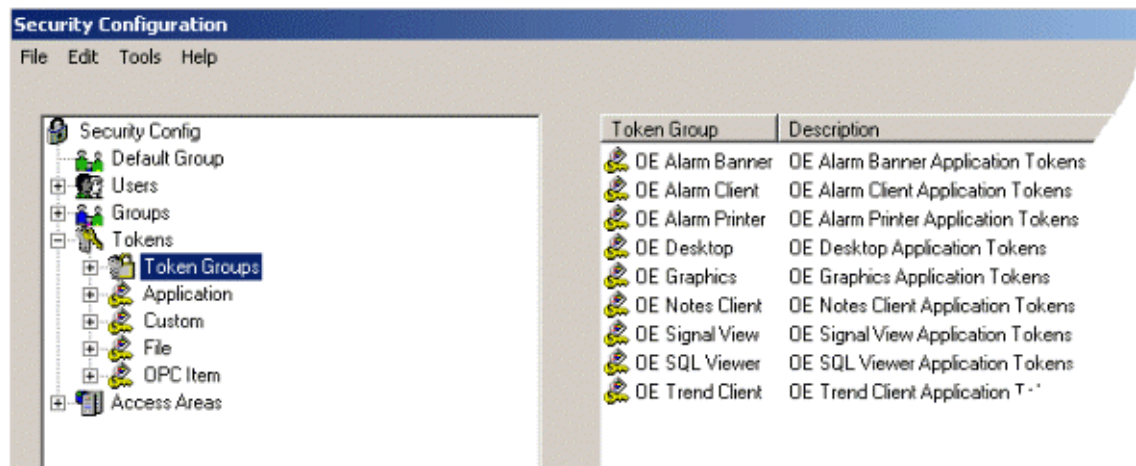
Deletes the selected User Group. A warning will appear before the actual deletion.



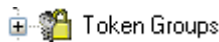
3.2.7 Tokens Node



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.



3.2.7.1 Token Groups Node



The Token Groups node has a context menu which enables the user to create new Token Groups. See the Creating New Token Groups topic for more information.

When the Token Groups Node is expanded, it exposes the Token Group Type nodes. For more information on Token Group Nodes see the Token Group Nodes topic.

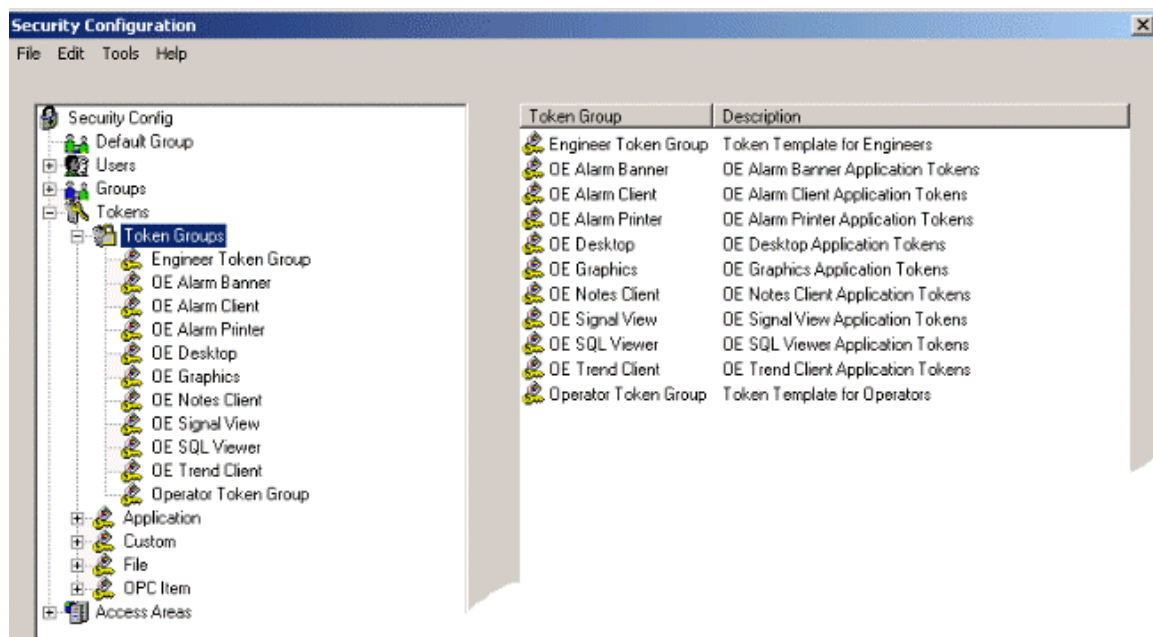
Token Groups are collections of Tokens, which may form a Template of Tokens to be associated with a User or User Group. User generated Token Groups may consist of a combination of any of the four types of tokens.

There are also several special Application Token Groups that are maintained independently of the Administrative User and are grouped by their Component name. They are the Alarm Banner, Alarm Client, Alarm Printer, OEDesktop, Graphics, Notes Client, Signal View, SQL Viewer and Trend View Token Groups. These Token Groups cannot be edited.

3.2.7.1.1 Token Group Nodes

Expanding this Node will display all the configured Token Groups. Selecting this node results in the Token Groups being listed in the List Pane, together with any Description.

By associating a Token Group with a User or User Group, all Tokens configured in that Token Group may be included or excluded from the User's or Group's security profile. Token Groups can be used as templates to assign selected Tokens to Users or User Groups.



3.2.7.1.1.1 User Configured Token Groups

Token Groups may be configured by an Administrator User. The Administrator User can add any of the default Application Tokens to this Token Group, as well as configure Custom, File and OPC Tokens for it. The Token Group may then be used as a Token template for User Groups, such as Operators or Engineers.

3.2.7.2 Application Tokens Node



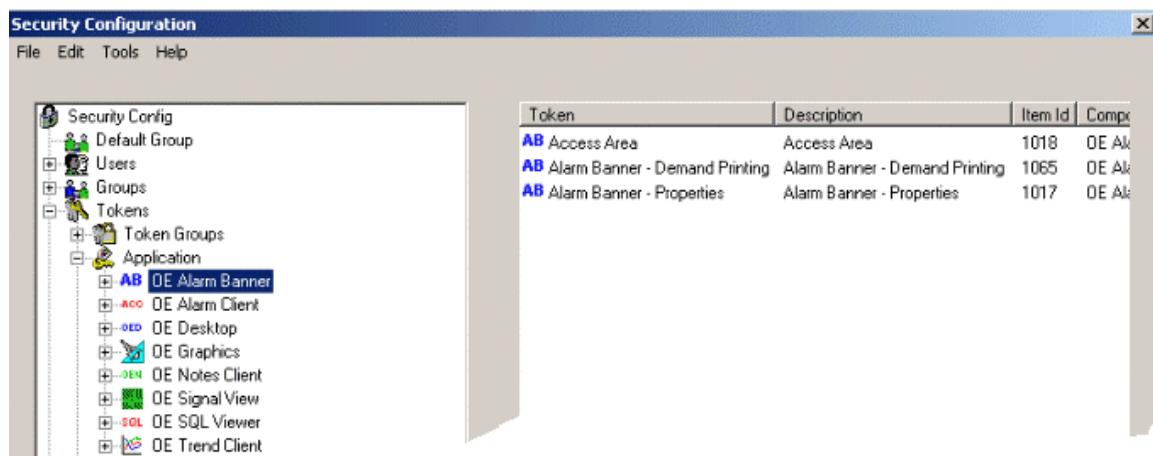
The Application Tokens node has no context menu because Application Tokens cannot be created, modified or deleted by the user. They are created at installation time.

Application Tokens are used 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.

3.2.7.2.1 Application Token Component Types

Expanding any of the application nodes by clicking the plus sign to the left of it will result in the individual associated application tokens being displayed in the tree. Selecting an application node itself will result in its associated tokens being displayed in the list pane on the right, together with its Description, Item Number and Component Name. This is illustrated below for an OpenEnterprise Alarm Banner Type.



3.2.7.2.2 Drag-dropping Application Tokens

Individually selected tokens may be dragged from the List Pane and dropped onto a User or Group in the Tree Pane to incorporate them onto an Include or Exclude list, depending on the Drag Option setting (See Section Drag Options for more detail). They may also be dragged onto Token Groups to add them to the Token Group.

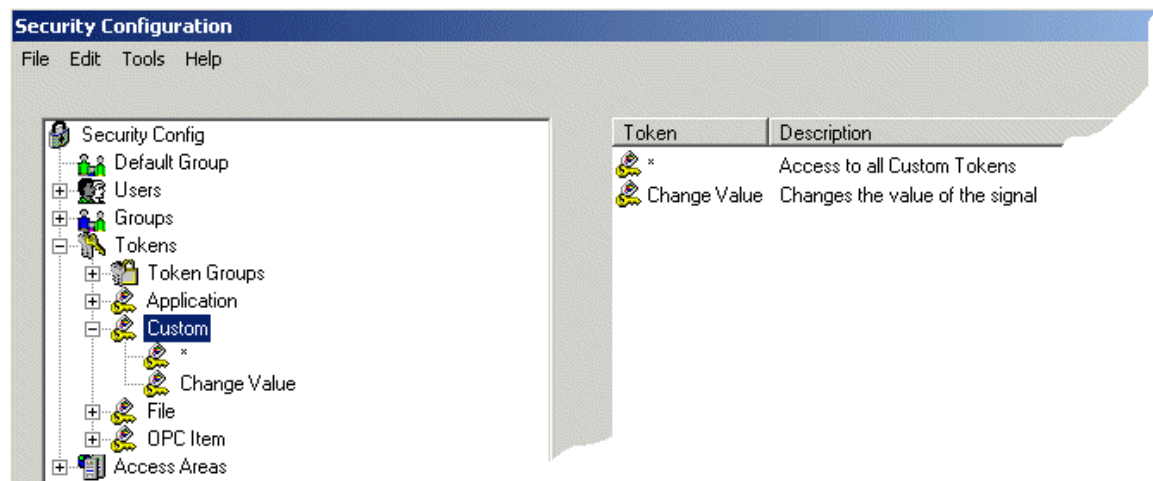
3.2.7.3 Custom Tokens



The Custom node has its own context menu that enables the user to create new Custom Tokens. See the Creating Simple String Type Tokens topic for more information.

When the Custom node is expanded, all configured Custom Tokens are displayed in the branch.

When it is selected the Tokens are displayed in the List Pane together with any Descriptions. Custom Tokens are strings used mainly to grant or deny access to Custom Menus, created with the OEMenu Editor.



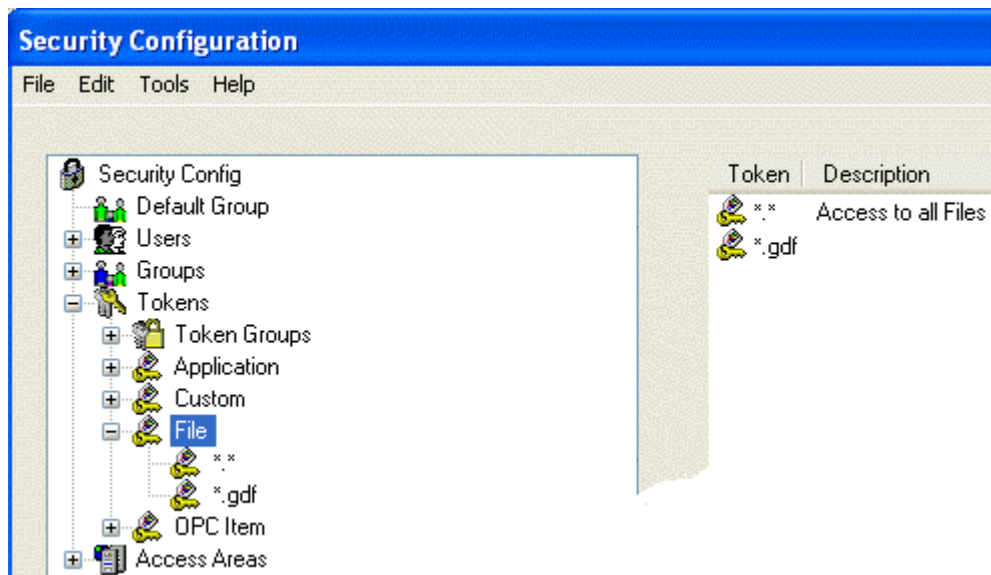
Selecting an individual Custom Token in the tree will simply list the individual token in the List Pane. Tokens may be dragged and dropped from List Pane onto Tree Nodes such as User, Group and Token Group targets in the same fashion as Application Tokens.

3.2.7.4 File Tokens



The File node has its own context menu that enables the user to create new File Tokens. File Tokens are strings used to grant or deny access to certain files or file types. See the Creating Simple String Type Tokens topic for more information.

When the Custom node is expanded, all configured File Tokens are displayed. When it is selected the Tokens are displayed in the List Pane together with any Descriptions.



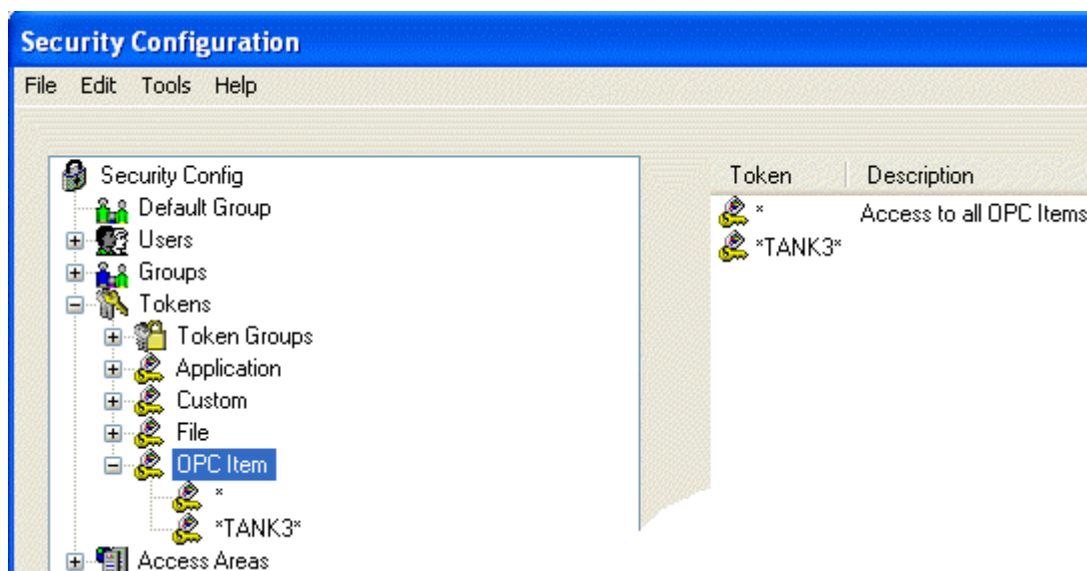
3.2.7.5 OPC Item Tokens



The OPCItem node has its own context menu that enables the user to create new File Tokens. See the Creating Simple String Type Tokens topic for more information on creating new OPC Item Tokens.

OPC Item Tokens are strings, which grant or deny write access to OPC tags. See the OPC Item Token Types topic for more information about how OPC Item Tokens work.

When the OPC Item node is expanded, all configured OPC Item Tokens are displayed. When it is selected the Tokens are displayed in the List Pane together with any Descriptions.



3.2.8 Access Areas Node

This is the Root Node for all Access Area Nodes. Expanding this branch will list the configured Access Areas. Selecting this node leads to the Access Areas and their associated Description being listed in the List Pane.

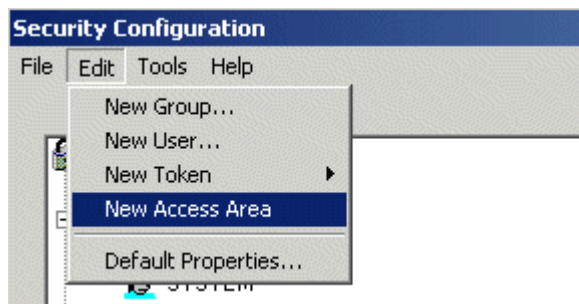
The Access Areas Icon has one context menu option. This enables a new Access Area token to be created.



3.2.8.1 Creating New Access Areas

A new Access Area may be entered either by

- Selecting the **Edit>New Access Area** menu option from the Security Configuration Tool menu bar



- By selecting the **New AccessArea** context menu option from the Access Areas node.



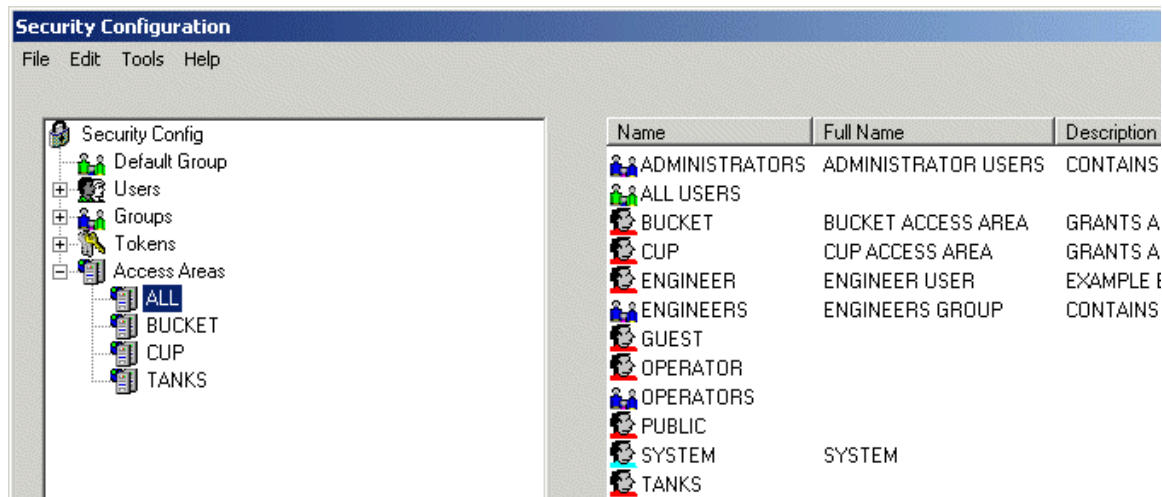
Selecting either of these options will result in prompting for an Access Area name in the right hand list and, upon successfully entering a unique name, the Access Area Properties dialog will be displayed.

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

3.2.9 Access Area Nodes

Selecting an individual Access Area node in the left hand pane will result in the Users and groups currently associated with the Access Area being displayed in the right hand list pane.

A right click on the node will bring up a 'Properties' context menu, which when selected will open the Access Area Properties Dialog.



3.3 The List Pane

Provides more detail on the particular object that has been selected in the Tree Pane. If an object type node is selected (i.e. Users), all of the configured objects that belong to that type are displayed in the List Pane.

Name	Full Name	Description
ADMINISTRATORS		System Administrators
ALL USERS		
ASINGH		
DISPATCHERS		
ENGINEERS		
GUESTS		
KEVB		
LEE	Lee Trayford	Peilnek
MARTIN_J		
OPERATORS		
PUBLIC		
SIMON	SIMON C	
SYSTEM		

The column headings and contents will 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. Re-ordering may be achieved by clicking on an individual column header. Clicking again on an already clicked column header will result in reverse ordering using that header, i.e. if a column was sorted in ascending order, it will be sorted in descending order, and vice versa. Should the data exceed the capacity of the window then vertical and/or horizontal scroll bars will appear to allow for scrolling, 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.

4 Security Config Tool Tasks

The Security Configuration tool allows Administrative Users to create, modify and delete security related objects such as Users, Groups, Tokens and Access Areas. The tool also allows Administrative Users to grant or deny Tokens and Access Areas to Users and Groups, providing comprehensive and integrated security configuration.

1. Create New Security Objects

Users and Groups

- Creating a new User
- Creating a new User Group
- Adding Default Groups

Tokens

- Creating new Token Group Tokens
- Creating new Custom Tokens
- Creating new File Tokens
- Creating new OPC Item Tokens
- Note on Application Tokens

Access Areas

- Creating new Access Areas

2. Edit Security Items

Users and Groups

- Modifying User account settings
- Modifying User Group account settings
- Modifying the Default User account settings
- Adding a New User to a Group
- Removing All Users From a Group

Tokens

- Modifying Token Groups
- Modifying Custom Tokens
- Modifying File Tokens
- Modifying OPC Item Tokens
- Linking Tokens with a Token Group
- Linking Tokens or Token Groups with a User or Group

- Viewing and Breaking Token Links

Access Areas

- Modifying Access Areas

3. Delete Security Items

- Deleting Users, Groups, Tokens and Access Areas.

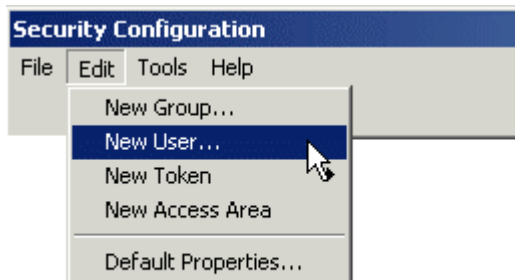
4.1 Creating Security Objects

4.1.1 New Users and Groups

4.1.1.1 Creating a New User

A new User may be created by any of the following methods:

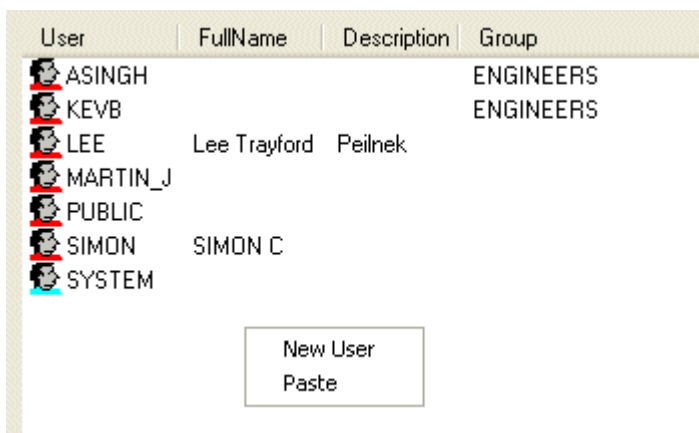
- Using the **Edit-New User** menu item from the Security Configuration Tool menu bar.



- Using the **New User** context menu from the Users icon in the Tree Pane.



- **New User** floating context menu from the List Pane with Users icon selected in Tree Pane.



Once the New User menu item has been selected, the List Pane will automatically display all the currently configured Users. A new entry with a blank name field is inserted at the top of the list.

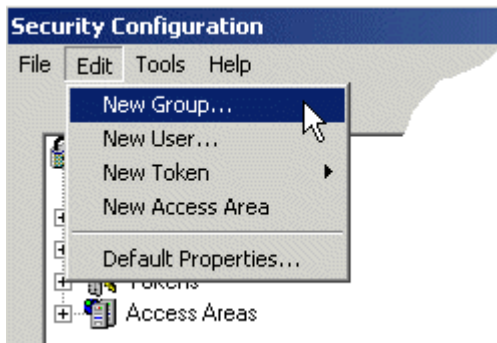
A valid name should be entered, and the Enter key selected. This will invoke the User Properties dialog, which will allow more detailed editing of the User.

Note: Once the new User name has been entered, it is not possible to edit it at a later time.

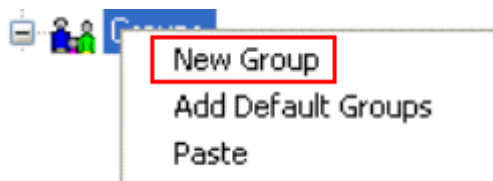
4.1.1.2 Creating New User Groups

A new Group may be created by any of the following methods:

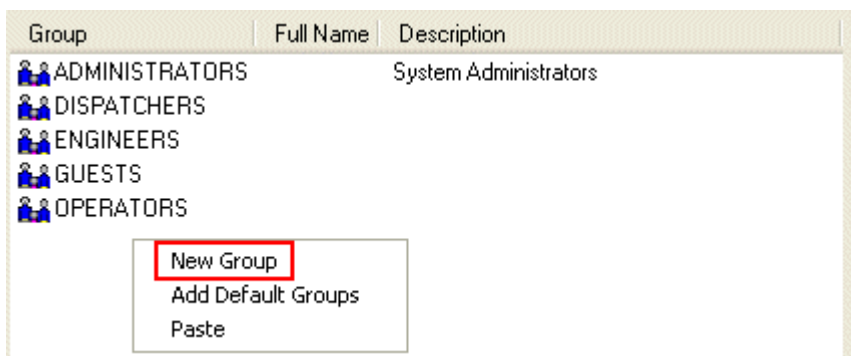
- Using the **Edit-New Group** menu item from the Security Configuration Tool menu bar.



- Using the **New Group** menu item from the Tree Pane:



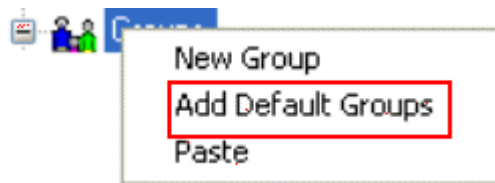
- Using the floating **New Group** context menu from the List Pane when the **Groups** node is selected in the Tree Pane.



Entering of 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.

4.1.1.3 Adding the Default Groups

If they were not created when the OpenEnterprise database was built, the Default OpenEnterprise Groups may be added from the Security Configuration tool by selecting the *Add Default Groups* option from the context menu off the main Groups icon.

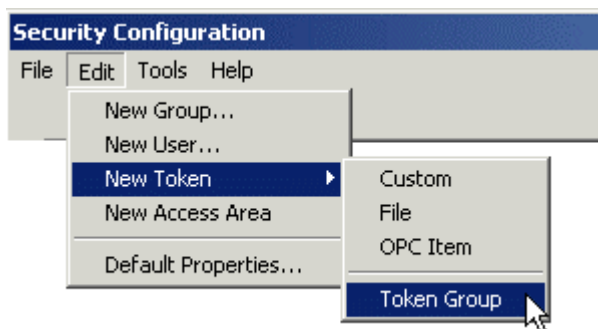


4.1.2 New Tokens

4.1.2.1 Creating New Token Groups

A new Token Group may be created by any of the following methods:

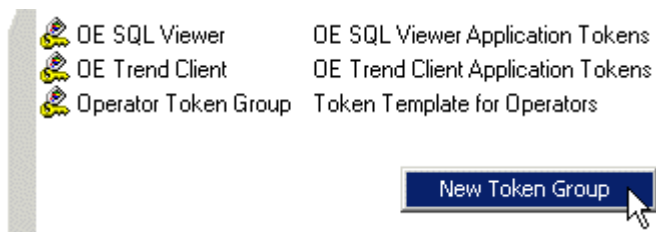
- Selecting the **Edit>New Token>New Token Group** menu item from the Security Tool menu bar.



- Selecting the **New Token Group** menu item from the expanded Tree Pane:



- Selecting the floating **New Token Group** context menu from the List Pane whilst the Token Group icon is selected in the Tree Pane:



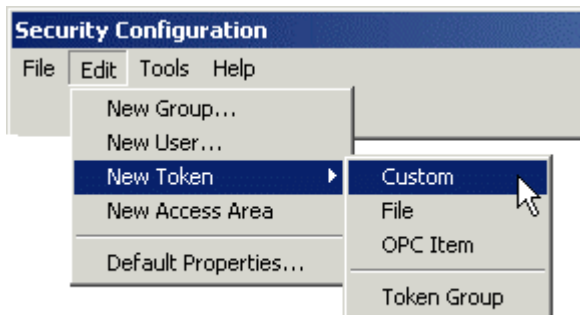
Once this menu item has been selected, the List Pane will automatically display all the currently configured Token Groups. A new entry with a blank name field is inserted at the top of the list. A valid, unique name should be entered, and the Enter key selected. This will invoke the Token Group Properties dialog, which will allow more detailed editing.

Note: once the new name has been entered, it is not possible to edit the name at a later time.

4.1.2.2 Creating Custom, File and OPC Item Tokens

Custom Tokens, File Tokens and OPC Item Tokens are created in the same way:

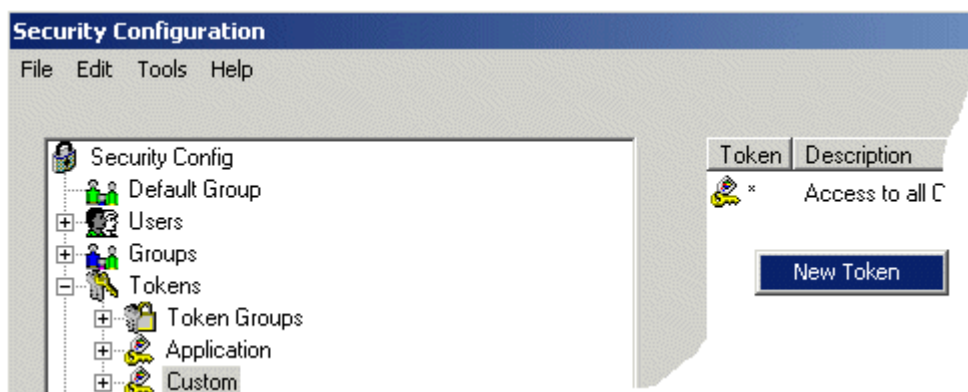
- Select the **Edit>New Token** menu item from the Security Tool menu bar. Then select the desired option from the list (e.g. Custom, File or OPE Item).



- Select **New Token** menu item from the expanded Tree Pane.



- Select the floating **New Token** context menu from the List Pane when the Custom, File or OPC Item node is selected in the Tree Pane.



Once this menu item has been selected, editing may proceed in a similar way as described in the section Adding a New Token Group. The name should be unique among other Custom Tokens, and is case-sensitive. Once the name has successfully been entered, the Custom Token Properties dialog will be displayed. **Note:** it is not possible to edit the Token name once it has been entered.

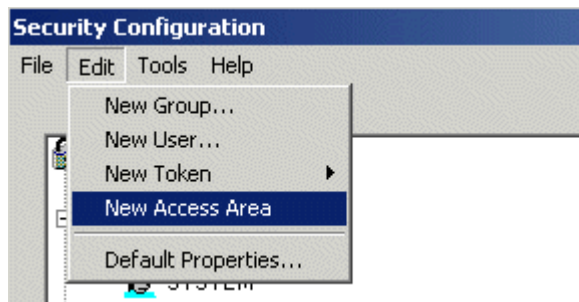
4.1.2.3 On Creating New Application Tokens

It is not possible to create a new Application Token by means of this tool. For an explanation of all Application Tokens see All Application Tokens.

4.1.3 Creating New Access Areas

A new Access Area may be entered either by

- Selecting the **Edit>New Access Area** menu option from the Security Configuration Tool menu bar



- By selecting the **New AccessArea** context menu option from the Access Areas node.



Selecting either of these options will result in prompting for an Access Area name in the right hand list and, upon successfully entering a unique name, the Access Area Properties dialog will be displayed.

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

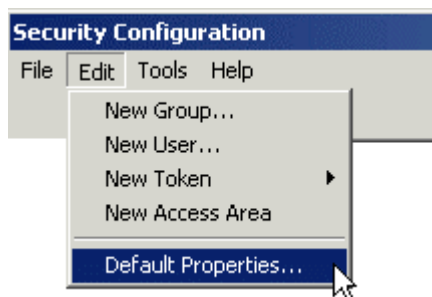
4.2 Modifying Security Objects

4.2.1 Modifying Users and Groups

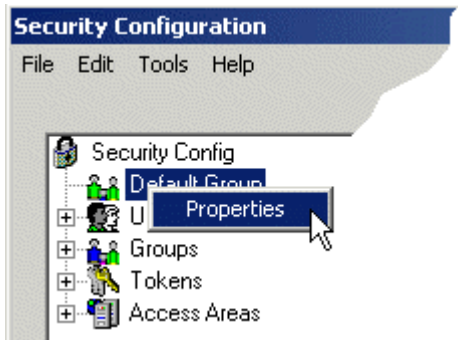
4.2.1.1 Modifying Default Group Settings

There are two ways to modify Security settings for the Default Group.

- From the **Edit>Default Properties** menu item.



- From the **Properties** context menu item on the Default Group node, which may be accessed from the Tree Pane



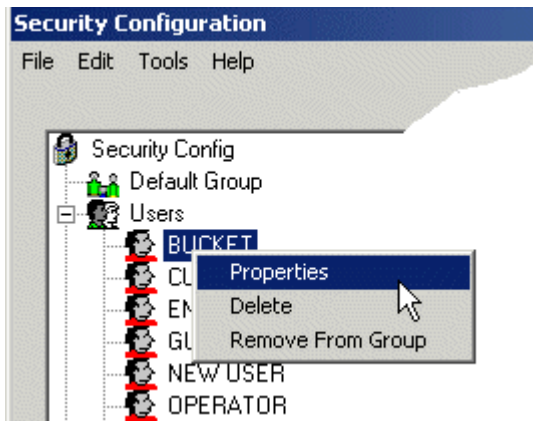
When either of the above menu options are chosen the Default Properties dialog is displayed.

Note: any tokens 'Included' and not Excluded in the Default Group may not subsequently be 'Excluded' from any other group or User. It is best, therefore, to 'Include' only the bare minimum of tokens necessary within the Default Group.

4.2.1.2 Modifying User Account Settings

There are two ways to modify Security settings for a User.

- Right click on a User and select the Properties menu item from the context menu.



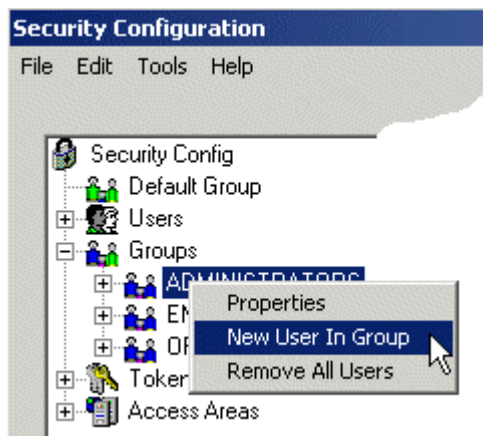
- Double click on a User

This will reveal the User Properties Dialog, from which security settings can be modified for the User.

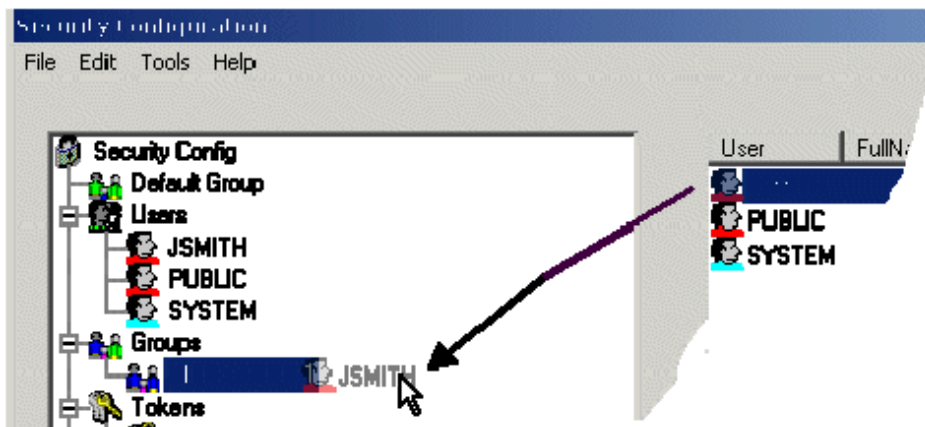
4.2.1.3 Adding a New User to a Group

There are two ways to add a new User to a User Group.

- Select the Group to which the new User will be added, right click and select 'New User In Group' from the context menu, as shown in the example below.

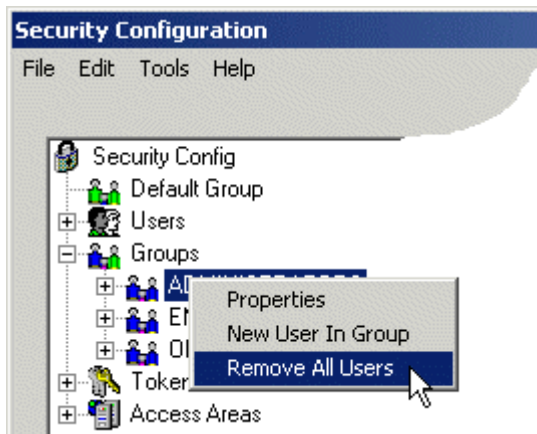


- Drag and Drop the User from the List Pane to a User Group in the Tree Pane



4.2.1.4 Removing All Users from a Group

Select the Group from which all Users will be deleted, right click and select 'Remove All Users From Group' from the context menu, as shown in the example below.

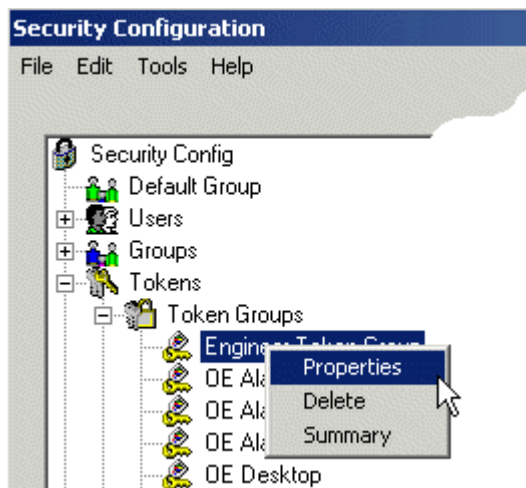


4.2.2 Modifying Tokens

4.2.2.1 Modifying Token Groups

There are two ways to modify Token Groups.

- Right click on a Token Group and select the Properties menu item from the context menu.



- Double click on a Token Group

This will reveal the Token Group Properties Dialog, from which security settings can be modified for the Token Group.

Note: Settings cannot be changed for the Application Token Groups. They are managed automatically by OpenEnterprise.

4.2.2.2 Linking Tokens with a Token Group

There are two ways to Link other Tokens with a Token Group.

1. Use the Token Group's Properties Dialog.
2. Select a Token from the List Pane and drag-drop it onto the Token Group in the Tree Pane.

4.2.2.3 Linking Tokens or Token Groups with Users or Groups

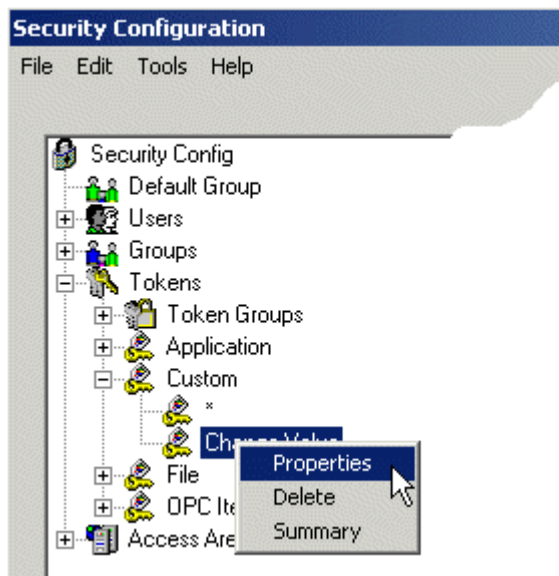
There are two ways to Link Tokens or Token Groups with Users or Groups

1. Use the User or Group Properties Dialog.
2. Select a Token from the List Pane and drag-drop it onto the User or Group in the Tree Pane.

4.2.2.4 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 the Properties menu item from the context menu.



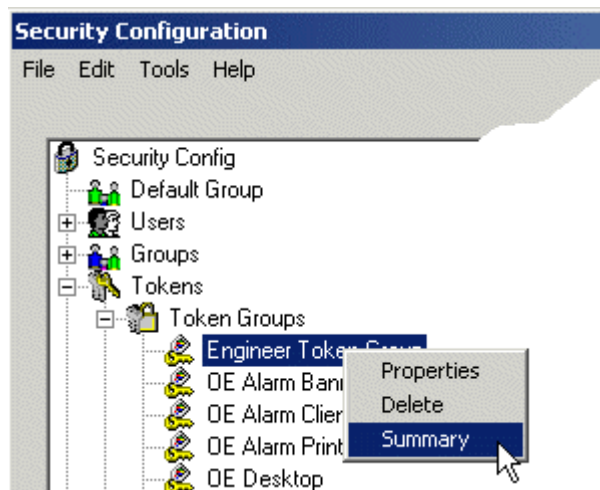
- Double click on any Custom, File or OPC Item Token

This will reveal the Token Properties Dialog, from which the Description can be modified for the selected Token.

Note: Only the description or Access Area can be modified for these types of Tokens.

4.2.2.5 Viewing and Breaking Token Links

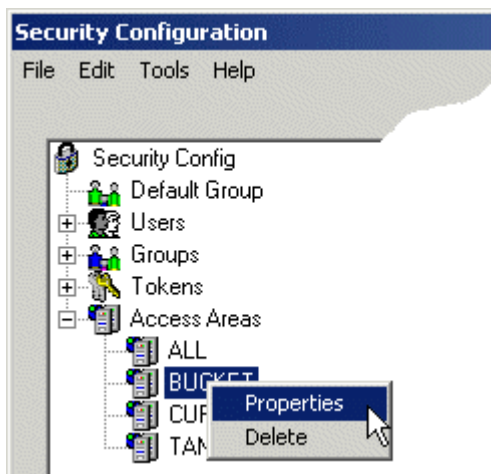
When a Token Group is placed into the Include or Exclude Token list for a User or Group, it is said to have a Link to that User or Group. These Links may be viewed and removed by accessing the Token Summary dialog. This dialog may be invoked by selecting the Summary option on a Token context menu.



4.2.3 Modifying Access Areas

There are two ways to modify Access Areas.

- Right click on an Access Area and select the **Properties** menu item from the context menu.



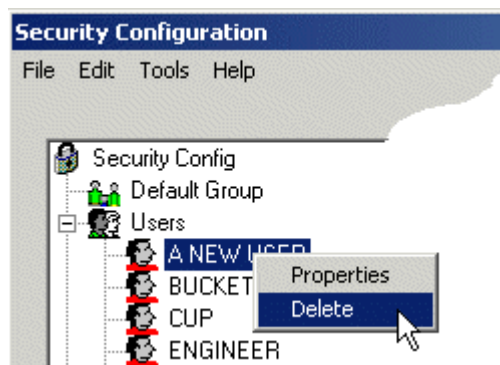
- Double click on any Access Area

This will reveal the Access Area Properties Dialog, from which the Description can be modified for the selected Access Area.

Note: Only the description can be modified.

4.2.4 Deleting Security Objects

To delete a User, Group, Token or Access Area, select the object, right click and then select the 'Delete' option from the context menu, as shown in the example below.



Note: The following objects cannot be deleted:-

1. The Default Administrator (SYSTEM)
2. Any Application Token Group
3. Any Application Token
4. Any Token associated with a User, Group or Token Group
5. Any Access Area associated with a User or Group

5 Security Configuration Dialogs

The dialogs available from the Security Configuration tool enable the Administrative User to configure every aspect of OpenEnterprise Workstation Security. Each dialog is accessed by means of a Menu item, or by double clicking or right clicking with the mouse on the appropriate object in either pane of the Security Configuration tool interface.

1. The User dialog
2. The User Group dialog
3. The Token Group dialog
4. The Token dialog
5. The Token Summary dialog
6. The SQL Import-Export File dialog
7. The File Import dialog
8. The Options dialog

5.1 User Property Pages

User properties are configured with the user property pages, which can be accessed from the context menu on any user selected from the tree pane or the list pane. There are nine user property pages.

1. User Properties page
2. User Account page
3. User Summary page
4. User Access Areas page
5. User Application Token page
6. User Custom Token page
7. User File Token page
8. User OPC Item page
9. User Token Group page

5.1.1 The User Properties Page

The Properties tab enables Administrator Users to configure basic security settings for each OpenEnterprise User. The Properties tab for a single User differs from the Default Group and User created Group pages, in that the Password, Verify Password and Parent Group fields are disabled, and there is no Summary tab for Groups.

User Properties - SEC_DEFAULT_USER1

Custom Token | File Token | OPC Item Token | Token Group

Properties | Account | Summary | Access Areas | Application Token

User Settings

User Name: SEC_DEFAULT_USER1

Full Name: Sec Default User

Description: Security Test Spec User

Password:

Verify Password:

Access Area: ALL

Administration

☐ Change Password At Next Logon

☐ User Cannot Change Password

☐ System Administrator

☐ Account Disabled

☐ Account LockOut

Grantor:

Group

Parent Group: SEC_DEFAULT_GROUP

Load .OED File

☐ Login

☐ Logout

OK Cancel Apply Help

5.1.1.1 User Name

This is a read only field: the name is not editable once the User has been created. The Security Configuration tool displays all User names in upper case.

5.1.1.2 Full Name

This is an optional character field. It may be used to specify the full name of the User if it was abbreviated in the Name field.

5.1.1.3 Description

This is an optional character field, which may be used to provide further information concerning the User.

5.1.1.4 Password

This field allows the password to be changed. It is greyed out when the logged in User does not have sufficient privileges to change this field. For security reasons this field is initially shown as 10 asterix symbols regardless of the password length.

Note: this field is disabled for Groups and the Default Group.

5.1.1.5 Verify Password

For verification purposes this field should contain a repeat of the User's password. This field is likewise shown initially shown as 10 asterix symbols regardless of the password length.

Note: this field is disabled for Groups and the Default Group.

5.1.1.6 Access Area

This field is defaulted to ALL when creating a new User. When a User's security is configured, the access areas available to the User will be those assigned to the Security Administrator. A suitable access area may be selected from the list.

5.1.1.7 Change Password at Next Logon

This allows a Security Administrator to force the User to change their password the next time they logon to Open Enterprise.

This field is mutually exclusive to the 'User Cannot Change Password' field.

5.1.1.8 User Cannot Change Password

There may be cases where a Security Administrator wishes to prevent a User from changing their password. Setting the User Cannot Change Password tick box for the User's account allows this functionality to be enforced.

This field is mutually exclusive to the 'User change password at next logon' field.

5.1.1.9 System Administrator

When checked, it enables a created User to be given the status of an Administrative User. Administrative rights can only be revoked by the Administrative User who granted those rights. Therefore, when viewing User Property pages, this field will be disabled if the currently logged in Administrative User did not originally grant Administrative rights to the Administrative User being reviewed.

Note: this field is disabled for Groups and the Default Group.

5.1.1.10 Account Disabled

Setting of this flag will disable a User's account. This prevents the User from logging on and from changing their password.

Only a Security Administrator can enable a disabled User account.

5.1.1.11 Account Lockout

This flag indicates a User's account is locked out. This prevents the User from logging on and from changing their password.

Although an account can be locked out manually, the most common use of account lockout will be to protect the OpenEnterprise SCADA System. For instance, consecutive failures to log on as a User due to an incorrect password can cause the User's account to be locked out.

The unlocking of an account may be achieved by either of the following:

- Manual unlocking by a Security Administrator using the configuration tool
- Time based, whereby the lock is automatically released after a pre-configured period of time

5.1.1.12 Grantor

The dialog box below details the setting of the Grantor field. Here the current Security Configuration Tool User is logged on as SYSTEM. The SYSTEM User has assigned administrative rights to a User called NEW User as indicated in the Grantor field.

Note: this field is disabled for Groups and the Default Group.

5.1.1.13 Configure Group Privileges

Opens up the Security Group Privileges Editor for configuring Database Privileges for the User Group. This button is only available on the User Group Properties Page. The User Properties Page has the Parent Group selection list in place of this button, because Database Privileges are only configured on a User Group basis.

5.1.1.14 Parent Group

It enables the Administrator to select a group from the available list to which a selected User will belong. A User may only belong to one parent group. The security privileges of the parent group will be added to the User's own privileges.

Note: This list is replaced by the 'Configure Group Privileges' button on the Groups Properties page.

5.1.1.15 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.1.16 Cancel Button

When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.1.17 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.1.18 Login Checkbox

When checked, the Logged in OEDesktop Filename field and its Browse button become enabled. This allows a specific OEDesktop file to be defined and loaded when a particular User logs in on an OpenEnterprise Workstation.

It is also possible to specify a Logged in OEDesktop file for a User Group, for the Default (All) Users Group, and also from within the saved OEDesktop file itself (for further information see the OEDesktop).

For an explanation of how OEDesktop Login - Logout file precedence works, see the Login - Logout File Precedence page.

5.1.1.19 OEDesktop Login - Logout File Precedence

Imagine that a User has been granted their own unique 'Logged in' OEDesktop file. This User belongs to a User Group that has a different 'Logged in' OEDesktop file assigned to it from the Security Configuration tool.

If this User now Logs into an OEDesktop that had been configured itself to load a 'Logged In' OEDesktop file, which OEDesktop file would be loaded? The order of precedence would be:

1. Load OEDesktop file specified at User level

2. Load OEDesktop file specified at User Group level
3. Load OEDesktop file specified at All (Default) Users Group level
4. Load OEDesktop file specified by the OEDesktop file itself.

Therefore, in the above example, the OEDesktop file specified at User level would be loaded.

5.1.1.20 Logout Checkbox

When checked, the Logged out OEDesktop Filename field and its Browse button become enabled. This allows a specific OEDesktop file to be loaded when this User Logs out of OpenEnterprise on a Workstation.

It is also possible to specify a Logged out OEDesktop file for a User Group, for the Default (All) Users Group, and also from within the saved OEDesktop file itself.

For an explanation of how OEDesktop Login - Logout file precedence works, see the Login - Logout File Precedence page.

5.1.1.21 Logged in OEDesktop Filename

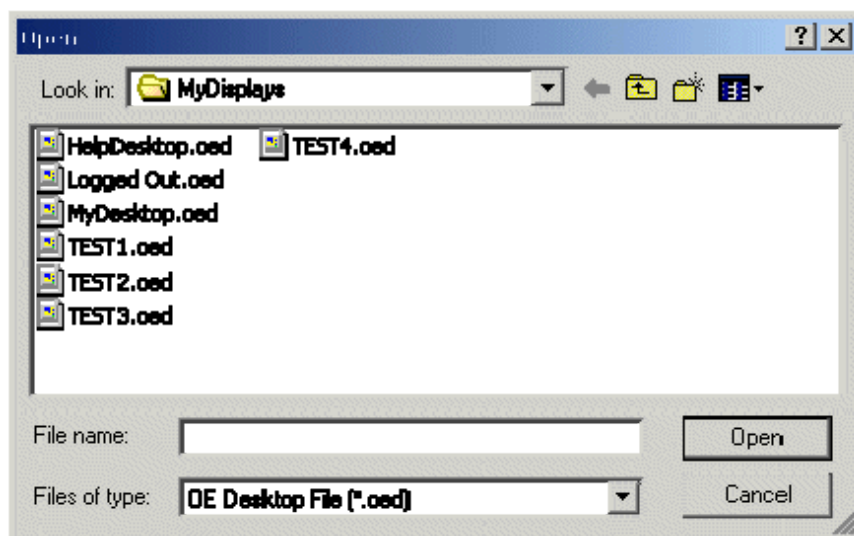
The full path name of the OEDesktop file to be loaded when the User or User Group logs in should be entered here. Of course, you can also use the browse button [...] to the right of this field to search for the actual file. When a file has been selected, the path and file name will be entered here automatically.

5.1.1.22 Logged out OEDesktop Filename

The full path name of the OEDesktop file to be loaded when the User or User Group logs out should be entered here. Of course, you can also use the browse button [...] to the right of this field to search for the actual file. When a file has been selected, the path and file name will be entered here automatically.

5.1.1.23 OED File Browse Button

When this button is selected, you will be presented with a standard Open file dialog.



Select the correct OED file to be loaded, and select the **[Open]** button. The file will not be opened, but the dialog will close, and the full path and name of the file will be entered into the appropriate OEDesktop file name field on the Properties tab.

5.1.2 User Group Properties Page

This page enables Administrator Users to configure security settings for User Groups. The dialog displayed in the example below is for the Default Group. The Default Group is created automatically by OpenEnterprise, and cannot be deleted. Since it is the Default Group, these settings apply to every User. Some of these settings can be overridden at a User or at a created User Group level, but others cannot. See Security Concepts and Glossary of Terms for more information on this. Note that there is no Summary tab, and Password and Verify Password fields are disabled. This is also true for the Properties Page of created Groups.

Group Properties - OPERATORS

File Token | OPC Item Token | Token Group

Properties | Account | Access Areas | Application Token | Custom Token

User Settings

User Name: OPERATORS

Full Name:

Description:

Password:

Verify Password:

Access Area: ALL

Administration

☐ Change Password At Next Logon

☐ User Cannot Change Password

☐ System Administrator

☐ Account Disabled

☐ Account LockOut

Grantor:

Group privileges

Configure group privileges

Load .OED File

☒ Login

C:\MyDisplays\MyDesktop.oed

☒ Logout

C:\MyDisplays\Logged Out.oed

OK Cancel Apply Help

5.1.3 The User Account Page

This tab enables the Administrator User to configure a User's password expiry, length and minimum age before a new password is allowed, as well as account lockout and auto logout settings.

User Properties - SEC_DEFAULT_USER1

Custom Token | File Token | OPC Item Token | Token Group

Properties | **Account** | Summary | Access Areas | Application Token

Password Expiry

☐ Expires In Days ☐ Expiry Warning Days Prior To Expiry

☐ Refuse Log In When Password Expires For OE Components

☐ Refuse Log In When Password Expires For ODBC/SQLC Components

Password Length

☐ Maximum Length Characters

☐ Minimum Length Characters

Password Age

☐ Minimum Age Days

Account Lock Out

☐ Lock Out Duration Minutes

☐ Number Of Failed Log On Attempts Before Lock Out

Auto Log Out

☐ Log Out (Fixed Period) In Minutes

☐ Log Out (Inactivity Period) In Minutes

OK Cancel Apply Help

5.1.3.1 Expires In

If not checked, then the User has Password Expiry disabled, and, as such, their Password never expires. The other fields in the Password Expiry section are disabled as long as the Expires In field is unchecked. When the Expires In field is checked, then the other fields in this section become enabled for editing.

Password Expiry is configured in days, and is applied relative to the last password change for the User. For instance, if a User changes their password at 11:23:07am on the 24th November 2000, and their account is configured such that the password expires after 3 days, then the User will be forced into a password change from 11:23:07am on the 27th November.

5.1.3.2 Expiry Warning

The Expiry Warning tick box will be greyed out unless the Expires In tick box has been enabled.

Configured in days, the Password Expiry Warning field allows a User to be warned in advance of an impending password expiry.

5.1.3.3 Refuse Login When Password Expires for OE Components

When a password expires for a User, the OpenEnterprise System can be configured such that the User is either: -

- Prevented from logging on to the system, or

- Permitted to log on to the OpenEnterprise System, but is expected to change their password immediately.

The Refuse Log In When Password Expires For OE Components tick box allows this functionality to be configured for OpenEnterprise Components, (e.g. OPC Server, HDA Server, Alarm Client Server).

The OELogin Client will enforce a password change for any User who is configured to allow log in when a password expires. If the User then chooses not to change their password, they will be automatically logged off the system.

5.1.3.4 Refuse Login When Password Expires for ODBC or SQL Components

If checked, OpenEnterprise will refuse to Login any User using a non-OpenEnterprise Component to access the Database. Such components would be ODBC (the Toolbox) or SQLC (the SQL Client). Since OpenEnterprise cannot enforce a Password change for non-OpenEnterprise components, this option should be checked for Users whose Password is set to expire.

5.1.3.5 Password Length Section

This section enables the User to configure Password dimensions.

5.1.3.6 Maximum Length

This field contains the maximum number of characters acceptable for a User's Password.

5.1.3.7 Minimum Length

This field contains the minimum number of characters allowed in a Password.

5.1.3.8 Password Age Section

This section enables the User to configure the length of time a new User password will last before a new password is required. Regular changing of User passwords is a necessary part of any good security regime.

5.1.3.9 Minimum Age

A User's account can be configured such that they are only allowed to change their password on a periodic basis.

The Minimum Age option can be used to enable this. The period is configured in days, and is applied based on the last password change for the User. For instance, if the Minimum Age is specified as 5 days, and the User changes their password at 2:45:34pm on the 24th November, then they will not be allowed to change their password again until 2:45:34pm on the 29th November.

If the Minimum Age value is greater than the Password Expiry value then there could be a situation where an expired password cannot be changed. The Configuration tool ensures that this situation cannot occur.

5.1.3.10 Account Lockout

This flag indicates a User's account is locked out. This prevents the User from logging on and from changing their password.

Although an account can be locked out manually, the most common use of account lockout will be to protect the OpenEnterprise SCADA System. For instance, consecutive failures to log on as a User due to an incorrect password can cause the User's account to be locked out.

The unlocking of an account may be achieved by either of the following:

- Manual unlocking by a Security Administrator using the configuration tool

- Time based, whereby the lock is automatically released after a pre-configured period of time

5.1.3.11 Lockout Duration

This field contains the number of minutes duration for which the User will be locked out of their account. Although an account can be locked out manually, the most common use of account lockout will be due to an incorrect User name or Password. A value of 0 for this field implies permanent lock out, as does leaving the associated tick box unchecked.

5.1.3.12 Number of Failed Logon Attempts Before Lockout

This field contains the number of minutes duration for which the User will be locked out of their account. Although an account can be locked out manually, the most common use of account lockout will be due to an incorrect User name or Password. A value of 0 for this field implies permanent lock out, as does leaving the associated tick box unchecked.

5.1.3.13 Auto Logout Section

This section can be used to ensure that Workstations are not left with Users logged on to the OpenEnterprise SCADA System.

5.1.3.14 Logout Fixed Period

A fixed period in minutes during which a user can remain logged in. After that time OpenEnterprise automatically logs the user out.

5.1.3.15 Logout After Inactivity

A period (in minutes) of mouse or keyboard inactivity allowed on the PC from which a user has logged in. After that time of inactivity has expired, OpenEnterprise logs the user out.

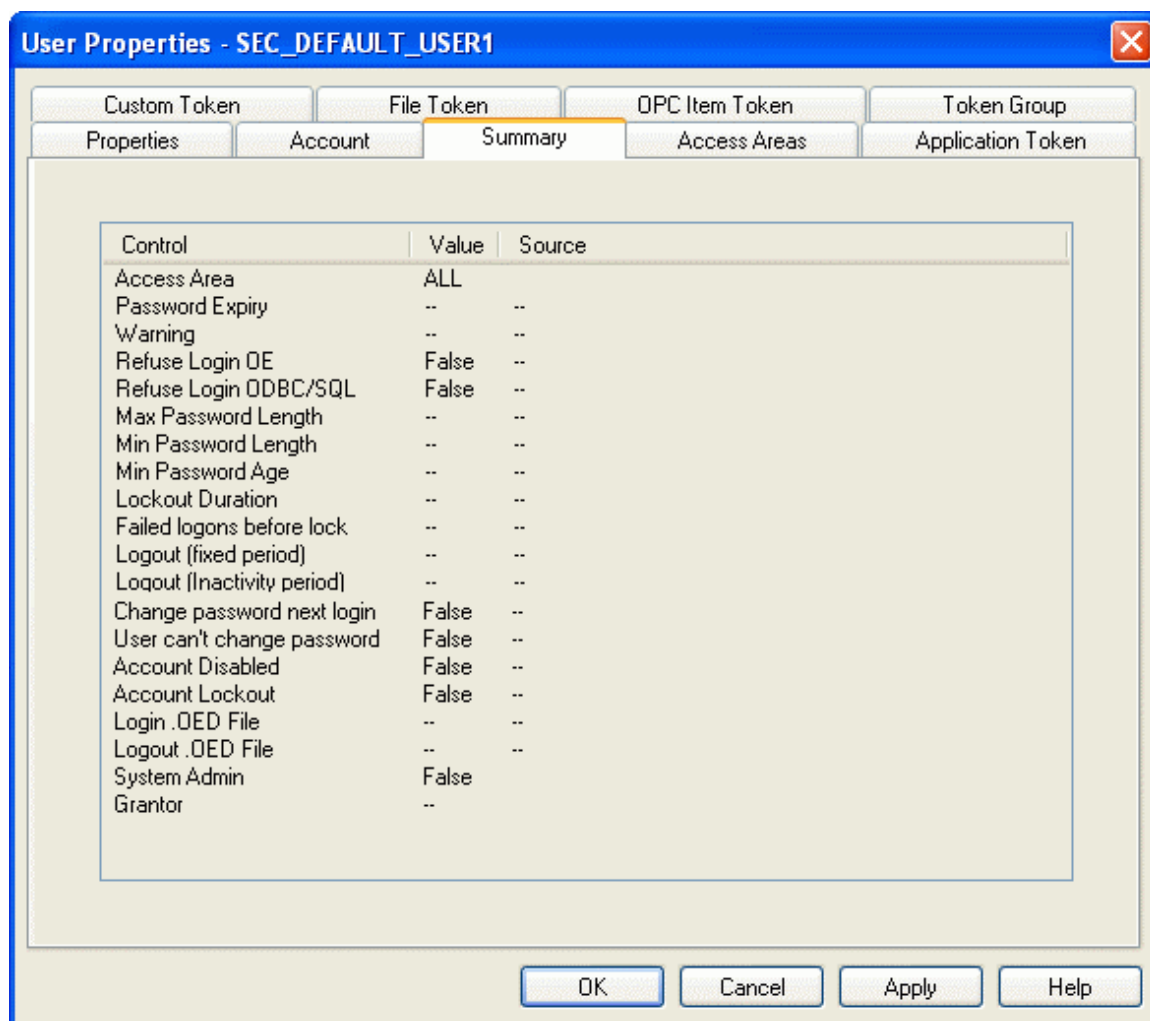
5.1.3.16 Apply Logout Per Database Connection

By default all auto log out functionality is applied on a per Workstation basis and this is the recommended configuration for all OpenEnterpriseWorkstation Users. By handling auto log out on a per Workstation basis, OpenEnterprise prevents the situation whereby some of the Database clients on a Workstation are logged on and others are not. A situation based on when those OpenEnterprise Database clients were started and when a new activity last occurred within each client would lead to an ambiguous situation in terms of determining the current log on status of a Workstation.

If, however, pseudo Users are used to provide access to automatic report generation, and are only likely to log on through one client, then it may be preferable to configure those Users to handle auto log out on a per connection basis.

5.1.4 The User Summary Page

This page summarizes the current settings for a User. This tab is not provided for either a User created Group or the Default Group.



5.1.4.1 Summary List

This list provides an Administrator with configuration details for a User at a glance. It shows a list of control items together with their current values, and the source of the control value. For example, if the User belongs to a Group that has set the minimum password length yet User hasn't, then the source will be shown as "Group", and the number displayed. Possible values in the Source column are: User, Group, Default. If no value is currently in use then a double dash "--" will be displayed.

5.1.4.2 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.4.3 Cancel Button

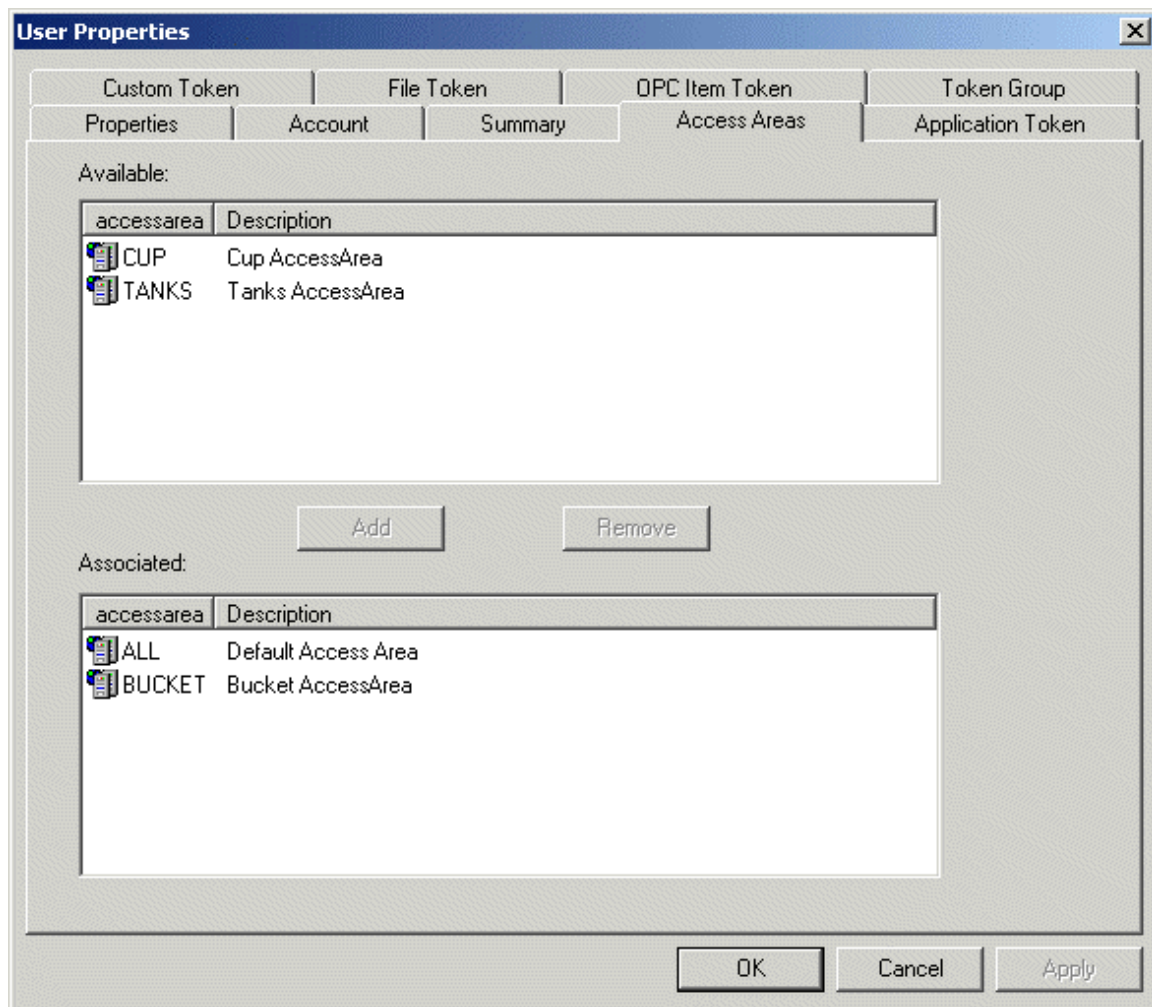
When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.4.4 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.5 The User Access Areas Page

This dialog is used to assign Access Areas to a User or User Group.



5.1.5.1 Available Access Areas

This list displays the Access Areas available which have not yet been associated with the User.

5.1.5.2 Add Access Area Button

When this button is selected, any Access Area chosen in the Available Access Areas List will be moved to the Associated list for the User.

5.1.5.3 Remove Access Area

Any Access Areas chosen from the Associated Access Areas List will be removed. They will no longer be associated with the User.

5.1.5.4 Associated Access Areas

This list displays the Access Areas already associated with the User.

5.1.5.5 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.5.6 Cancel Button

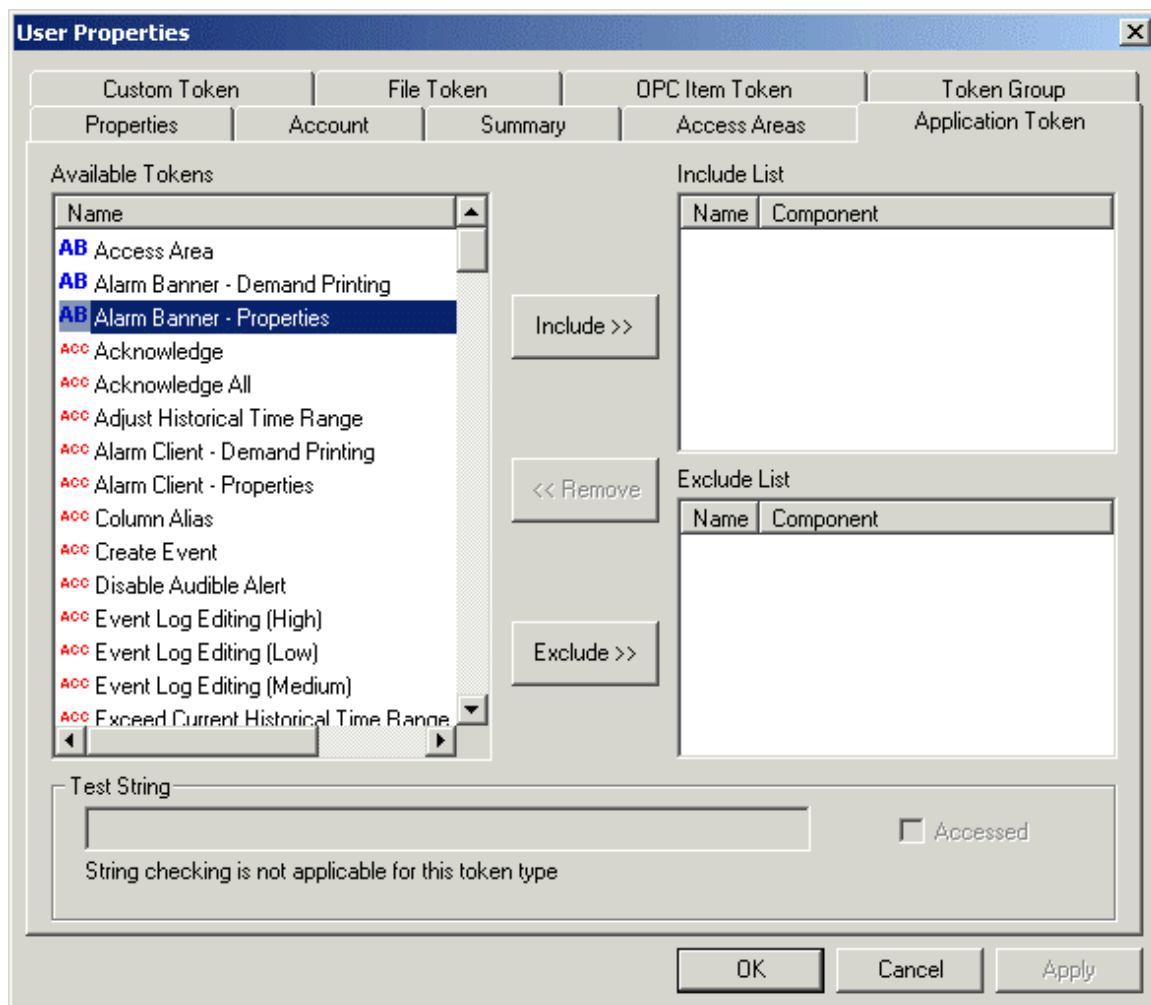
When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.5.7 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.6 The User Application Token Page

This tab enables the Administrative User to award or deny individual Application Tokens to Users.



5.1.6.1 Available Tokens

This list displays the Tokens available to the User.

5.1.6.2 Include Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Exclude List'. When the button is clicked, the token selected is removed and placed in to the 'Include List' for the User.

5.1.6.3 Remove Button

This button becomes enabled when a Token is selected from the 'Include List' or 'Exclude List'. Clicking the button will remove the selected Token from the List in which it currently resides and replace it into the 'Available Tokens' list.

5.1.6.4 Exclude Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Include List'. When the button is clicked, the token selected is removed from that list and placed in to the 'Exclude List' for the User.

5.1.6.5 Test String

If a string is entered here, then the check box will indicate whether or not the string in question would be accessible based on the current Include/Exclude list for these Token Types

Note: Any Tokens assigned indirectly via Token Groups are not included in this pattern match. Also, the state reflects the currently displayed lists. These may not yet have been updated in the database if Apply has not been selected.

Note: This field is disabled on the Application Token and Token Groups Tabs.

For an explanation of how Token strings are matched and how the Include and Exclude lists are searched see Token Pattern Matching.

5.1.6.6 String Accessed

If the String typed into the Test String field is matched in the User's included list, then this box is checked.

5.1.6.7 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.6.8 Cancel Button

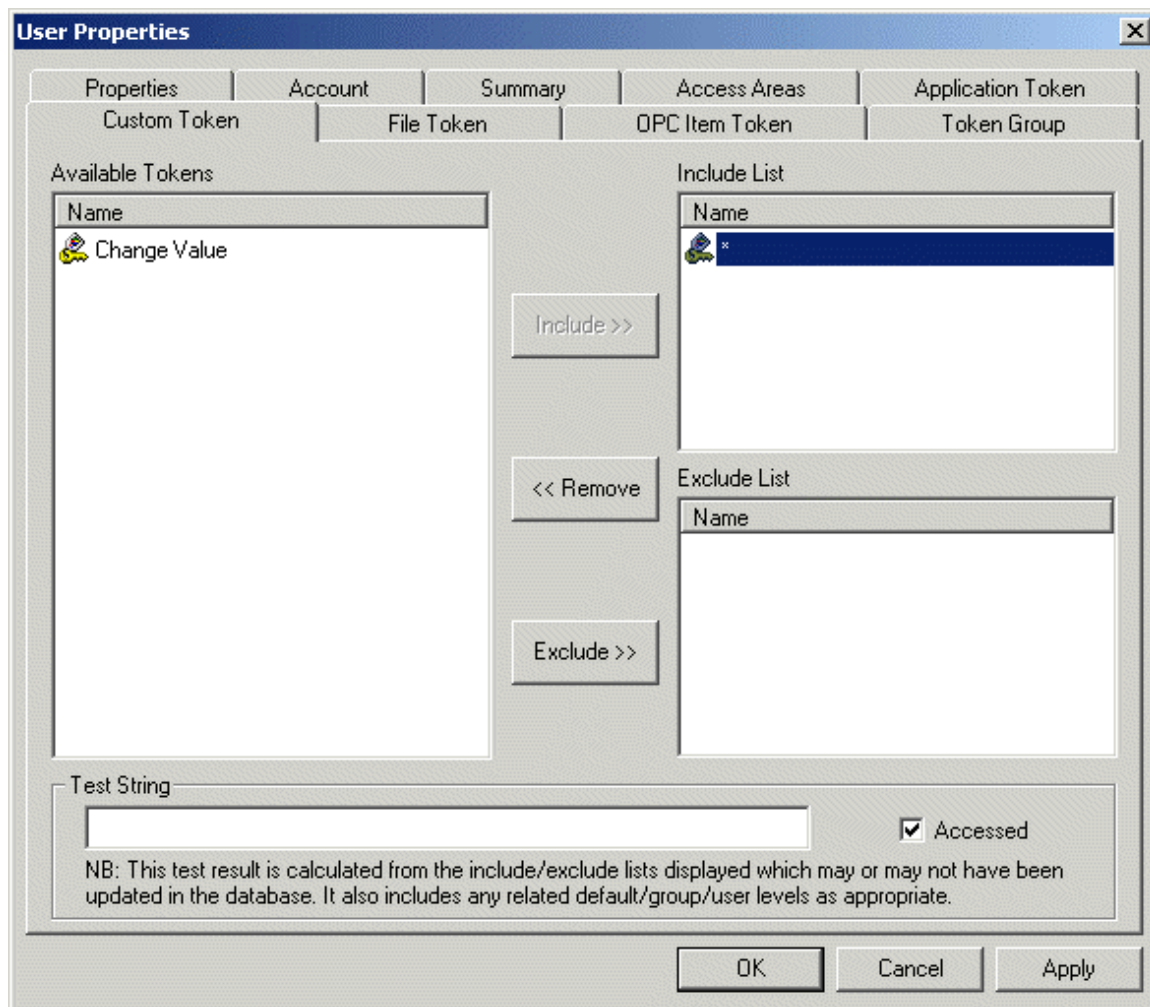
When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.6.9 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.7 The User Custom Token Page

It is on the Custom Token Tab that Users can be awarded or denied individual Custom Tokens. This tab is very similar in operation to the Application Token tab, but these tokens do not have a Component displayed.



5.1.7.1 Available Tokens

This list displays the Tokens available to the User.

5.1.7.2 Include Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Exclude List'. When the button is clicked, the token selected is removed and placed in to the 'Include List' for the User.

5.1.7.3 Remove Button

This button becomes enabled when a Token is selected from the 'Include List' or 'Exclude List'. Clicking the button will remove the selected Token from the List in which it currently resides and replace it into the 'Available Tokens' list.

5.1.7.4 Exclude Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Include List'. When the button is clicked, the token selected is removed from that list and placed in to the 'Exclude List' for the User.

5.1.7.5 Include List

This list displays the Custom Tokens that have been awarded to the User. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: It will not list any Custom Tokens that may have indirectly been assigned to this User by means of a Token Group, unless they have also specifically been awarded as individual Tokens.

Note: There may be contention issues whereby 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.

5.1.7.6 Exclude List

This list displays the Application Tokens that have been denied to the User from this configuration page. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: it will not list any Custom Tokens that may have indirectly been removed from this User by means of a Token Group, unless they have also specifically been excluded as individual Tokens.

5.1.7.7 Test String

If a string is entered here, then the check box will indicate whether or not the string in question would be accessible based on the current Include/Exclude list for these Token Types

Note: Any Tokens assigned indirectly via Token Groups are not included in this pattern match. Also, the state reflects the currently displayed lists. These may not yet have been updated in the database if Apply has not been selected.

Note: This field is disabled on the Application Token and Token Groups Tabs.

For an explanation of how Token strings are matched and how the Include and Exclude lists are searched see Token Pattern Matching.

5.1.7.8 Accessed Check Box

This box becomes checked if a string typed into the Test String field matches a string in the User's Included Token list. It verifies that the User has access to the Token.

5.1.7.9 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.7.10 Cancel Button

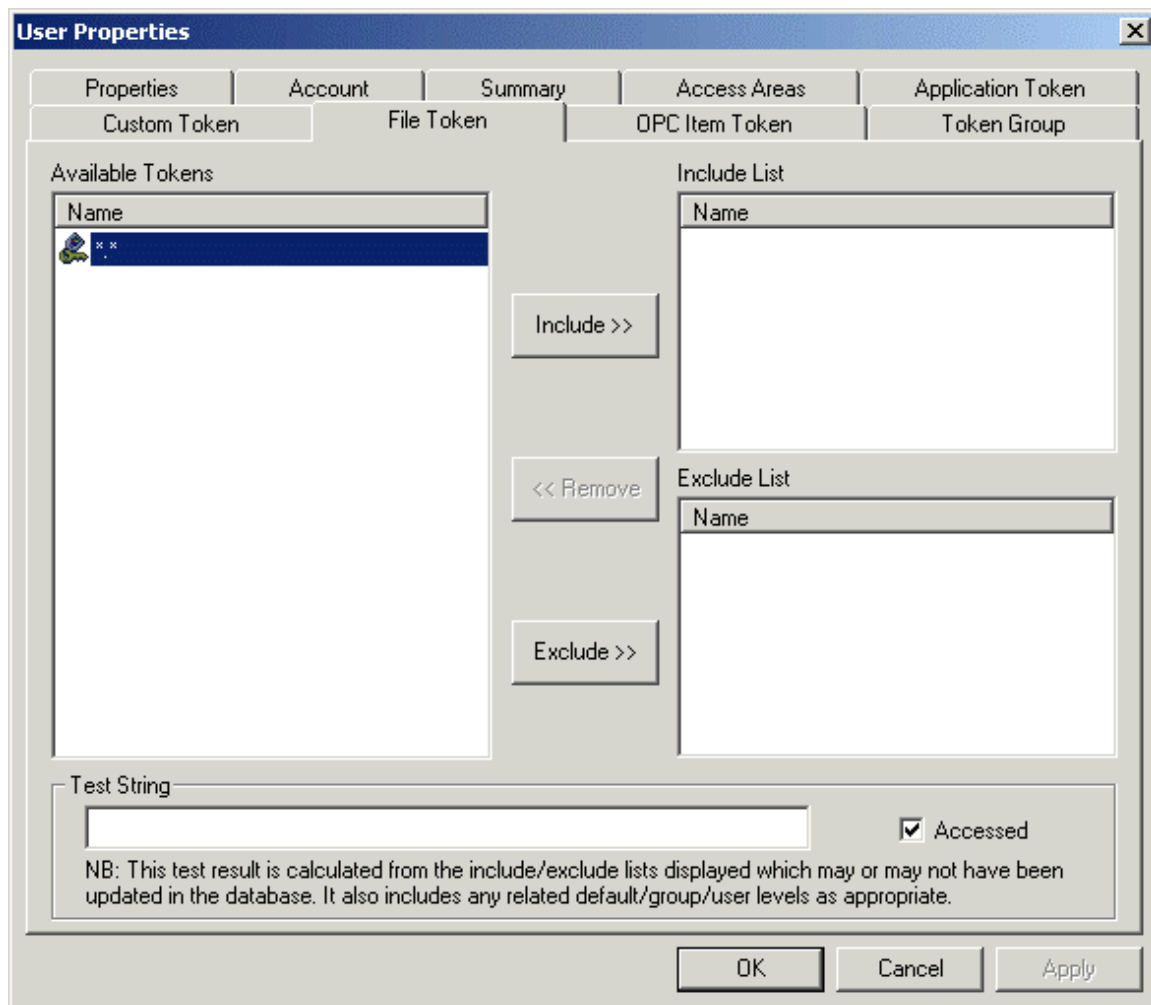
When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.7.11 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.8 The User File Token Page

It is on the File Token Tab that Users can be awarded or denied individual File Tokens. This provides or denies access to files on the User's Workstation (e.g. could be certain displays).



5.1.8.1 Available Tokens

This list displays the Tokens available to the User.

5.1.8.2 Include Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Exclude List'. When the button is clicked, the token selected is removed and placed in to the 'Include List' for the User.

5.1.8.3 Remove Button

This button becomes enabled when a Token is selected from the 'Include List' or 'Exclude List'. Clicking the button will remove the selected Token from the List in which it currently resides and replace it into the 'Available Tokens' list.

5.1.8.4 Exclude Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Include List'. When the button is clicked, the token selected is removed from that list and placed in to the 'Exclude List' for the User.

5.1.8.5 Include List

This list displays the Custom Tokens that have been awarded to the User. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: It will not list any Custom Tokens that may have indirectly been assigned to this User by means of a Token Group, unless they have also specifically been awarded as individual Tokens.

Note: There may be contention issues whereby 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.

5.1.8.6 Exclude List

This list displays the Application Tokens that have been denied to the User from this configuration page. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: it will not list any Custom Tokens that may have indirectly been removed from this User by means of a Token Group, unless they have also specifically been excluded as individual Tokens.

5.1.8.7 Test String

If a string is entered here, then the check box will indicate whether or not the string in question would be accessible based on the current Include/Exclude list for these Token Types

Note: Any Tokens assigned indirectly via Token Groups are not included in this pattern match. Also, the state reflects the currently displayed lists. These may not yet have been updated in the database if Apply has not been selected.

Note: This field is disabled on the Application Token and Token Groups Tabs.

For an explanation of how Token strings are matched and how the Include and Exclude lists are searched see Token Pattern Matching.

5.1.8.8 Accessed Check Box

This box becomes checked if a string typed into the Test String field matches a string in the User's Included Token list. It verifies that the User has access to the Token.

5.1.8.9 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.8.10 Cancel Button

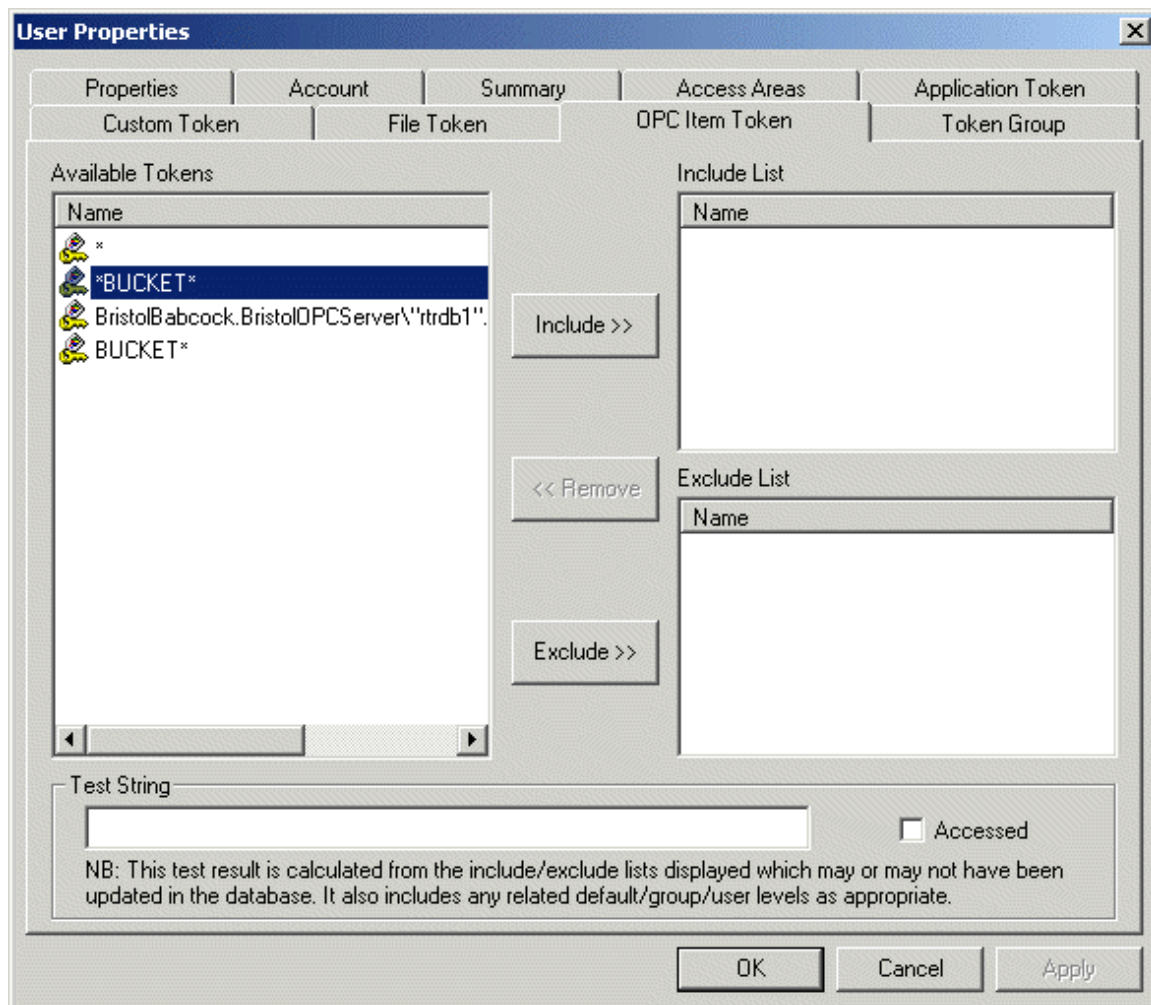
When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.8.11 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.9 The User OPC Item Page

It is on the OPC Token Tab that Users can be awarded or denied individual OPC Tokens, allowing or denying a User to update a value on a Graphic View display.



5.1.9.1 Available Tokens

This list displays the Tokens available to the User.

5.1.9.2 Include Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Exclude List'. When the button is clicked, the token selected is removed and placed in to the 'Include List' for the User.

5.1.9.3 Remove Button

This button becomes enabled when a Token is selected from the 'Include List' or 'Exclude List'. Clicking the button will remove the selected Token from the List in which it currently resides and replace it into the 'Available Tokens' list.

5.1.9.4 Exclude Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Include List'. When the button is clicked, the token selected is removed from that list and placed in to the 'Exclude List' for the User.

5.1.9.5 Include List

This list displays the Custom Tokens that have been awarded to the User. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: It will not list any Custom Tokens that may have indirectly been assigned to this User by means of a Token Group, unless they have also specifically been awarded as individual Tokens.

Note: There may be contention issues whereby 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.

5.1.9.6 Exclude List

This list displays the Application Tokens that have been denied to the User from this configuration page. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: it will not list any Custom Tokens that may have indirectly been removed from this User by means of a Token Group, unless they have also specifically been excluded as individual Tokens.

5.1.9.7 Test String

If a string is entered here, then the check box will indicate whether or not the string in question would be accessible based on the current Include/Exclude list for these Token Types

Note: Any Tokens assigned indirectly via Token Groups are not included in this pattern match. Also, the state reflects the currently displayed lists. These may not yet have been updated in the database if Apply has not been selected.

Note: This field is disabled on the Application Token and Token Groups Tabs.

For an explanation of how Token strings are matched and how the Include and Exclude lists are searched see Token Pattern Matching.

5.1.9.8 Accessed Check Box

This box becomes checked if a string typed into the Test String field matches a string in the User's Included Token list. It verifies that the User has access to the Token.

5.1.9.9 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.9.10 Cancel Button

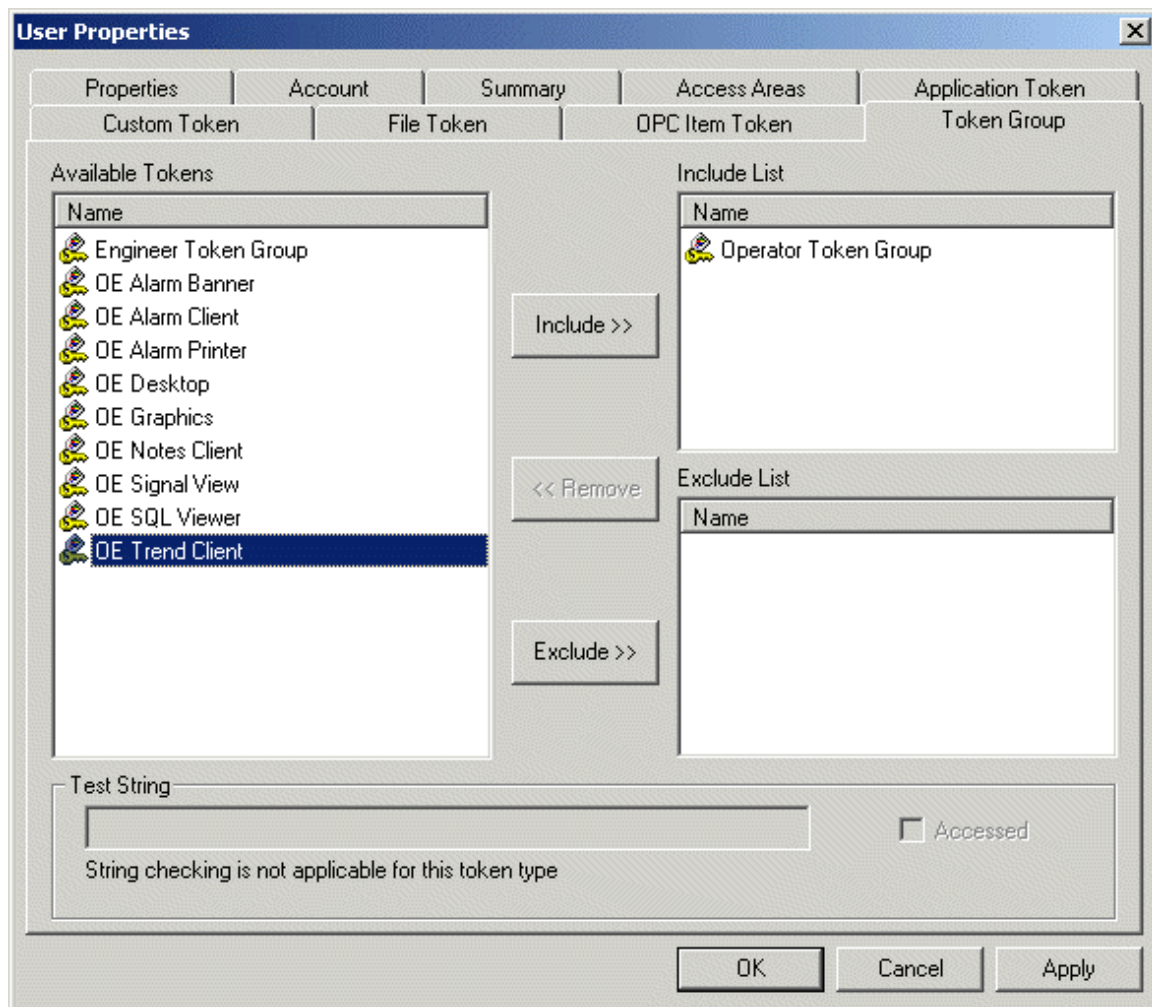
When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.9.11 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.1.10 The User Token Group Page

This dialog enables the Administrative User to configure individual Tokens of any type to be included within the Token Group. The whole Token Group may then be awarded or denied to Users or Groups. This feature simplifies the process of assigning commonly used sets of Tokens to Users or Groups.



5.1.10.1 Available Tokens

This list displays the Tokens available to the User.

5.1.10.2 Include Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Exclude List'. When the button is clicked, the token selected is removed and placed in to the 'Include List' for the User.

5.1.10.3 Remove Button

This button becomes enabled when a Token is selected from the 'Include List' or 'Exclude List'. Clicking the button will remove the selected Token from the List in which it currently resides and replace it into the 'Available Tokens' list.

5.1.10.4 Exclude Button

This button becomes available when a token is selected from the 'Available Tokens' list or the 'Include List'. When the button is clicked, the token selected is removed from that list and placed in to the 'Exclude List' for the User.

5.1.10.5 Include List

This list displays the Custom Tokens that have been awarded to the User. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: It will not list any Custom Tokens that may have indirectly been assigned to this User by means of a Token Group, unless they have also specifically been awarded as individual Tokens.

Note: There may be contention issues whereby 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.

5.1.10.6 Exclude List

This list displays the Application Tokens that have been denied to the User from this configuration page. Items in this list may be removed by using the [<<Remove] button.

Items may be moved to the Include list by selecting them in the Exclude List and pressing the Include button.

Note: it will not list any Custom Tokens that may have indirectly been removed from this User by means of a Token Group, unless they have also specifically been excluded as individual Tokens.

5.1.10.7 Test String

If a string is entered here, then the check box will indicate whether or not the string in question would be accessible based on the current Include/Exclude list for these Token Types

Note: Any Tokens assigned indirectly via Token Groups are not included in this pattern match. Also, the state reflects the currently displayed lists. These may not yet have been updated in the database if Apply has not been selected.

Note: This field is disabled on the Application Token and Token Groups Tabs.

For an explanation of how Token strings are matched and how the Include and Exclude lists are searched see Token Pattern Matching.

5.1.10.8 Accessed Check Box

This box becomes checked if a string typed into the Test String field matches a string in the User's Included Token list. It verifies that the User has access to the Token.

5.1.10.9 OK Button

When selected, the dialog closes, and any configuration changes are sent to the database.

5.1.10.10 Cancel Button

When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.1.10.11 Apply Button

When selected, the changes already made on the dialog will be sent to the database without closing the dialog.

5.2 Token Group Property Dialog

This dialog enables an Administrative User to configure the Tokens that will be included within a User created Token Group. It is accessed by double clicking on any Token Group displayed in either the left or right panes of the Security Configuration tool. The default application Token Groups cannot be edited, and the Token Association section will be disabled if a default Token Group is selected.

Once created, the whole Token Group may be included or excluded in a User or Group's security profile. This feature simplifies the process of assigning commonly used sets of Tokens to Users.

Token Group Properties

Token Group Name: Access Area:

Description:

Token Association:

TokenType: ☐ File ☒ Application ☐ Custom ☐ OPC Item

Available Tokens:

Name	Component
AB Access Area	OE Alarm Banner
AB Alarm Banner - Demand Printing	OE Alarm Banner
AB Alarm Banner - Properties	OE Alarm Banner
ACC Acknowledge All	OE Alarm Client
ACC Adjust Historical Time Range	OE Alarm Client
ACC Alarm Client - Demand Printing	OE Alarm Client
ACC Alarm Client - Properties	OE Alarm Client
ACC Column Alias	OE Alarm Client
ACC Create Event	OE Alarm Client
ACC Disable Audible Alert	OE Alarm Client
ACC Event Log Editing (High)	OE Alarm Client
ACC Event Log Editing (Low)	OE Alarm Client
ACC Event Log Editing (Medium)	OE Alarm Client

Configured Tokens:

Name	Type
ACC Acknowledge	Application

Buttons: Add, Remove, OK, Cancel

5.2.1 Token Group Name

This field contains the name that was given to the Token Group when it was created. It is not editable after the Token Group has been created.

5.2.2 Token Access Area

By selecting this field the Administrative User is able to select a different access area for this Token. Default is ALL for a new Token.

5.2.3 Token Group Description

This field may contain a lengthier description of the purpose of this Token Group.

5.2.4 Token Type Section

This section contains four radio buttons, which represent the four Token types. As the Administrative User selects each of the radio buttons, the Available Tokens list is filled with the available Tokens of that type. The Administrative User is then able to select Tokens of every type to include in the Token Group.

5.2.5 Available Tokens

This list displays the Tokens available to the User.

5.2.6 Component Column

The Application Token Tab supports an additional column for 'Component' in the three lists. It names the OEView component for which the Application action is valid.

The lists may be sorted on either Name or Component by clicking the column header. Initial sorting of the Available Tokens is on Component Type. The Component column may not be visible if the Name field is too wide, but may be scrolled to by use of scrolling bars.

This column is only available for Application Tokens.

5.2.7 Configured Tokens List - Token Groups

This list is filled with configured Tokens for the Token Group. The Administrative User may remove any Token from this list by selecting it and then selecting the [Remove] button. This list may be sorted on either Name or Type. Default sorting is on Name.

5.2.8 Add Button

This button adds selected Tokens from the Available Token List to the Configured Token List.

5.2.9 Remove Tokens Button

This button removes selected Tokens from the Configured Tokens list for the Token Group.

5.3 Token Properties Dialog

This dialog enables the Administrative User to change the Description or Access Area of any individual Token. An Application Token Properties dialog is shown as an example, but the three other types are very similar, with different text and graphics, though the other three types do not have a Component or Item Id displayed.

The screenshot shows the 'Token Properties' dialog box. It has a title bar with the text 'Token Properties'. Inside, there are three main sections. The first section is labeled 'Type' and shows 'Application' with a key icon and a descriptive paragraph: 'Application tokens are predefined programmatically and may not be added to via the security configuration tool. They protect access to specific User Interface actions within the Open Enterprise Graphical Components.' The second section is labeled 'Properties' and contains three fields: 'Token Name' with the value 'Access Area', 'Access Area' with a dropdown menu showing 'ALL', and 'Description' with the value 'Access Area'. The third section is labeled 'Application' and contains two fields: 'Item Id' with the value '1018' and 'Component' with the value 'OE Alarm Banner'. There is a small 'AB' icon next to the 'Component' field. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

5.3.1 Token Name

This cannot be edited, since it is a primary key in the Token table.

5.3.2 Token Access Area

By selecting this field the Administrative User is able to select a different access area for this Token. Default is ALL for a new Token.

5.3.3 Token Description

The Administrative User is able to type in a more informative description of this Token.

5.3.4 OK Button

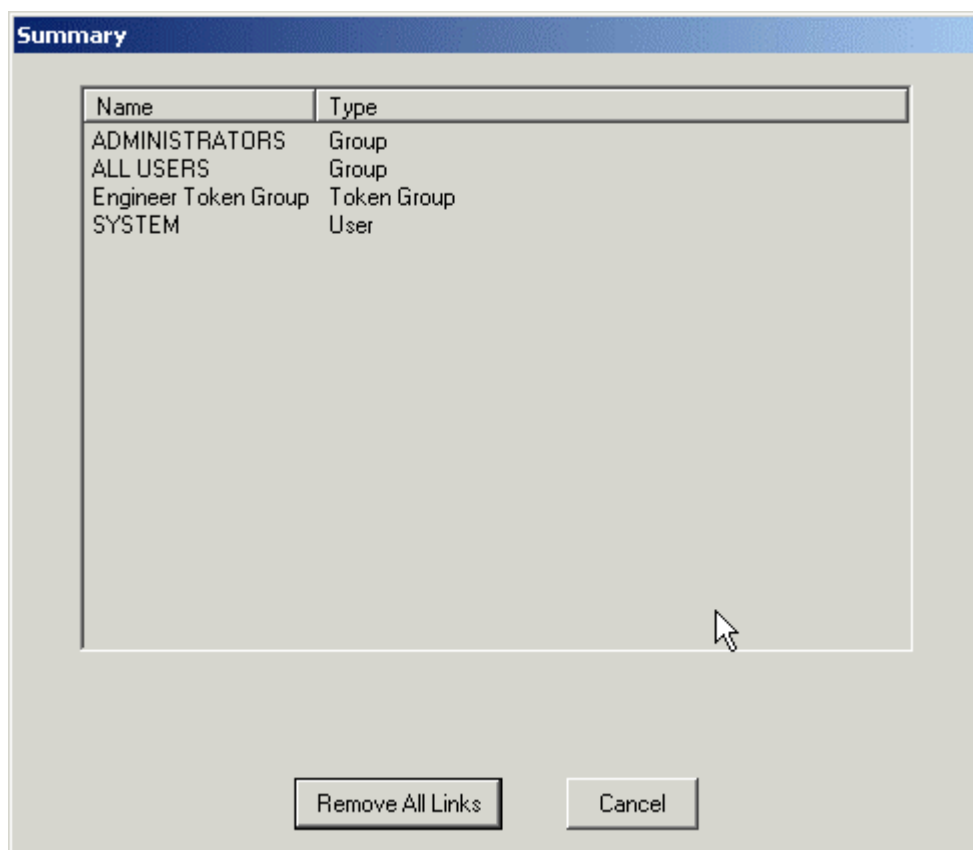
When selected, the dialog closes, and any configuration changes are sent to the database.

5.3.5 Cancel Button

When this button is selected, the dialog will close. Any configuration changes made will not be sent to the database.

5.4 Token Summary Dialog

This dialog displays the Users and Groups that are linked with the selected Token.



5.4.1 Token Summary

The token Summary window displays any Users and Groups that currently have the selected Token in their Include or Exclude list.

5.4.2 Remove All Links Button

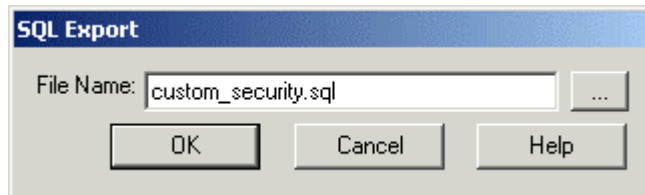
The link between any associated Users and Groups can be removed by selecting this button.

5.4.3 Token Summary Cancel Button

When this button is selected the Token Summary dialog will close.

5.5 SQL Import-Export File Dialog

This dialog enables the user to override the default SQL script file for Export or Import or to specify the name of a file to which the Import Status will be saved. The Title of the dialog will differ depending on what action is being taken.



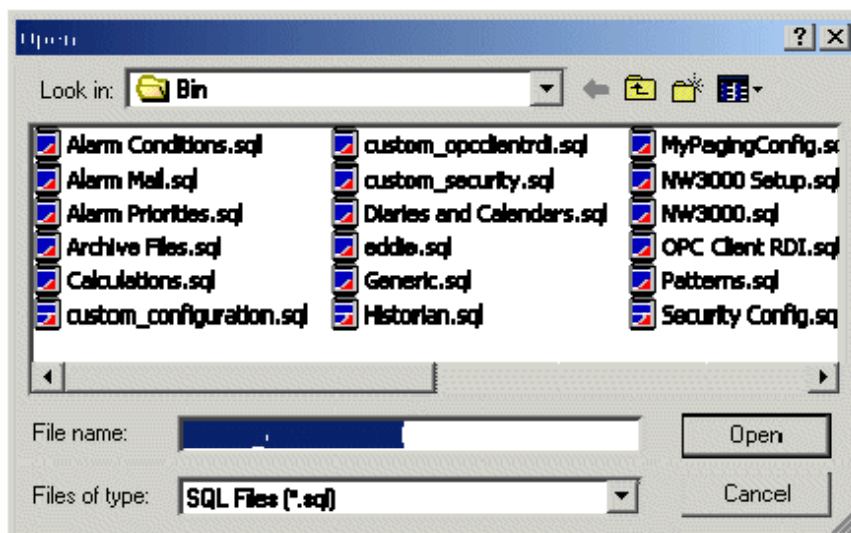
5.5.1 File Name

By default the Import or Export file will be named *custom_<Component>.sql*, where <Component> indicates the OpenEnterprise configuration component from which the Import/Export is initiated, and will be written to the standard OEToolbox export file directory. The Status file has a default name of *custom_<Component>.txt*. If a file already exists in the directory with the filename specified, then the existing file should be renamed such that .old is appended to the end of it, e.g. *custom_opcclientrtdi.sql.old*.

When Importing or Exporting, this file will be selected automatically and placed in the *File Name* field. The user will however have the ability to override both the name and location if they so require, using the browse button, or by manually editing the filename.

5.5.2 File Browse Button

When the File Browse Button is selected, a standard File Open or File Save dialog is displayed, depending on which function has been chosen. The user can then select a file for Import, Export or Saving Import Status.



File Browse Dialog

5.5.3 OK Button

When selected, the appropriate action will be commenced, using the file specified in the *File Name* field, depending on the action that was chosen: -

Export

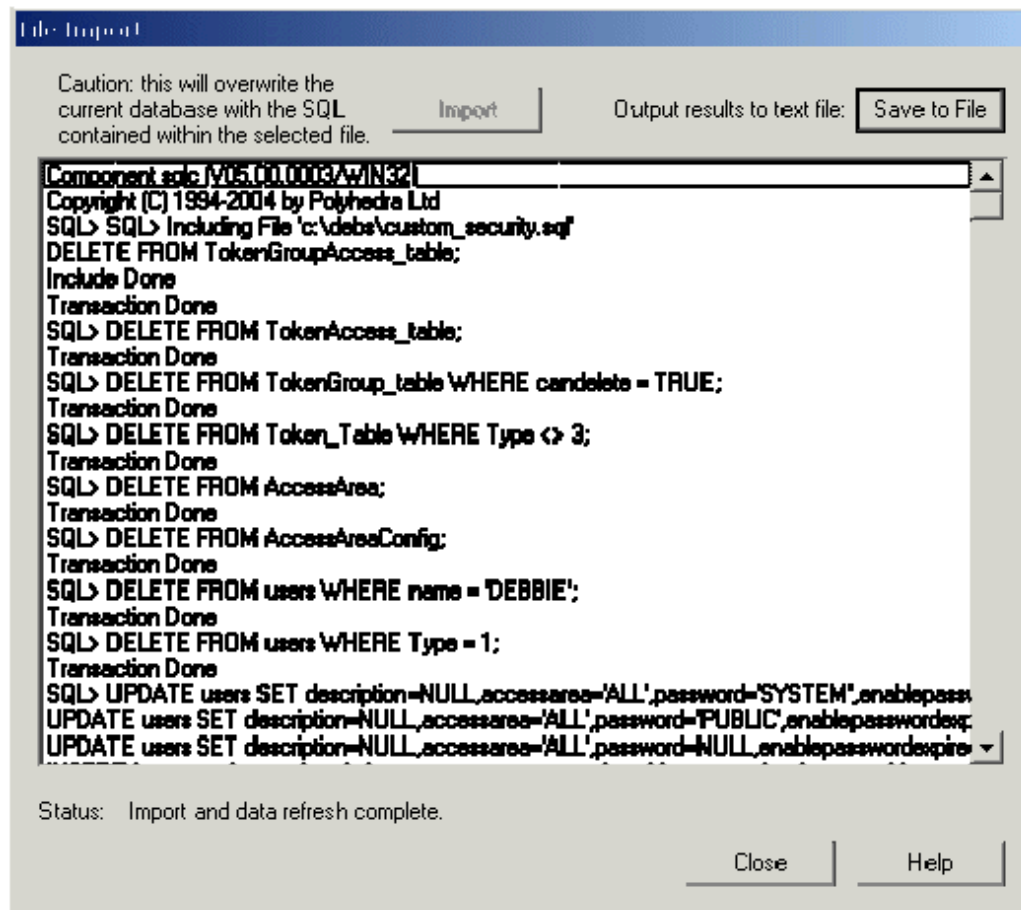
Import

5.5.4 Cancel Button

When selected, the File Import, Export or Save Status to File will be aborted.

5.6 File Import Dialog

The 'File Import' dialog enables the user to initiate and view the progress of the Import process, and to save the contents of the Status window to a file.



5.6.1 Import Button

Selection of this button will initiate the Import process.

5.6.1.1 Import Warning

If the user is about to Import a previous configuration from a saved SQL file, then the user will also be presented with an additional confirmation dialog, to ensure that they are aware that they are about to overwrite their entire existing Security configuration. If the **[OK]** button is selected from this Message, the Import will commence.

5.6.2 Save to File Button

Saves the contents of the Status Window to a text file. The SQL Import-Export File Dialog will be presented so that the user can select or specify a file to save to. The file will be a text file, having a .TXT extension.

5.6.3 Status Pane

This pane displays the status of the Import process as it happens. The existence of duplicate key errors does not necessarily indicate failure of the whole importation process.

The entire contents of the pane can be saved to a text file by selecting the **[Save to File]** button.

5.6.4 Status Message

This message displays the most recent action from the Status Pane.

5.6.5 Close Button

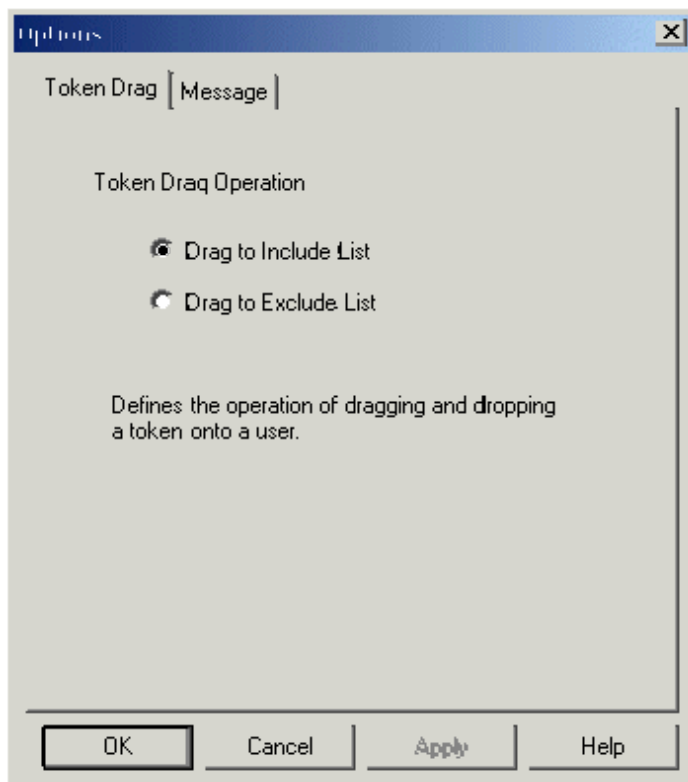
Selecting this button closes the Import Status dialog.

5.6.6 Help Button

Selecting this button will display context sensitive help for the dialog.

5.7 Options Dialog

This tab enables the Administrative User to configure the way that Token drag and drop functionality works within the Security Configuration tool.



5.7.1 Token Drag to Include List

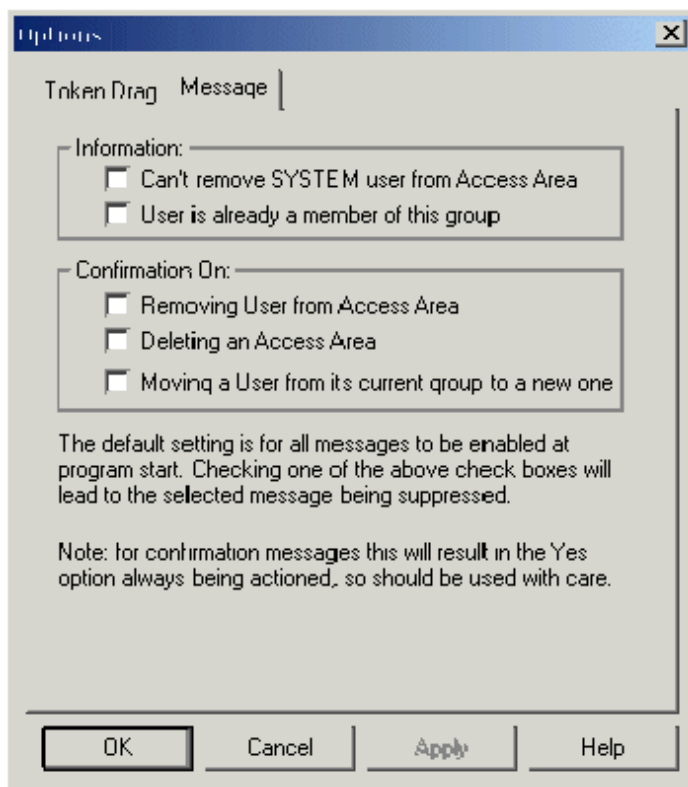
If this box is checked, a Token or Token Group selected from the Right Pane and dragged and dropped onto a User or User Group within the Left Pane will be added to the Included List for the User or User Group.

5.7.2 Token Drag Exclude

If this box is checked, a Token or Token Group selected from the Right Pane and dragged and dropped onto a User or User Group within the Left Pane will be added to the Excluded List for the User or User Group.

This tab allows the Administrative User to suppress system messages by checking the boxes on the dialog. It may be desirable to suppress informational messages during multi-selection moves.

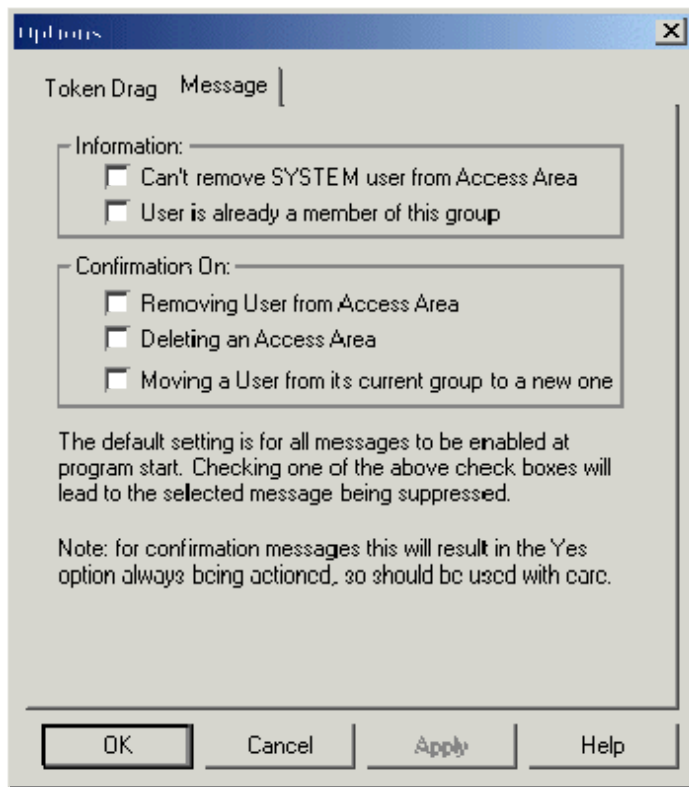
The options are reset (i.e. unchecked) at program start such that all messages are seen.



5.7.3 Options Dialog - Messages Tab

This tab allows the Administrative User to suppress system messages by checking the boxes on the dialog. It may be desirable to suppress informational messages during multi-selection moves.

The options are reset (i.e. unchecked) at program start such that all messages are seen.



5.7.3.1 Removing SYSTEM User from Access Area

This informational message is normally seen when an attempt is made to remove the SYSTEM User from an Access Area. By default a SYSTEM User must always be in every Access Area. If this message is suppressed then it won't be seen when this operation is attempted.

5.7.3.2 Already a Member of this Group

This informational message is normally seen when trying to drag and drop a User onto a Group that they are already associated with.

5.7.3.3 Removing User from Access Area

This confirmation message is normally seen when removing a User from an Access Area. If the message is suppressed, i.e. checked in this dialog box, then no confirmation is sought before proceeding with the removal.

5.7.3.4 Deletion of Access Area

This confirmation message is normally seen when deleting an Access Area. If the message is suppressed, i.e. checked in this dialog box, then no confirmation is sought before proceeding with the deletion.

5.7.3.5 Moving User from Current Group

This confirmation message is normally seen when moving a User from its current User Group to a new one. If the message is suppressed, i.e. checked in this dialog box, then no confirmation is sought before proceeding with the move..

This dialog enables you to configure how the Export file displays passwords. It is not visible by default. To make it visible, follow the instructions on the *Enabling the Password Tab* page.



5.7.4 Options Dialog - Password Tab

This dialog enables you to configure how the Export file displays passwords. It is not visible by default. To make it visible, follow the instructions on the *Enabling the Password Tab* page.



5.7.4.1 Password Visible

When this box is checked, the saved SQL log file will show all User passwords. When it is unchecked, passwords will be saved to the file as asterisks. The default behaviour is to show passwords as asterisks.

5.7.4.2 Enabling the Password Tab

By default the Password tab is not available on the Options dialog. It can be enabled, however, by creating a new *Options* key off the *Security Configuration* key:-

```
HKLM\BristolBabcock\OpenEnterprise\Tasks\OEToolbox\Editors\Security  
Configuration\Options
```

Then, on the new *Options* key, add a DWORD value called *Menu*, and give this a value of 1. Close the Toolbox, re-open it and the Security Configuration tool should now be displaying the *Password* tab on the *Options* dialog.

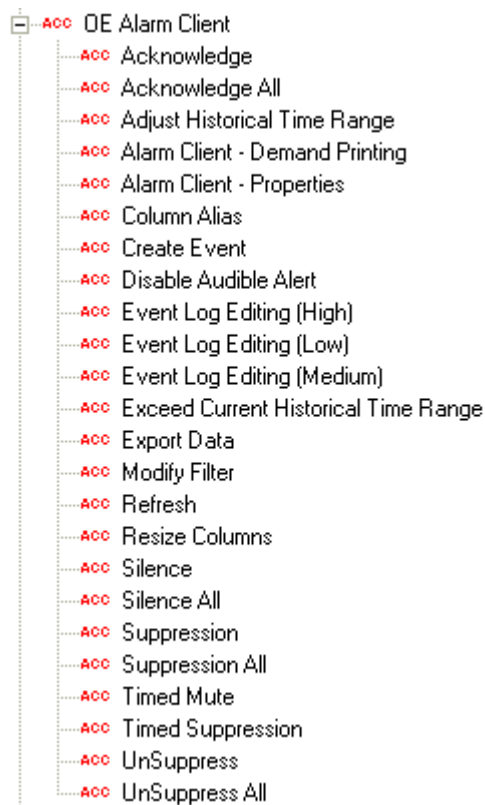
Options Dialog - Password Tab

6 Application Tokens Reference

- Alarm Banner Tokens
- Alarm View Tokens
- OEDesktop Tokens
- Graphics View Tokens
- Notes Client Tokens
- Signal View Tokens
- SQL View Tokens
- Trend View Tokens
- Secure Desktop Tokens
- Report Selector Tokens

6.1 Alarm View Tokens

Exclusion of any Token means the item will not appear on the Alarm View's context menu when the User or members of the User Group are logged into OpenEnterprise.



6.1.1 Acknowledge

This Token enables the User to acknowledge selected alarms by accessing the Acknowledge menu item on the Alarm Client's context menu

6.1.2 Acknowledge All

This Token enables the User to acknowledge all alarms with a single click of the mouse.

6.1.3 Adjust Historical Time Range

When the Alarm Client is configured for historical usage (i.e. as an event log), this Token enables the User to adjust the time range. The User having this Token is able to shorten the time for which the Alarm Client returns event data.

6.1.4 Alarm Client Demand Printing

This Token enables the User to print the whole or a selection of alarms from the Alarm Client window.

6.1.5 Alarm Client Properties

This Token enables the User to access the Property pages of the Alarm Client in Runtime mode and make configuration changes.

6.1.6 Column Alias

This Token allows the User to specify aliases for the column headings within the Alarm Client. When the User right clicks on a column heading a text box is displayed. The User types the name of the alias into this and the alias replaces the real column name.

6.1.7 Create Event

This Token enables the User to create a new event within the Event Log. The User has to select a current event, and is then able to 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.

6.1.8 Disable Audio Alert

This Token enables the User to disable the audible alert on the Sound page of the Alarm Client Property pages. If the User is given this Token, they must also be given the Alarm Client Properties.

6.1.9 Event Log Editing (High)

This Token lists the Event Log fields that the user 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.

6.1.10 Event Log Editing (Medium)

With this Token included, the attributes that may be changed when creating an event are: -

description, alarmtext, devicename, base, extension, helptext, operatortext.

6.1.11 Event Log Editing (Low)

With this Token, the User may edit the description attribute of the selected 'copy' event when creating a new event.

6.1.12 Exceed Current Historical Time Range

With this Token, the User may exceed the currently set Historical Time Range on an Alarm Client configured for Historical (i.e. event) viewing.

6.1.13 Export Data

With this Token, the User may export the 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 a Ms Excel spreadsheet.

6.1.14 Modify Filter

With this Token the User can modify the Filters applied to the Alarm Client. Without it the **[Modify]** button on the Filter Page of the Alarm Client Property Pages is disabled. The User must have the Alarm Client - Properties Token to be able to use this one.

6.1.15 Refresh

This Token enables the User to refresh the data being displayed by the Alarm Client. If the Alarm Client is configured for Historical (i.e. events) display, then a new query is initiated.

6.1.16 Resize Columns

With this Token, the User is able to resize the columns of the Alarm Client.

6.1.17 Silence

With this Token the User can select an alarm and silence it if it is set to create a sound.

6.1.18 Silence All

This Token enables the User to silence all current alarms that are set to sound. As new alarms come in, they will begin to sound.

6.1.19 Suppression

This Token enables the User to suppress selected alarms. This means that the alarm is still in the Alarm Summary, but 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.

6.1.20 Suppression All

This enables a User to suppress all alarms.

6.1.21 Timed Mute

This Token enables a User to apply a timed suppression of alarm annunciation.

6.1.22 Timed Suppression

This Token enables a User to suppress 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.

6.1.23 Unsuppress

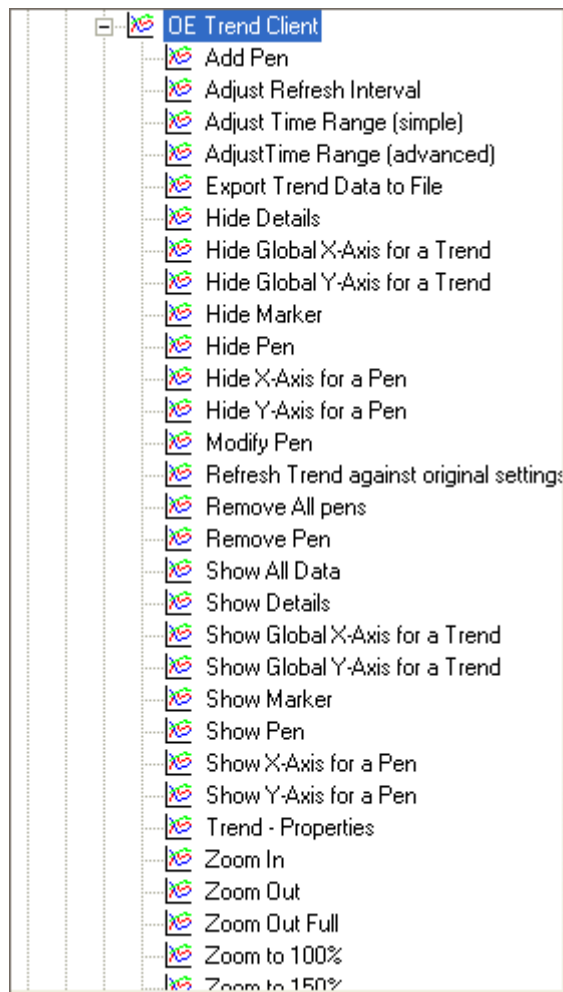
This Token enables a User to immediately unsuppress a previously suppressed alarm.

6.1.24 Unsuppress All

This Token enables a User to immediately unsuppress all previously suppressed alarms.

6.2 Trend View Tokens

All of the following Tokens are used in Runtime mode unless stated.



6.2.1 Add Pen

This Token enables the User to add a new Pen to a Trend View.

6.2.2 Adjust Refresh Interval

If a User has this Token, they can change the refresh rate of the Trend View.

6.2.3 Adjust Time Range (Simple)

This Token enables a Runtime context menu item that allows the User to change the Start Time and the Range of the Trend View window (i.e. the trend can be made to retrieve more or less data).

6.2.4 Adjust Time Range (Advanced)

This Token gives the User access to the Advanced button on the Trend View's Data Page. This allows the User to change the Data Collection Interval, Number of Samples per Pen and Maximum Pages of Data for the trend. This feature is only used in Configure mode.

6.2.5 Export Trend Data to File

This Token enables the User to export 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.

6.2.6 Hide Details

This Token enables a context menu item that allows a User to hide the Pen Details window, which by default appears at the bottom of the Trend View window.

6.2.7 Hide Global X-Axis for a Trend

This Token gives the User the ability from a context menu to hide the Trend's Global X-Axis.

6.2.8 Hide Global Y-Axis

This Token enables a User to hide the Global Y-Axis of a Trend

6.2.9 Hide Marker

With this Token the User can choose to hide the Marker bar for the Trend.

6.2.10 Hide Pen

This Token enables the User to hide any Pen selected from the Trend Details pane.

6.2.11 Hide X-Axis for Pen

With this Token the User can select a Pen from the Details pane and hide its individual X-Axis.

6.2.12 Hide Y-Axis for Pen

With this Token the User can select a Pen from the Details pane and hide its individual Y-Axis.

6.2.13 Modify Pen

This Token enables the User to perform limited Pen modification whilst in Runtime mode.

6.2.14 Refresh Trend Against Original Settings

This Token enables a User to refresh a Trend using the original settings of the Trend

6.2.15 Remove All Pens

With this Token the User is able to remove all Pens from the trend

6.2.16 Remove Pen

This Token enables the User to remove a Pen selected in the Details pane.

6.2.17 Show All Data

Controls the 'Show All Data' context menu item, available from the Trend Graph pane. The 'Show All Data' menu item allows the user to display all data for a Trend that has Trend optimization configured. Unless the user has this token, the option not appear on the context menu. For more information on Trend optimization refer to the Trend documentation.

6.2.18 Show Details

This Token enables the User to show the Details window after it has been hidden.

6.2.19 Show Global X-Axis for a Trend

With this Token the User is able to show the Global X-Axis if it has been hidden.

6.2.20 Show Global Y-Axis for a Trend

With this Token the User is able to show the Global Y-Axis if it has been hidden.

6.2.21 Show Marker

This Token enables the User to show the Trend Marker line if it has been hidden.

6.2.22 Show Pen

With this Token the User is able to re-show a Pen that has been hidden.

6.2.23 Show X-Axis for a Pen

This Token enables the User to show the individual X-Axis for a Pen selected within the Details pane.

6.2.24 Show Y-Axis for a Pen

This Token enables the User to show the individual Y-Axis for a Pen selected within the Details pane.

6.2.25 Trend - Properties

This Token enables the User to access the Trend's Properties context menu in Configuration mode.
This enables full configuration of the Trend View.

6.2.26 Trend View - Demand Printing

This Token enables the User to print the contents of a Trend View window, whilst it runs in the OEDesktop.

6.2.27 Zoom In

This Token enables the User to Zoom in by a margin of 50%.

6.2.28 Zoom Out

This Token enables the User to Zoom out by a margin of 50%.

6.2.29 Zoom Out Full

The User is able to zoom out to the original setting from any magnification.

6.2.30 Zoom to 100%

This has the effect of zooming out to the original setting.

6.2.31 Zoom to 150%

Sets the Trend's magnification to the setting indicated.

6.2.32 Zoom to 25%

Sets the Trend's magnification to the setting indicated.

6.2.33 Zoom to 250%

Sets the Trend's magnification to the setting indicated.

6.2.34 Zoom to 50%

Sets the Trend's magnification to the setting indicated.

6.2.35 Zoom to 75%

Sets the Trend's magnification to the setting indicated.

6.2.36 Zoom to Custom

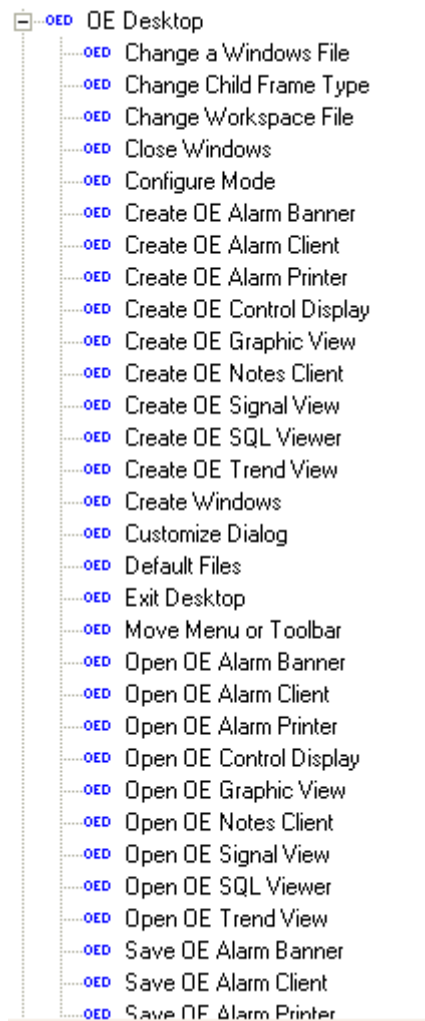
The User is able to Set the Trend's magnification to a custom setting.

6.2.37 Zoom Undo

This moves the Trend's magnification back to the previous setting.

6.3 OEDesktop Tokens

These are the application Tokens belonging to the OEDesktop.



6.3.1 Change a Windows File

A User needs this token to change the file within an open window in the OEDesktop. For example, if a window displaying a trend file was open in the OEDesktop, the User could only open a different trend file into the same window if they had the "Change a Windows File" Token.

6.3.2 Change Child Frame Type

With this Token the User is able to change the window type of window within the OEDesktop by right clicking on its Title Bar and accessing the window type context menu.

6.3.3 Change Workspace File

This Token gives the User the ability to change the OEDesktop file.

6.3.4 Configure Mode

This Token enables the User to enter Configure mode for the OEDesktop or any View Component within the OEDesktop.

6.3.5 Create Alarm Banner

This Token enables the User to access the OEDesktop's New menu item and create a new Alarm Banner.

6.3.6 Create Alarm Client

This Token enables the User to access the OEDesktop's New menu item and create a new Alarm View.

6.3.7 Create Alarm Printer

This Token enables the User to access the OEDesktop's New menu item and create a new Alarm Printer View.

6.3.8 Create OEControl Display

This Token enables the User to access the OEDesktop's New menu item and create a new OEControl Display.

6.3.9 Create Graphic View

This Token enables the User to access the OEDesktop's New menu item and create a new Graphic View.

6.3.10 Create Notes View

This Token enables the User to access the OEDesktop's New menu item and create a new Notes View.

6.3.11 Create Signal View

This Token enables the User to access the OEDesktop's New menu item and create a new Signal View.

6.3.12 Create SQL Viewer

This Token enables the User to access the OEDesktop's New menu item and create a new SQL View.

6.3.13 Create Trend View

This Token enables the User to access the OEDesktop's New menu item and create a new Trend View.

6.3.14 Create or Close Window

A User must have this Token to be able to create a new window within the OEDesktop or close down any child window within the OEDesktop.

6.3.15 Customize Dialog

This Token enables the User to access the Customize menu option, which belongs to the OEDesktop's File menu. The User is then able to configure the OEDesktop.

6.3.16 Exit Desktop

Without this Token the User cannot exit the OEDesktop application.

6.3.17 Move Menu or Toolbar

The User with this Token is able to change the position of the OEDesktop Menu bar and/or Toolbar.

6.3.18 Open Alarm Banner

This Token enables the User to open a previously saved Alarm Banner file into the OEDesktop.

6.3.19 Open Alarm Client

This Token enables the User to open a previously saved Alarm View file into the OEDesktop.

6.3.20 Open Alarm Printer

This Token enables the User to open a previously saved Alarm Printer file into the OEDesktop.

6.3.21 Open Control Display

This Token enables the User to open a previously saved OEControl Display file into the OEDesktop.

6.3.22 Open Graphic View

This Token enables the User to open a previously saved OEGraphic View file into the OEDesktop.

6.3.23 Open Notes Client

This Token enables the User to open a previously saved Notes View file into the OEDesktop.

6.3.24 Open Signal View

This Token enables the User to open a previously saved Signal View file into the OEDesktop.

6.3.25 Open SQL Viewer

This Token enables the User to open a previously saved SQL View file into the OEDesktop.

6.3.26 Open Trend View

This Token enables the User to open a previously saved Trend View file into the OEDesktop.

6.3.27 Save Alarm Banner

This Token enables the User to save a configured Alarm Banner file from within the OEDesktop.

6.3.28 Save Alarm Client

This Token enables the User to save a configured Alarm Client file from within the OEDesktop.

6.3.29 Save Alarm Printer

This Token enables the User to save a configured Alarm Printer file from within the OEDesktop.

6.3.30 Save OEControl Display

This Token enables the User to save a configured OEControl Display file from within the OEDesktop.

6.3.31 Save Graphic View

This Token enables the User to save a configured Graphic View file from within the OEDesktop.

6.3.32 Save Notes Client

This Token enables the User to save a configured Notes View file from within the OEDesktop.

6.3.33 Save Signal View

This Token enables the User to save a configured Signal View file from within the OEDesktop.

6.3.34 Save SQL Viewer

This Token enables the User to save a configured SQL View file from within the OEDesktop.

6.3.35 Save Trend View

This Token enables the User to save a configured Trend View file from within the OEDesktop.

6.3.36 Toggle Status Bar

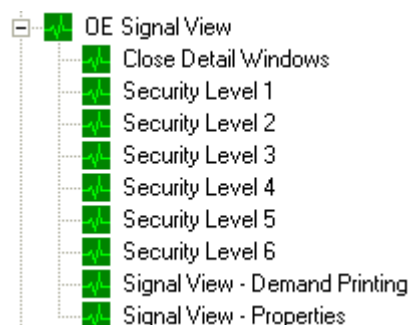
This Token enables the User to hide or show the Status bar for the OEDesktop and its child windows.

6.3.37 Toggle Toolbar

This Token enables the User to hide or show the OEDesktop Toolbar.

6.4 Signal View Tokens

These are the application Tokens available for use with the Signal View component.



6.4.1 Close Detail Windows

This Token enables the User to close all of the Signal details windows at once.

6.4.2 Security Level 1 - 6

Each of the Security Level Tokens represents a level of security within the Open BSI Netview application. Higher Security Levels represent greater privileges.

6.4.3 Signal View - Demand Printing

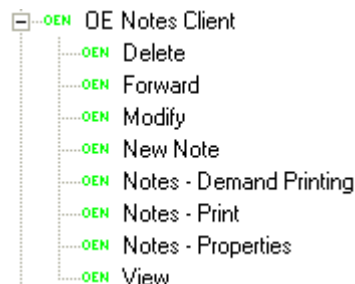
This Token gives the User the ability to print the Signal View window.

6.4.4 Signal View - Properties

This Token enables the User to access the Signal View's Property Pages whilst in Configure mode.

6.5 Notes View Tokens

These are the application Tokens which are available for the Notes View component.



6.5.1 Delete

The User with this Token can delete a selected Note.

6.5.2 Forward

This Token enables the User to forward Notes.

6.5.3 Modify

This Token enables the User to Modify Notes.

6.5.4 New Note

The User with this Token is able to create New Notes.

6.5.5 Notes - Demand Printing

This Token enables the User to print the contents of the Notes window.

6.5.6 Notes - Print

This Token enables the User to print a selected Note.

6.5.7 Notes - Properties

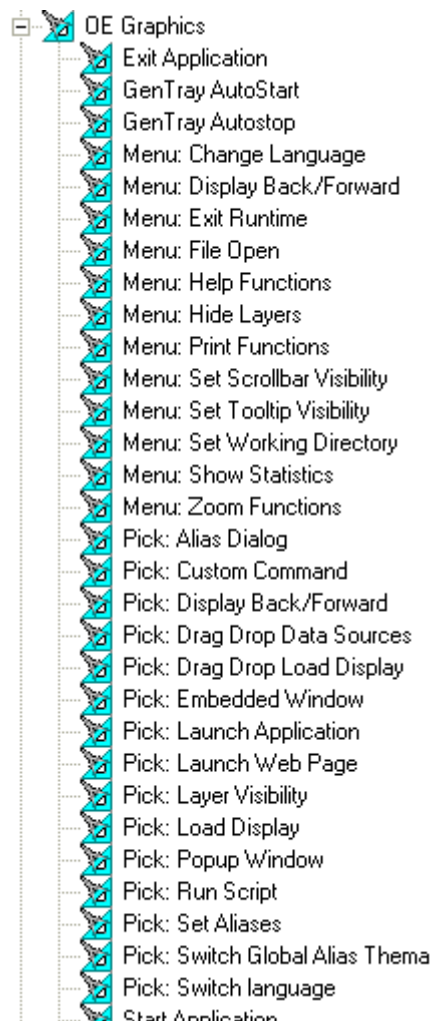
The User who has this Token is able to access the Property Pages of the Note View when in Configuration mode.

6.5.8 View

The User must have this Token to view individual Notes that are displayed within the Notes View window.

6.6 Graphics View Tokens

Some of the Graphics View Menu Tokens (prefaced **Menu:**) only affect the Graphics application when it is run 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.



6.6.1 Exit Application

This Token enables a User to exit 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.

6.6.2 GenTray AutoStart

This Token gives the User the ability to Auto-Start the Graphics View application with the GenTray utility. This Token is only relevant when starting the OpenEnterprise Graphics View application outside of the OEDesktop environment.

6.6.3 GenTray AutoStop

This Token gives the User the ability to Auto-Stop the Graphics application with the GenTray utility when it is running outside of the OEDesktop environment.

6.6.4 Menu: Change Language

This Token gives the User the ability to change the language of the Graphics application. It is not recommended to assign this Token to normal Users of the OpenEnterprise application.

6.6.5 Menu: Display Back/Forward

This Token enables the User to move backwards or forwards through a series of configured displays. Since display navigation is best achieved through OEMenus, it is not recommended to use this method.

6.6.6 Menu: Exit Runtime

The User must have this Token to be able to switch the display into Configure mode when running the Graphics application outside of the OEDesktop environment. When running within the OEDesktop environment, the OEDesktop's Configure Mode Token enables Users to switch all Views into Configure mode.

6.6.7 Menu: File Open

Gives access to the Graphics View File/Open menu item. It is not relevant if the OEDesktop File/Open menu item is available.

6.6.8 Menu: Help Functions

Gives access to context sensitive Graphics View Help.

6.6.9 Menu: Hide Layers

Gives access to the Graphics View Hide Layers menu item.

6.6.10 Menu: Print Functions

Gives access to the Graphics View Print menu functions when the Graphics application is run outside of the OEDesktop. When being run within the OpenEnterprise Desktop the OEDesktop File Menu has an option to print any View window that is selected. The OEDesktop File menu is displayed by default, but can be hidden from the Menu tab of the OEDesktop's Property pages (accessed from the **Desktop>Customize...** menu item).

6.6.11 Menu: Set Scrollbar Visibility

Gives access to the Graphics View "Set Scrollbar Visibility" menu item.

6.6.12 Menu: Set Tooltip Visibility

Gives access to the Graphics View "Set Tooltip Visibility" menu item.

6.6.13 Menu: Set Working Directory

Provides access to the Graphics View "Set Working Directory" menu item.

6.6.14 Menu: Show Statistics

Provides access to the Graphics View "Show Statistics" menu item, which gives display statistics.

6.6.15 Menu: Zoom Functions

Provides access to the Graphics View Zoom menu items.

6.6.16 Pick: Alias Dialog

This Token enables the User to access a Pick action object which displays the Alias Dialog, so that aliases can be edited.

6.6.17 Pick: Custom Command

The most important of the Pick commands from an OpenEnterprise perspective. This Token enables the User to access any Graphics View Pick action object that uses a Custom Command. The Custom Command provides access to OEMenus and the OEMenus editor interface.

6.6.18 Pick: Display Back/Forward

This Token enables the User to access any Graphics Pick action object that uses the Display Back/Forward commands.

6.6.19 Pick: Drag Drop Data Sources

A User with this Token can access any Graphics View Pick action object that uses the Drag Drop Data Sources functionality.

6.6.20 Pick: Drag Drop Load Display

A User with this Token can access any Graphics View Pick action object that uses the Drag Drop Load Display functionality.

6.6.21 Pick: Embedded Window

A User with this Token can access any Graphics View Pick action object that uses the Embedded Window functionality.

6.6.22 Pick: Launch Application

A User with this Token can access any Graphics View Pick action object that uses the Launch Application functionality.

6.6.23 Pick: Layer Visibility

A User with this Token can access any Graphics View Pick action object that uses the Layer Visibility functionality.

6.6.24 Pick: Load Display

A User with this Token can access any Graphics View Pick action object that uses the Load Display functionality.

6.6.25 Pick: Popup Window

A User with this Token can access any Graphics View Pick action object that uses the Popup Window functionality.

6.6.26 Pick: Run Script

A User with this Token can access any Graphics View Pick action object that uses the Run Script functionality.

6.6.27 Pick: Set Aliases

A User with this Token can access any Graphics View Pick action object that uses the Set Aliases functionality.

6.6.28 Pick: Switch Language

A User with this Token can access any Graphics View Pick action object that uses the Switch Language functionality.

6.6.29 Start Application

A User with this Token can access the Graphics View Start Application functionality.

6.6.30 Tab Load Display

A User with this Token can access the Graphics View Tab Load Display functionality.

6.6.31 Graphics View File Token: Layers

Please note, 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 only applies to the Graphics View component of OpenEnterprise, therefore it is mentioned here.

To enable security on layers within Graphics displays add a File Token which uses the following format:-

- <Filename>|<Layername>

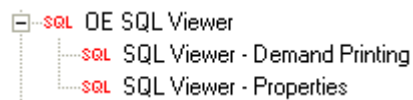
Then include this File Token in the Security configuration for any users who should have access to that layer.

For example, if you have a display called "PumpRoom.gdf", and a layer that is named "SecretLayer", you would create a new File Token (see the "Creating Custom, File and OPC Item Tokens" topic). The name of this Token would be:-

- PumpRoom.gdf|SecretLayer

6.7 SQL View Tokens

These are the application Tokens available for the SQL View component.



6.7.1 SQL Viewer - Demand Printing

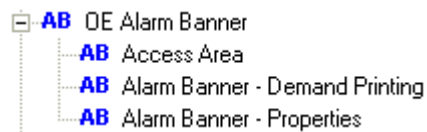
This Token enables the User to print the contents or a selection of the contents of any OEDesktop window containing an SQL Viewer file.

6.7.2 SQL Viewer - Properties

This Token enables the User to access the Properties menu to display the SQL Viewer Property Pages in Configure mode.

6.8 Alarm Banner Tokens

These are the application Tokens available for the Alarm Banner.



6.8.1 Access Area

This Token enables the User to access the menu item that provides a filter on the Alarm Banner based on access area.

6.8.2 Alarm Banner - Demand Printing

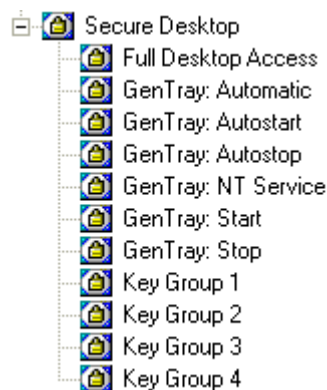
This Token enables the User to print the contents or a selection of the contents of any OEDesktop window containing an Alarm Banner file.

6.8.3 Alarm Banner - Properties

This Token enables the User to access the Properties menu to display the Alarm Banner's Property Pages in Configure mode.

6.9 Secure Desktop Tokens

The Secure Desktop Tokens provide or deny access to the Windows Desktop for an OpenEnterprise user.



6.9.1 Full Desktop Access

Anyone having this token in their include list will be able to access all of the normal Windows Desktop features, including the System keys (i.e Ctrl-Alt-Delete, the Windows key to activate the Start button, the System Tray etc.).

Anyone not having this token or having it in their exclude list will not be able to access normal Windows Desktop functionality. They will be able to use the Ctrl-Alt-Delete combination to bring up the **Windows Security** dialog, but all buttons on it except for the **Cancel** button will be disabled.

6.9.2 GenTray: Automatic

Controls whether users will be able to select the option to make Secure Desktop an Automatic Windows service from the GenTray icon on the Windows System bar when logged into OpenEnterprise. This option is only available if the Secure Desktop has already been designated as a Windows service.

6.9.3 Gentry: Autostart

Controls whether users will be able to select the option to make Secure Desktop start automatically when a user logs into OpenEnterprise. This option is available from the Gentry icon on the Windows System bar when logged into OpenEnterprise.

6.9.4 Gentry: Autostop

Controls whether users will be able to select the option to make Secure Desktop stop automatically when a user logs out of OpenEnterprise. This option is available from the Gentry icon on the Windows System bar when logged into OpenEnterprise.

6.9.5 Gentry: NT Service

Controls whether users will be able to select the option to make Secure Desktop a Windows service from the Gentry icon on the Windows System bar when logged into OpenEnterprise.

6.9.6 Gentry: Start

Controls whether users will be able to start Secure Desktop from the Gentry icon on the Windows System bar when logged into OpenEnterprise.

6.9.7 Gentry: Stop

Controls whether users will be able to stop Secure Desktop from the Gentry icon on the Windows System bar when logged into OpenEnterprise.

6.9.8 Keygroup 1

Any users having this token will be able to access the keyboard keys specified in this Keygroup when logged into OpenEnterprise. Any users not having this token will not be able to access these keys.

6.9.9 Keygroup 2

Any users having this token will be able to access the keyboard keys specified in this Keygroup when logged into OpenEnterprise. Any users not having this token will not be able to access these keys.

6.9.10 Keygroup 3

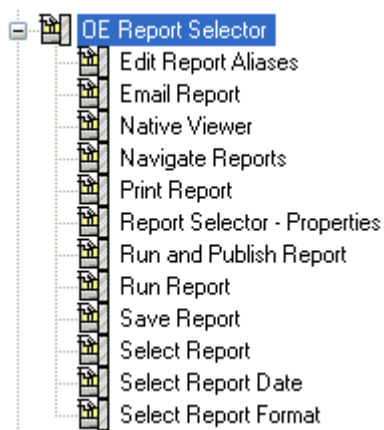
Any users having this token will be able to access the keyboard keys specified in this Keygroup when logged into OpenEnterprise. Any users not having this token will not be able to access these keys.

6.9.11 Keygroup 4

Any users having this token will be able to access the keyboard keys specified in this Keygroup when logged into OpenEnterprise. Any users not having this token will not be able to access these keys.

6.10 Report Selector Tokens

The Report Selector Tokens provide access to functional options within the Report Selector View.

**6.10.1 Edit Report Aliases**

Enables the user to edit the alias values for the report.

6.10.2 Email Report

Allows the user to email the report.

6.10.3 Native Viewer

Enables the user to launch the report in its native viewer.

6.10.4 Navigate Reports

Enables the user to navigate reports using the next/previous buttons.

6.10.5 Print Report

Enables the user to print a report.

6.10.6 Report Selector - Properties

Enables the user to configure the report selector.

6.10.7 Run and Publish Report

Enables the user to run and publish a report.

6.10.8 Run Report

Enables the user to run a report.

6.10.9 Save Report

Enables the user to save a report to a different location.

6.10.10 Select Report

Enables the user to select a report using the report selector drop-down list.

6.10.11 Select Report Date

Allows the user to select a date for the report.

6.10.12 Select Report Format

Enables the user to select a report format using the format drop-down list.

7 Index

A

Access Area	73
Access Area Field	47
Access Area Tokens	33
Access Areas	43
Access Areas Tab	54
Accessed Check Box	59, 61, 63, 65
Account Disabled	47
Account Lockout	47, 52
Account Tab	50
Add Access Area Button	55
Add Button	67
Adding	41
Alarm View Tokens	75
All Users	41
Already	73
Apply Logout Per Database Connection	53
Associated Access Areas	55
Auto Logout Section	53
Available Access Areas	55
Available Tokens	56, 58, 60, 62, 64, 66

B

Breaking Token Links	43
Browse Dialog	68

C

Cannot Remove SYSTEM User	73
Change Password	47
Component Column	66
Configured Tokens List Token Groups	67
Confirm on Deletion	73
Confirm on Moving User	73
Confirm on Removing User	73
Creating	18, 19, 20, 21, 22, 24, 26, 33, 35, 36, 37, 38, 39
New Access Areas	22, 33, 39
New Application Tokens	39
New Token Groups	21, 37
New User	19, 24, 35
New User Groups	18, 26, 36
Simple String Type Tokens	20, 38
Current Group	73
Custom	43
Custom Token Tab Dialog	57

Custom Tokens	31
---------------------	----

D

Default Group Properties Dialog	49
Default User Settings	40
Deleting	44
Description Field	46

E

Exclude Button	57, 58, 60, 62, 64
Exclude List	59, 61, 63, 65
Expires In	51
Expiry Warning	51

F

Failed Logon Attempts Before Lockout	53
Number	53
File Button	70
Save	70
Full Name Field	46

G

Glossary	9
Terms	9
Grantor	47
Graphics View Tokens	85
Group	41, 73
Group Icons	28
Groups	9, 42

I

Iconics Security Server	9
Include Button	56, 58, 60, 62, 64
Include List	58, 60, 62, 64

L

Limiting	13
Toolbox Table Mode	13
Linking	42
Tokens	42
List Pane	34
Lockout Duration	53
Login Checkbox	48
Logout After Inactivity	53
Logout File Precedence	48
Logout Fixed Period	53

M

Maximum Length.....	52
Member	73
Already	73
Message Suppression Options Dialog.....	71, 72
Minimum Age	52
Minimum Length.....	52
Modifying.....	40, 42, 43
Access Areas.....	43
Custom	43
Default User Settings.....	40
Token Groups.....	42
User Account Settings.....	40

N

New Access Areas	22, 33, 39
Creating	22, 33, 39
New Application Tokens.....	39
Creating	39
New Group	73
Current Group.....	73
New Token Groups	21, 37
Creating	21, 37
New User.....	19, 24, 35, 41
Adding	41
Creating	19, 24, 35
New User Groups.....	18, 26, 36
Creating	18, 26, 36
Next Logon Field	47
Number.....	53
Failed Logon Attempts Before Lockout	53

O

ODBC.....	52
Refuse Login When Password Expires.....	52
OE Components.....	51
Refuse Login When Password Expires.....	51
OEDesktop Login	48
OELogin Client.....	8
OESecurity Concepts.....	9
OESecurity Config Tool Interface	16
OESecurity Config Tool Overview	34
OESecurity Configuration Tool.....	9
OESecurity Manager.....	8
OESecurity Menu Bar	17
OESecurity Tool Edit Menu.....	18
OESecurity Tool File Menu	17
OESecurity Tool Help Menu.....	22
OESecurity Tool Tools Menu	22

OPC Item Tab Dialog.....	61
OPC Item Tokens	32
OPC Tokens	43
Overview	8

P

Parent Group	48
Password Age Section.....	52
Password Field	46
Password Length Section	52

R

Refuse Login When Password Expires	51, 52
ODBC	52
OE Components.....	51
Remove Access Area	55
Remove Button	56, 58, 60, 62, 64
Remove Tokens Button	67
Removing.....	41
All Users.....	41

S

Save.....	70
File Button	70
Sec File	9
Security Objects.....	44
Deleting	44
Simple String Type Tokens.....	20, 38
Creating.....	20, 38
SQL Components	52
Summary List.....	54
System Administrator.....	47

T

Terms.....	9
Glossary	9
Test String.....	57, 59, 61, 63, 65
Token Access Area.....	66, 67
Token Description	67
Token Drag Exclude	71
Token Drag Include.....	71
Token Group	42
Token Group Description	66
Token Group Icons	29
Token Group Name	66
Token Group Property Dialog	65
Token Group Tab.....	63
Token Groups	42

<i>Modifying</i>	<i>42</i>
<i>Token Icons.....</i>	<i>28, 30</i>
<i>Token Name.....</i>	<i>67</i>
<i>Token Pattern Matching.....</i>	<i>13</i>
<i>Token Properties Dialog.....</i>	<i>67</i>
<i>Token Summary Dialog.....</i>	<i>68</i>
<i>Token Tab Dialog.....</i>	<i>56, 59</i>
<i>Token Type Section</i>	<i>66</i>
<i>Token Wildcards</i>	<i>13</i>
<i>Tokens.....</i>	<i>11, 31, 42</i>
<i> Linking</i>	<i>42</i>
<i>Toolbox Table Mode</i>	<i>13</i>
<i> Limiting</i>	<i>13</i>
<i>Tree Pane.....</i>	<i>23</i>

U

<i>User</i>	<i>73</i>
<i>User Account Settings</i>	<i>40</i>
<i> Modifying.....</i>	<i>40</i>
<i>User Cannot Change Password</i>	<i>47</i>
<i>User Configured Token Groups.....</i>	<i>30</i>
<i>User Icons.....</i>	<i>25</i>
<i>User Name Field.....</i>	<i>46</i>
<i>User Properties Dialog.....</i>	<i>45</i>
<i>User Summary Tab Dialog</i>	<i>53</i>
<i>Users.....</i>	<i>9, 42</i>

V

<i>Verify Password Field.....</i>	<i>46</i>
-----------------------------------	-----------

Reference Guide

D301530X412

APRIL 2012

DISCLAIMER

Bristol, Inc., Bristol Babcock Ltd, Bristol Canada, BBI SA de CV and the Flow Computer Division, are wholly owned subsidiaries of Emerson Electric Co. doing business as Remote Automation Solutions ("RAS"), a division of Emerson Process Management. ROC, FloBoss, ROCLINK, Bristol, Bristol Babcock, ControlWave, TeleFlow and Helicoid are trademarks of RAS. AMS, PlantWeb and the PlantWeb logo are marks of Emerson Electric Co. The Emerson logo is a trademark and service mark of the Emerson Electric Co. All other marks are property of their respective owners.

The contents of this publication are presented for informational purposes only. While every effort has been made to ensure informational accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. RAS reserves the right to modify or improve the designs or specifications of such products at any time without notice. All sales are governed by RAS' terms and conditions which are available upon request. RAS does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any RAS product remains solely with the purchaser and end-user.

Engineered and supported by:

Remote Automation Solutions,

Blackpole Road, Worcester, WR3 8YB, UK

Registered office: Meridian East, Leicester, LE19 1UX

Registered in England and Wales, Registration No. 00671801

VAT Reg No. GB 705 353 652

Emerson Process Management
Remote Automation Solutions
1100 Buckingham St
Watertown, CT 06795
T 1 (860) 945 2200
F 1 (860) 945 2278
www.EmersonProcess.com/Remote
binfo@EmersonProcess.com

Emerson Process Management
Remote Automation Solutions
Blackpole Road
Worcester, WR3 8YB
T 44 (0) 1905 856848
F 44 (0) 1905 856930
www.EmersonProcess.com/Remote
oedsupport@EmersonProcess.com

