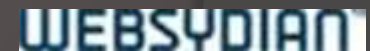
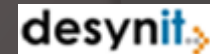
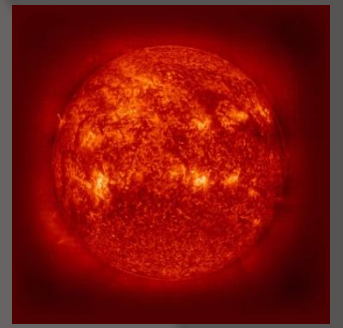


DYNAMICALLY SECURING YOUR CA PLEX APPLICATIONS

Gavin Beangstrom
ARAD Computing

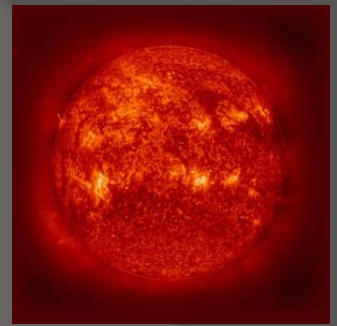


Agenda



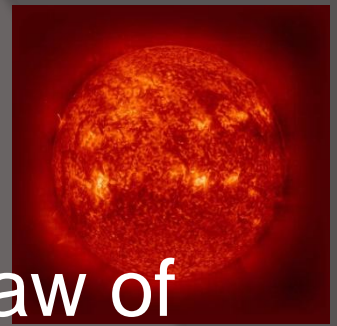
- Company overview
- Overview of functionality
- Data creation and Presentation
- Pattern Implementation
- Future Plans
- Questions

Company Overview



- Company Formed in 2005
- Area of expertise
 - Plex and 2e consulting and development
 - Solution Architecture
 - Enterprise Architecture
 - Hardware provisioning
- Members worked with Plex since 1995 and 2e since 1992

Introduction



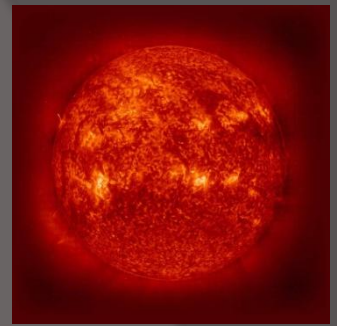
- Application security is a fundamental flaw of most development efforts – Often Overlooked until the end
- Securing your Plex applications should be a simple process
- Provides a complete configurable environment
- Security Model is commercially available
- Current Customers
 - Spar
 - Columbus Stainless



Overview Of Functionality

Features

Overview Of Functionality



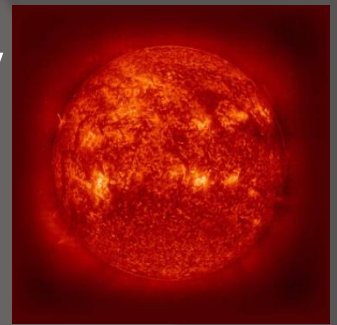
- Group and Role Based authority
- Object level access control
- Secure MDI Parent with dynamic menu building and explorer
- Field level access control
- Event access control
- Segregation of Authority
- Session Management (IBMi)
- Server/Environment Management (IBMi)
- Security Management Console



Overview Of Functionality

Group and Role
Based authority

Group and Role Based authority



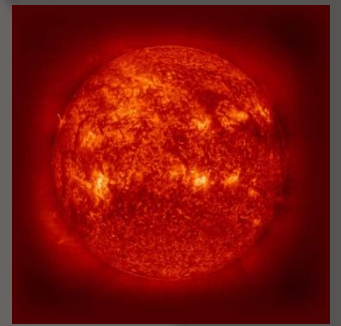
- A **ROLE** can be considered as a process performed within the Business unit or Job
- A **GROUP** can have multiple **ROLES**
- Conversely a **ROLE** can belong to multiple **GROUPS**
- A **GROUP** can be considered as a Business Unit or Job Description



Overview Of Functionality

Object level access
control

Object Level Access Control



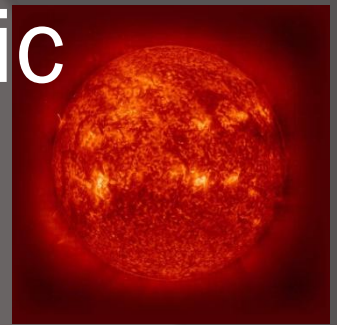
- Access to functions is granted at the object level
- Functions are linked to a ROLE
- A ROLE is linked to a GROUP ROLE
- A GROUP ROLE is linked to a USER
- Access is assigned at the object level to enable integration to other Plex systems, i.e YouEye (Desynit).



Overview Of Functionality

Secure MDI Parent
with dynamic
menu building
and Explorer

Secure MDI Parent With Dynamic Menu Building and Explorer



- An MDI function provides the calling mechanism of the Security Model
- Menus are dynamically built according to the Group Role that the user belongs to
- Users only see Menus that have an authorised function associated with it
- NOTE: Authority is granted at the function level and not the menu level

Secure MDI Parent With Dynamic Menu Explorer

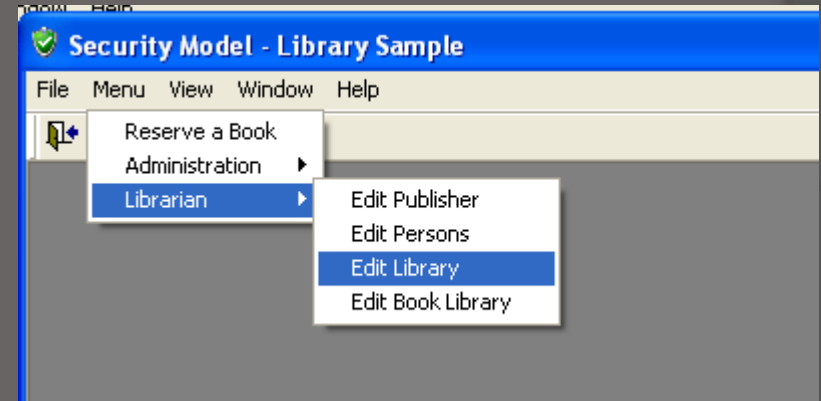
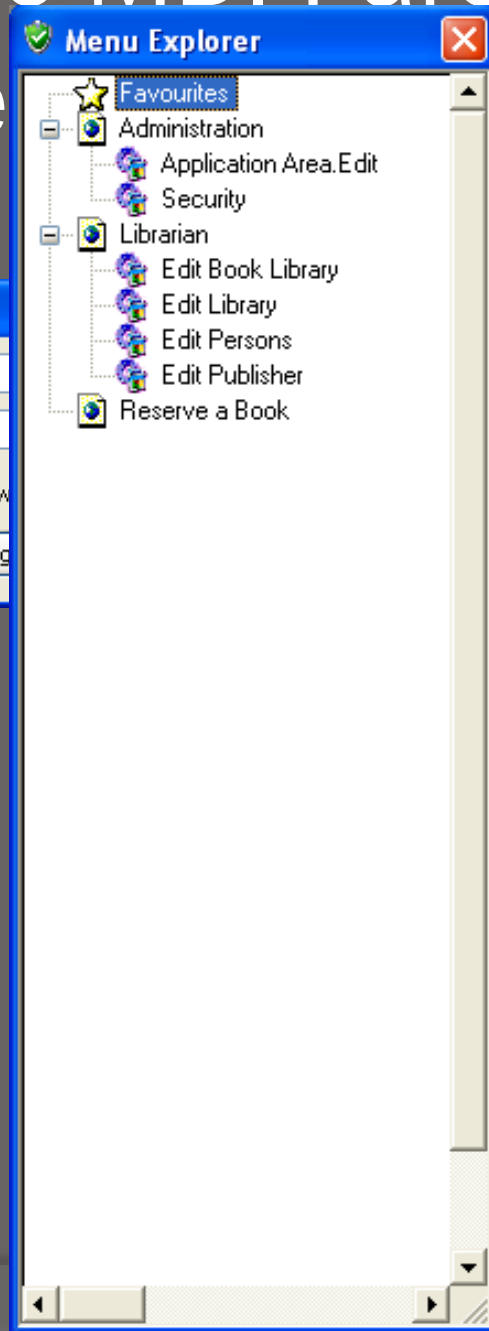
Logon

User ID

Password

Change Password

Log

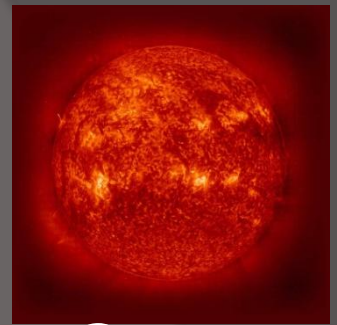




Overview Of Functionality

Field level access
control

Field Level Access Control



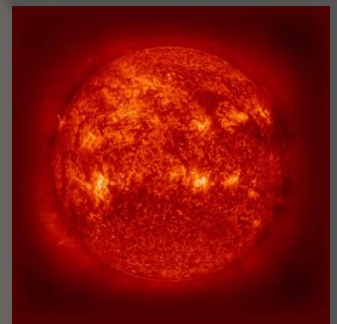
- Field level access control is granted at the Group Level
- Access Levels can be
 - DEFAULT – Keep as is
 - MODIFY – Modify field
 - PASSWORD PROTECTED – Masks field with ‘*’ and makes read only
 - READ ONLY – Cannot modify data



Overview Of Functionality

Event Access Control

Event Access Control



Sub Set button authority

Seq Sample Code

Things to do:

Change "Function: Test Secure Function A" to the function to be checked, drag this directly from the object browser

Set the state of the event attached to your button by adding the code "Set State Default, Event: ButtonCheck" and "Set State Protected, Event: ButtonCheck"

=====
+++Define Field: +FunctionImplementationName

+++Define Field: FIELDS/+Function

Change the function below to your function to be checked

+++Define Function: Test Secure Function A

Change the function below to your function to be checked

+++Set Value Field: FIELDS/+Function, Function: Test Secure Function A

+For Defined Value Field: FIELDS/+Function

+For Each Property FNC impl name NME

+++Set Value To Current Field: +FunctionImplementationName, .Target

++Name Defined Field: +FunctionImplementationName, Local<SEC Function Id>

Call Security Roles List.Fetch.Check Authority

If Local<Authorised> == <Authorised.Yes>

Add this as Code below here, Changing to the correct event : "Set State Default, Event: ButtonCheck"

Else

Add this as Code below here, Changing to the correct event : "Set State Protected, Event: ButtonCheck"

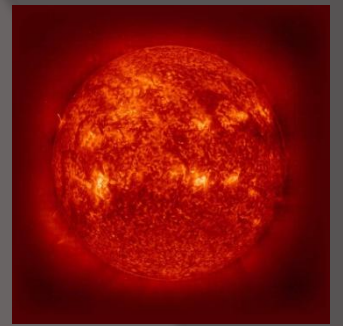
📄 Edit Point Set button authority



Overview Of Functionality

Segregation of
Authority

Segregation of Authority



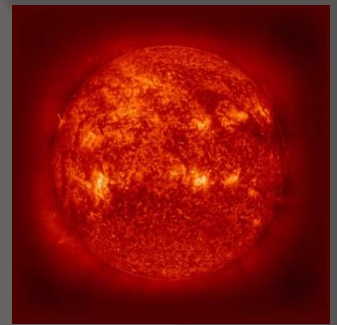
- Administrators are segregated from each other by application areas
- Application areas prevent unauthorised granting of authority across application owner boundaries
- Roles and authorities can be seen but not assigned



Overview Of Functionality

Session
Management
(IBMi)

Session management



Session Management provides an audit trail of

Session Manager

P6_SessionManagement Base Job Log Remote Job Log

Base Job number: 136709 Base User Id: QPGMR Base Job name: YOBSYTCPCT

5722SS1 V5R4M0 060210 Display Job Log CLBDEV 27/05/11 09:27:53

MSGID	TYPE	SEV	DATE	TIME	FROM PGM	LIBRARY	INST	TO PGM	LIE
CPF1124	Information	00	27/05/11	09:25:43.560056	QWTPIIPP	QSYS	0671	*EXT	
Message Job 136709/QPGMR/YOBSYTCPCT started on 27/05/11 at 09:25:43 in subsystem P6SBS00 in P6SBS00. Job entered system on 27/05/11 at 09:25:43.									
CPC2101	Completion	00	27/05/11	09:25:43.817880	QLICHLIB	QSYS	00CF	QC2SYS	QSY
From user : PLEX									
To module : QC2SYS									
To procedure : system									
Statement : 6									
Message : Library list changed.									
Cause : The user library list was replaced by the specified list of libraries.									
CPF2104	Escape	40	27/05/11	09:25:44.447016	QLICHLBL	QSYS	02D5	SCADDSC	P6E
From user : PLEX									
Message : Library P6DEVDTAS not removed from the library list.									
Cause : Library P6DEVDTAS is not in the user portion (typeUSR) of the library list and therefore cannot be removed. Recovery : Display the library list (DSPLIBL command) to determine if the library name specified is correct or if the specified library is in the system portion (typeSYS) of the library list. If the library is a product library (typePRD), the library will be removed when the command completes. If the library									

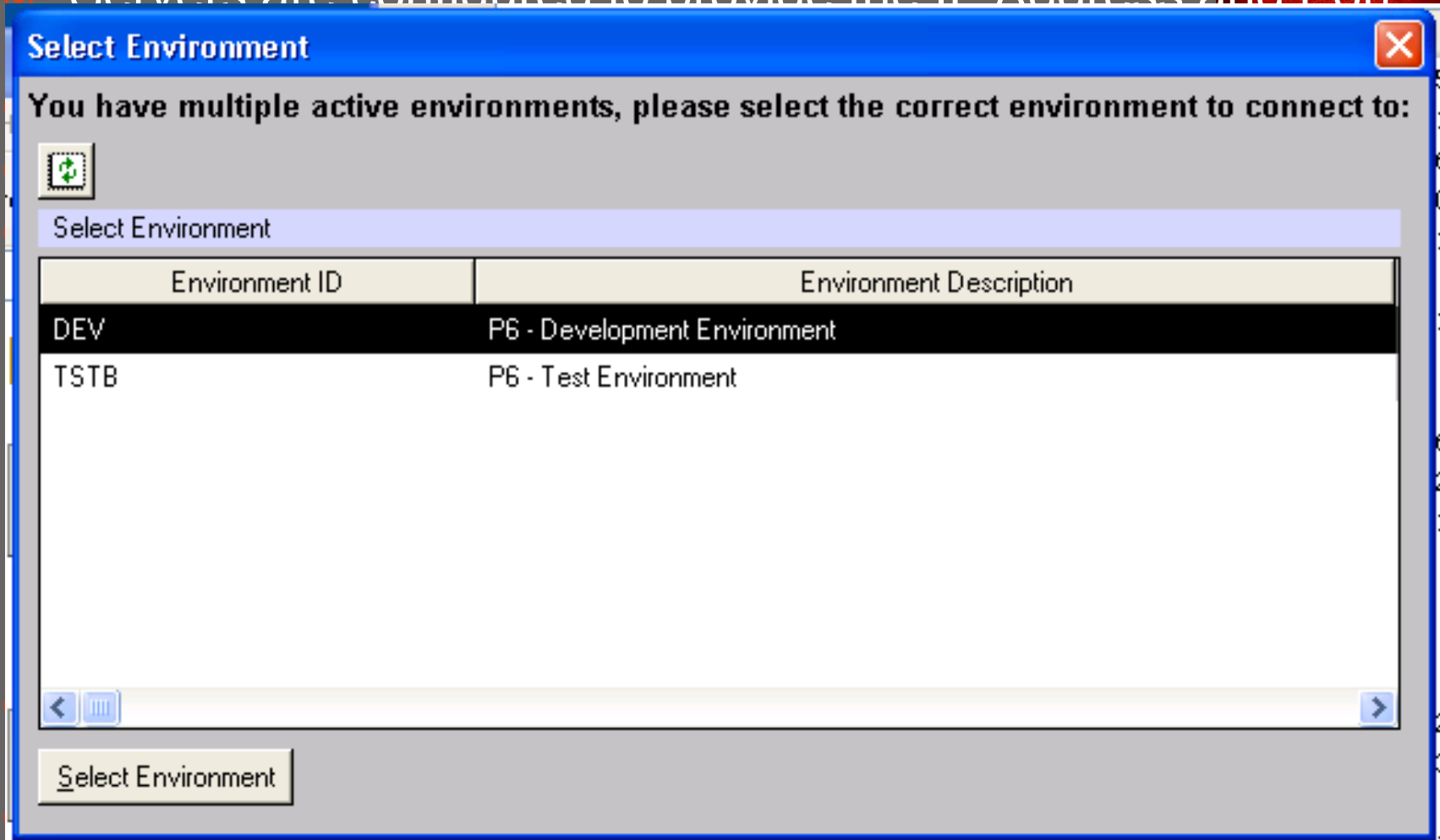


Overview Of Functionality

Server/Environment
Management
(IBMi)

Server/Environment Management

- Servers are configured to provide the IP Address and Port



Select Environment

You have multiple active environments, please select the correct environment to connect to:

Environment ID	Environment Description
DEV	P6 - Development Environment
TSTB	P6 - Test Environment

Select Environment

when logging on.



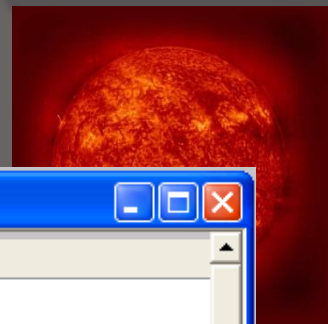
Overview Of Functionality

Security

Management

Console

Security Management Console



P6_Security [Minimize] [Maximize] [Close]

Menu Authority | **Function Authority** | Field Security | Maintain Menu | Functions | Users | Roles | Environments

Group Roles


Role Description
Administration
Commercial Group
No Access

Roles

Authority	Include	Role Description
	<input type="checkbox"/>	Commercial Role
	<input checked="" type="checkbox"/>	ITAdmin
	<input type="checkbox"/>	No Access
	<input type="checkbox"/>	Store Manager
	<input type="checkbox"/>	SuperUserSecurity
	<input checked="" type="checkbox"/>	TCS User
	<input checked="" type="checkbox"/>	UDC Backup
	<input checked="" type="checkbox"/>	UDC Primary

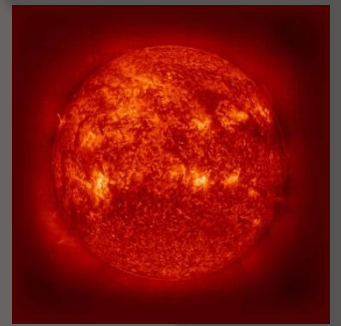
Function **Role Authority**

- Configuration
- Costing
- Formato Maintenance
- General
 - Business Reporting Portal
 - ITAdmin
 - Contact Enquiry
 - ITAdmin
 - TCS User
 - General Help
- IT Admin
- Material Management
- Order Management
- Transportation Management
- TroubleShooting
- User Defined Codes

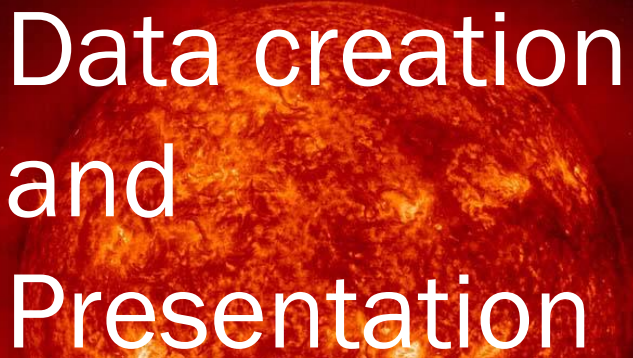


Data creation and Presentation

Data Creation And Presentation



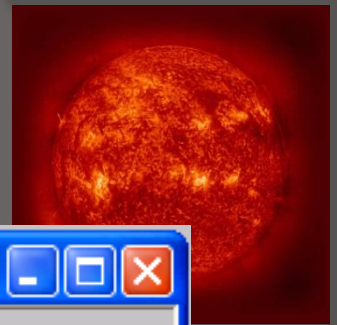
- Servers/Environments
- Roles
- System Users
- Functions
- Maintain Menu
- Field Security
- Function Authority
- Menu Authority
- Segregation of authority



Data creation and Presentation

Servers/
Environments

Server Configuration



Server Maintain

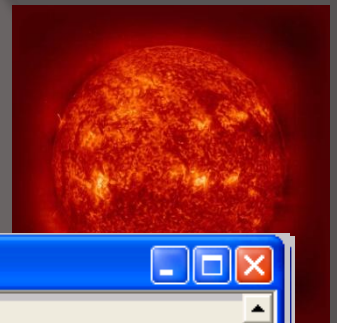
Servers

Server Name	Server Type	Server Description
CLBDEV	IBM i	Development
CLBP6D	IBM i	P6 Development

Server Name: CLBDEV
Server Type: IBM i
Server Description: Development
IP Address: 26.1.28.26
Port: 3789

Apply New Delete Refresh Verify Server

Environments



P6_Security

Menu Authority | Function Authority | Field Security | Maintain Menu | Functions | Users | Roles | **Environments**

Environment | Variables | Paths | **Libraries**

Environment ID:

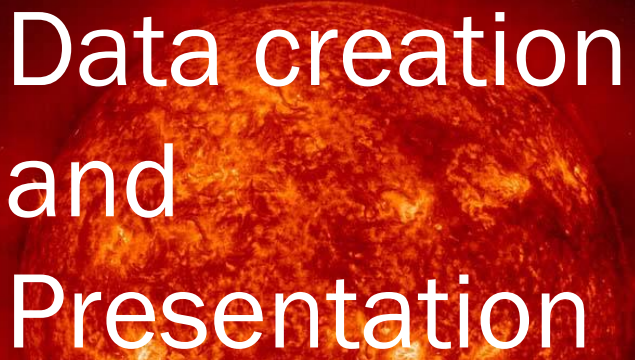
Environment Description:

Library Sequence	Library Name	Library Description
1	P6DEVDB00	P6 Database - IBM iSeries CLBDEV
2	P6DEVFN00	P6 Server Function Library (PLEX Programs)
3	P6DEVUT00	P6 Server Function Library (Non-PLEX Programs)
4	MAXDTACLB	MAX
5	P6DEVDM00	P6 Views to MAXDB
6	LIBHTTP	LIBHTTP

Library Sequence: Library Name:

Library Description:

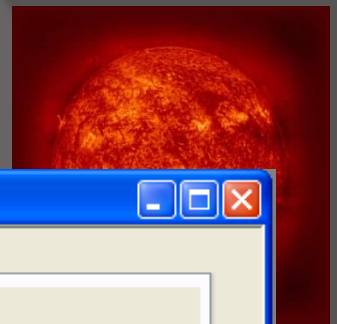
Continue new?



Data creation and Presentation

Roles

Roles



Security

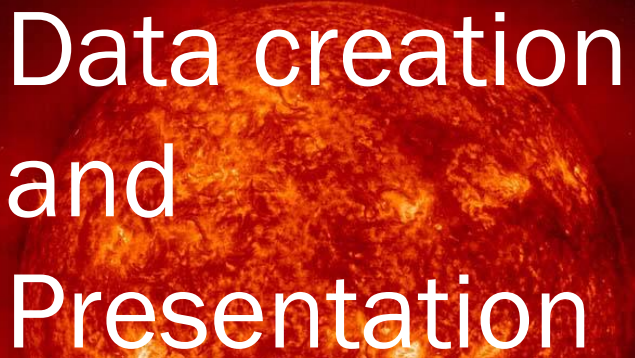
Menu Authority | Function Authority | Field Security | Maintain Menu | Functions | Users | Roles

Role Description: Position:

Role Description	Group Role
Admin	<input type="checkbox"/>
Administrators	<input checked="" type="checkbox"/>
Borrower	<input type="checkbox"/>
Librarians	<input checked="" type="checkbox"/>
Library Worker	<input type="checkbox"/>
Public	<input checked="" type="checkbox"/>

Role Description: Group Role

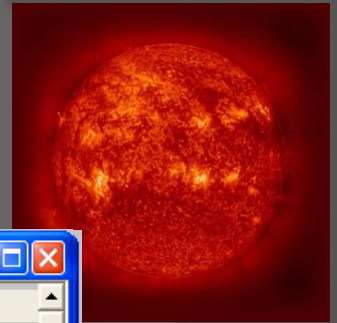
Continue new?



Data creation and Presentation

System Users

Users



P6_Security [Minimize] [Maximize] [Close]

Menu Authority | Function Authority | Field Security | Maintain Menu | Functions | **Users** | Roles | Environments

Edit | **User Environments** | Logon Audit

User ID:

Environment ID	EffectiveDate	ExpiryDate
DEV	0000/00/00	0000/00/00
TSTB	0000/00/00	0000/00/00

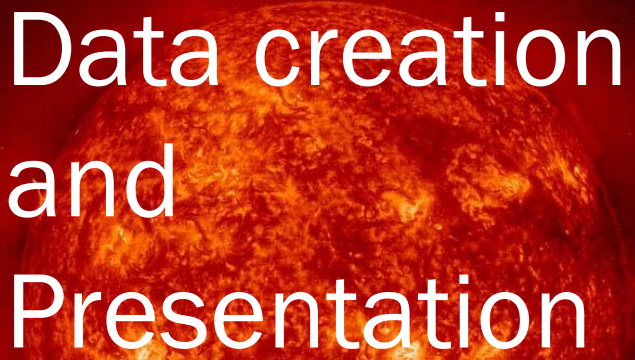
Environment ID:

Environment Description:

EffectiveDate: ExpiryDate:

Continue new?

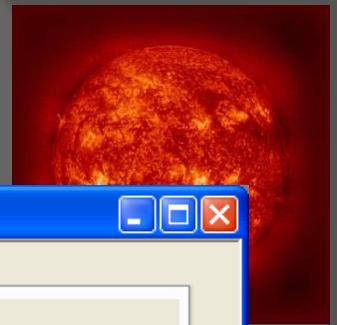
e



Data creation and Presentation

Functions

Functions



Security

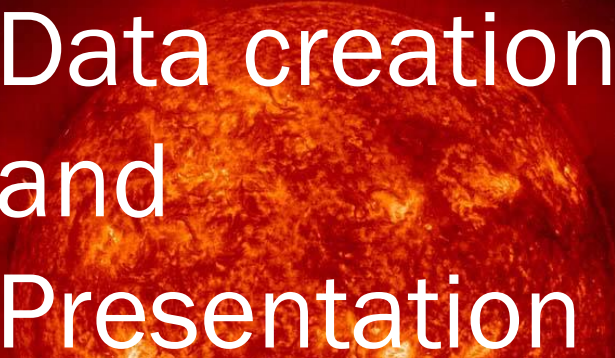
Menu Authority | Function Authority | Field Security | Maintain Menu | **Functions** | Users | Roles

Function ID: Position:

Function ID	Function Description	Secure Panel Generator	Function Type
LB3ZF	Edit Book Library		Client Server
LB5FF	Edit Library		Client Server
LB6KF	Edit Persons	AA2F	Client Server
LB6ZF	Edit Publisher		Client Server
LB8JF	Reserve a Book		Client Server
SC34F	Application Area.Edit		Client Server
SC_Admin	Security		Client Server

Function ID:
Function Description: Secure Panel Generator:
Function Type:

Continue new?



Data creation and Presentation

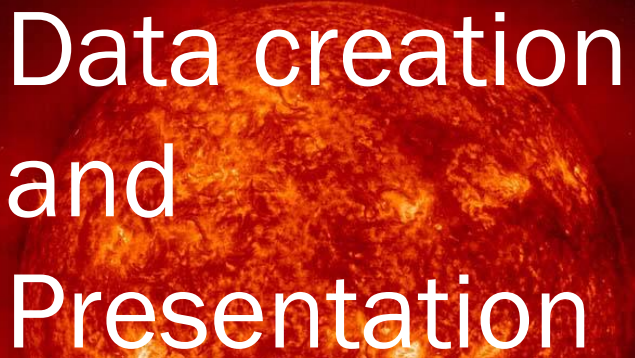
Maintain Menu

Maintain Menu

The screenshot displays the 'Security' application window with the 'Maintain Menu' tab selected. The left-hand tree view shows a hierarchy of menu items: Administration (Application Area.Edit, Security) and Librarian (Edit Book Library, Edit Library, Edit Persons, Edit Publisher, Reserve a Book). A 'Change Menu Entry' dialog box is open in the foreground, containing the following fields:

Menu Text	<input type="text" value="Application Area.Edit"/>
Sequence	<input type="text" value="0"/>
Function ID	<input type="text" value="SC34F"/> ... <input type="text" value="Application Area.Edit"/>

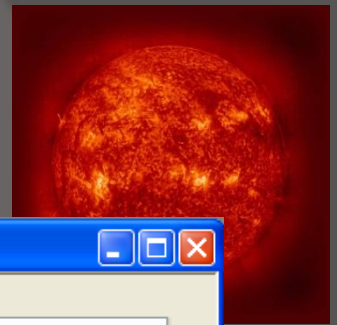
Buttons for 'Change' and 'Cancel' are located at the bottom of the dialog box.



Data creation and Presentation

Field Security

Field Security



Security

Menu Authority | Function Authority | **Field Security** | Maintain Menu | Functions | Users | Roles

Functions

Function ID	Function Description
LB6KF	Edit Persons

Authority Groups

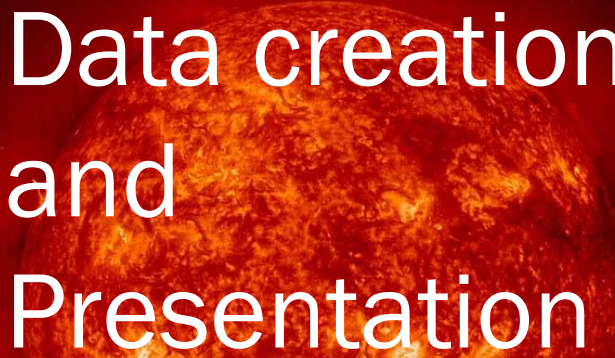
Include	Group ID	Group Description
<input checked="" type="checkbox"/>	2	Administrators
<input checked="" type="checkbox"/>	3	Librarians
<input checked="" type="checkbox"/>	5	Public

Fields

Field Description	Field Restriction Type
Person E-mail Address	READ ONLY
Person ID	PASSWORD PROTECT
Person Name	DEFAULT

Rebuild Fields

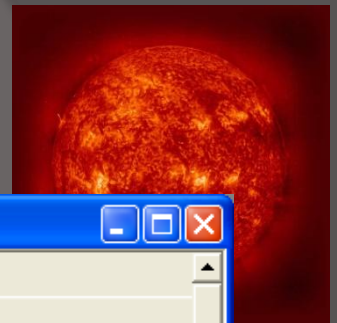
ed



Data creation and Presentation

Function Authority

Function Authority



Security [Window Title Bar]

Menu Authority | **Function Authority** | Field Security | Maintain Menu | Functions | Users | Roles

Group Roles

Role Description
Administrators
Librarians
Public

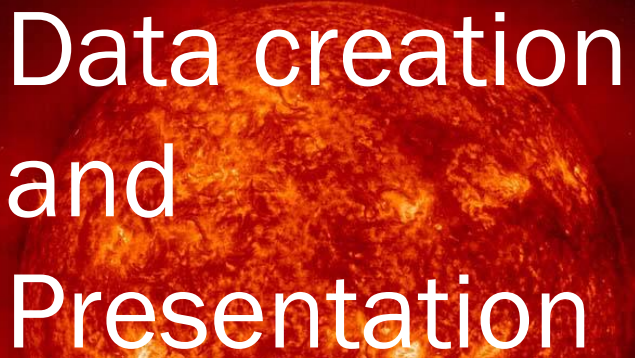
Roles

Authority	Include	Role Description
	<input checked="" type="checkbox"/>	Admin
	<input checked="" type="checkbox"/>	Borrower
	<input checked="" type="checkbox"/>	Library Worker

Function

Role Authority

- Add Book
 - Admin
 - Borrower
- Application Area.Edit
 - Admin
- Edit Book.Library
 - Admin
 - Library Worker
- Edit Library
 - Admin
 - Library Worker
- Edit Persons
 - Admin
 - Library Worker
- Edit Publisher
 - Admin
 - Library Worker
- Google Web Page
 - Admin
- Reserve a Book
 - Admin
 - Library Worker
 - Borrower
- Security
 - Admin



Data creation and Presentation

Menu Authority

Menu Authority

The screenshot displays the 'Security' application window with the 'Menu Authority' tab selected. The interface is divided into three main sections: 'Group Roles', 'Roles', and 'Function Role Authority'.

Group Roles: A table listing role descriptions.

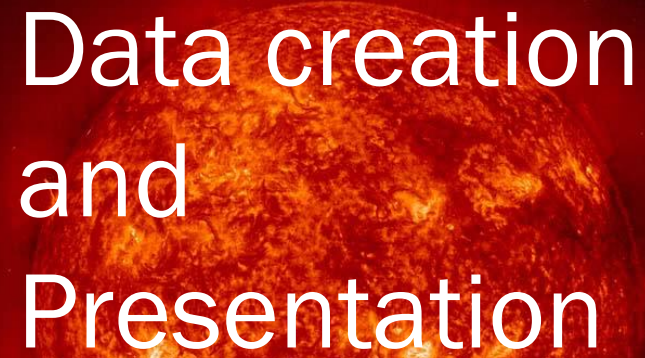
Role Description
Administrators
Librarians
Public

Roles: A table listing roles with their authority and inclusion status.

Authority	Include	Role Description
	<input checked="" type="checkbox"/>	Admin
	<input checked="" type="checkbox"/>	Borrower
	<input checked="" type="checkbox"/>	Library Worker

Function Role Authority: A tree view showing the assignment of roles to various functions.

- Administration
 - Application Area.Edit
 - Admin
 - Security
 - Admin
- Librarian
 - Edit Book Library
 - Admin
 - Library Worker
 - Edit Library
 - Admin
 - Library Worker
 - Edit Persons
 - Admin
 - Library Worker
 - Edit Publisher
 - Admin
 - Library Worker
 - Web Pages
 - Google
 - Admin
 - Reserve a Book
 - Admin
 - Library Worker
 - Borrower



Data creation and Presentation

Segregation of
authority

Segregation of A

Edit Application Area

Application Area

Application Area

Application Area
Administration
Library Administrator

Application Area: Administration

Apply New Delete Refresh Continue

Edit Application Area Roles

Application Area: Administration

Role Description Position

Role Description
Admin
Borrower
Library Worker

Edit Application Area Administrators

Application Area: Administration

User ID Position

User ID	User Name
ADMIN	

User ID ADMIN ...

User Name

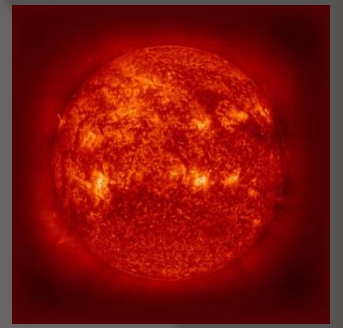
User Surname

Apply New Delete Refresh Continue new?



Pattern Implementation

Pattern Implementation



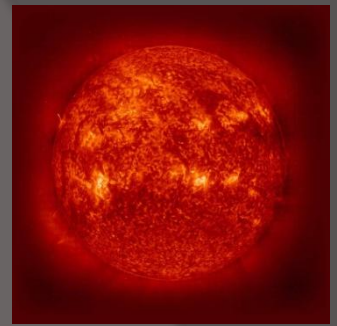
- Secure MDI
- Secured Buttons and Function
- Security Panel



Pattern Implementation

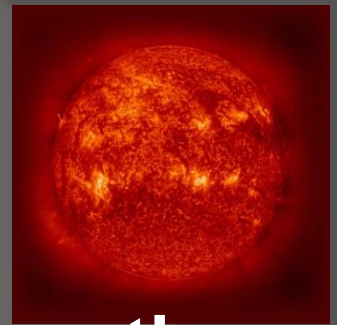
Secure MDI

Secure MDI



- The Secure MDI provides the Logon, Menu Building, Function Explorer and Calling functionality
- The authentication system needs to be set
 - **Security_AD_iSeries** provides a single sign on environment, authenticating against Active Directory and using a single user id for connecting to the iSeries.
 - **Security_iSeries** uses individual iSeries ID's and passwords for connecting to an iSeries.
 - **Security_Local** uses the local user id and password as defined to the security model.

Secure MDI



- To be able to modify the MDI and Explorer the following triples are needed

Model Editor - Function: BookMenuMDI...

BookMenuMDI is a FNC Secure MDI

Function <All> Function

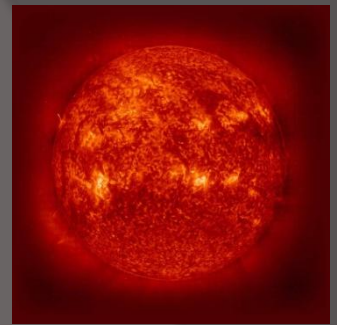
BookMenuMDI	is a	Security/Secure MDI
	includes	Build Menu Explorer
BookMenuMDI.Build Menu	is a	Security/Security Menu.Build Menu
	replaces	Security/Security Menu.Menu Explorer
	...by	BookMenuMDI.Explorer
BookMenuMDI.Explorer	is a	Security/Security Menu.Menu Explorer
	replaces	Security/Secure MDI.MDIParent
	...by	BookMenuMDI.MDIParent
BookMenuMDI.MDIParent	replaces	Security/Security Menu.Menu Explorer
	...by	BookMenuMDI.Explorer
	replaces	Security/Security Menu.Build Menu
	...by	BookMenuMDI.Build Menu
	option	Security/Security_Local
	...value	Yes



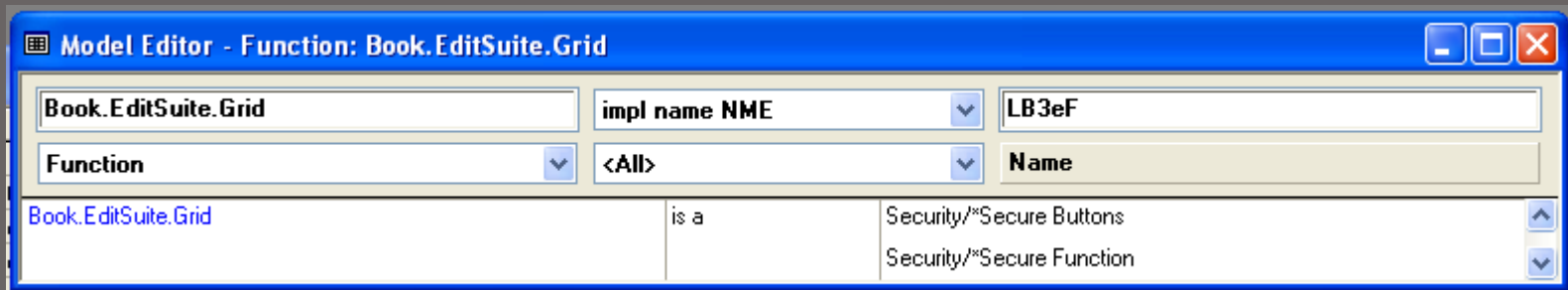
Pattern Implementation

Secured Buttons and
Function

Secured Buttons and Function



- The *Secure Function Pattern prevents functions from being called from within Plex or the Command Line
- The *Secure Buttons provides a framework for setting the state of events depending on a functions authority

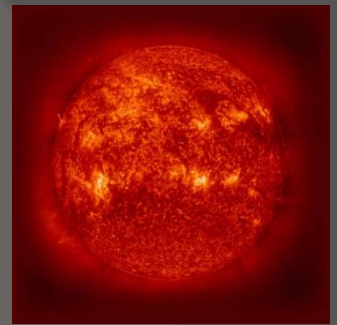




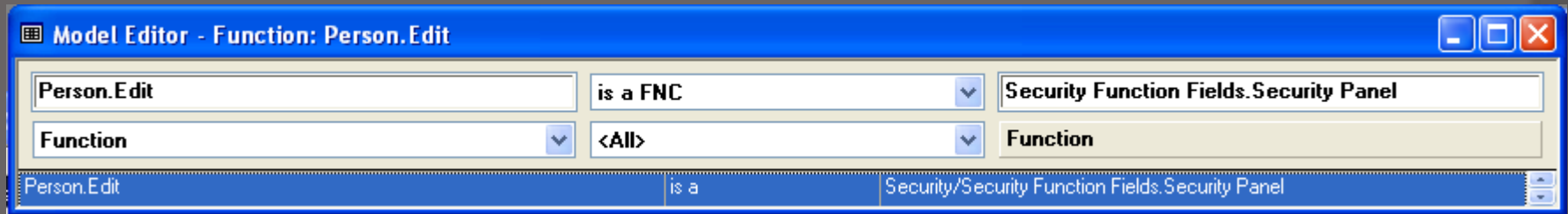
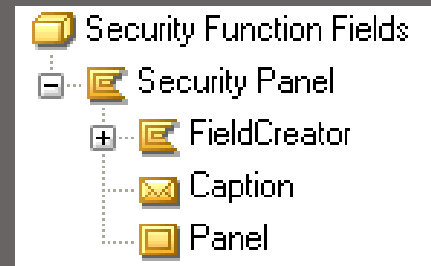
Pattern Implementation

Security Panel

Security Panel



- To Provide field level security inherit from
 - Security Panel





Customer Testimonial

Customer Testimonial (Summarised)

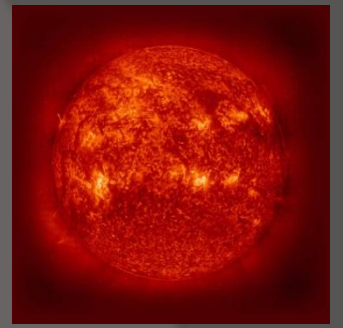


- *...the main advantages of the security pattern is that it gives you a whole lot of functionality and a framework for your applications which is extremely flexible and configurable all in one module*
- *...it also provides us with full functionality to manage the access control to the application and managing the access to different environments (Development, Testing and Production) which is a huge advantage as we have a single point of entry to our different environments with the option to give users access to the different environments*
- *The security pattern gave us a huge advantage in allowing us to keep our focus on the application functionality without the need to assign valuable resources to develop the above mentioned functionality.*



Future Plans

Future Plans



- Acting Authority
- Full auditing, allowing traceability of Function call to Authority Assignment



QUESTIONS