

Securing Your IBM Rational ClearQuest Environment

Alan Murphy

IT Specialist - IBM Rational Brand Services

IBM Certified Rational ClearQuest Administrator

alan.murphy@uk.ibm.com

IBM Rational Software Development Conference UK 2007



▶ What keeps me **Rational**?



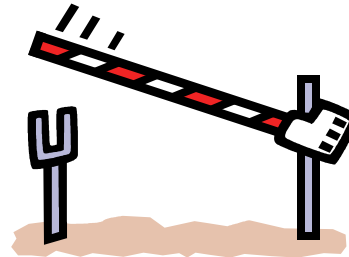
Overall Goal

- Open and Secure Lines of:
 - ▶ Communication
 - ▶ Collaboration
- Leverage Out-Of-The-Box (OOTB) functionality:
 - ▶ Schemas and Schema Capabilities
 - ▶ Security features
- Auditability
- Traceability



Terminology

- What Do We Mean By "Security"?
 - ▶ Traditional Sense
 - Put under lock and Key
 - Access Control
 - Authentication / Authorisation
 - ▶ Wider Sense
 - Privacy
 - Confidentiality
 - Abstraction
 - Data Hiding
 - Different Views of Data
 - ▶ Process Security
 - Traceability / Auditability



Scenario Background

- **Large Enterprise**
 - ▶ Implementing ClearQuest across the entire organization
 - ▶ 10-15 distributed project teams
- **Their Security Concerns are:**
 1. **Authentication & Authorisation**
 - ▶ Ability to control who can login and what they can do
 2. **Role Based Access (“Trusted” Zone)**
 - Ability to view and modify records, but transitioning state is role based
 3. **Confidentiality Between Projects and Project Teams (“Trusted” Zone)**
 - Only members of designated teams can view their records
 4. **Vendor/Contractor/Customer Access to ClearQuest (“Untrusted” Zone)**
 - Ability for vendors/contractors/customers to submit and only view records that pertain to their organization.



ClearQuest and LDAP

What is LDAP?

- The Lightweight Directory Access Protocol (LDAP) is an open industry standard that computers and networked devices can use to access common information over a network.
- LDAP is both an information model and a protocol for querying and manipulation.
- Originally developed to provide easy access to X.500 directories.
- LDAP is designed to run over the TCP/IP stack.
- LDAP is optimised for high volume read access.

LDAP is an access protocol that shares data using a particular information model.

LDAP Programming, Management, and Integration by *Clayton Donley*



ClearQuest and LDAP

Authentication VS Authorisation

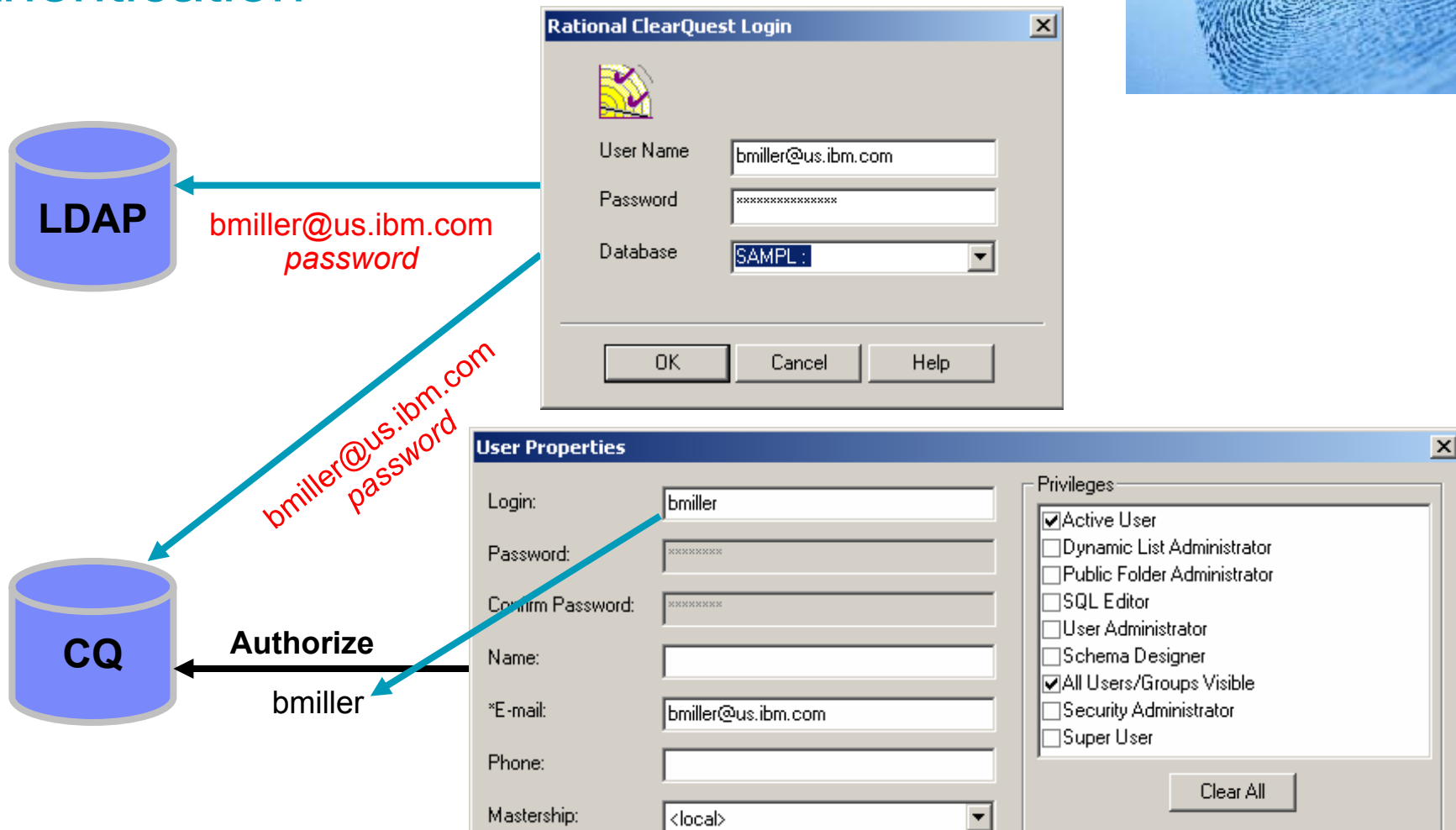


- Authentication => Who are you? What is your Identity?
 - ▶ Login Name
 - ▶ Password

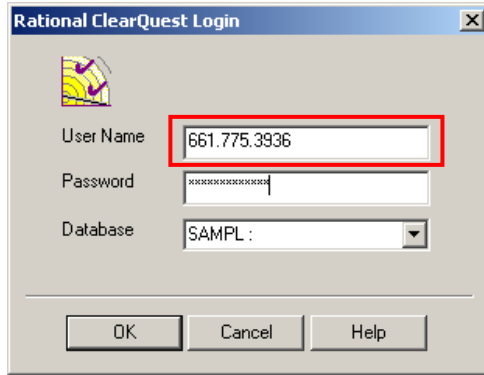
- Authorisation => What are you allowed to do?
 - ▶ UserDB Access
 - ▶ Privileges (Super User, Schema admin, Public Folder admin...)
 - ▶ Groups



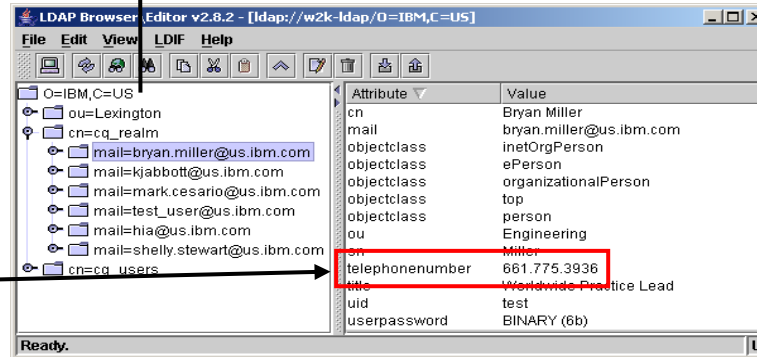
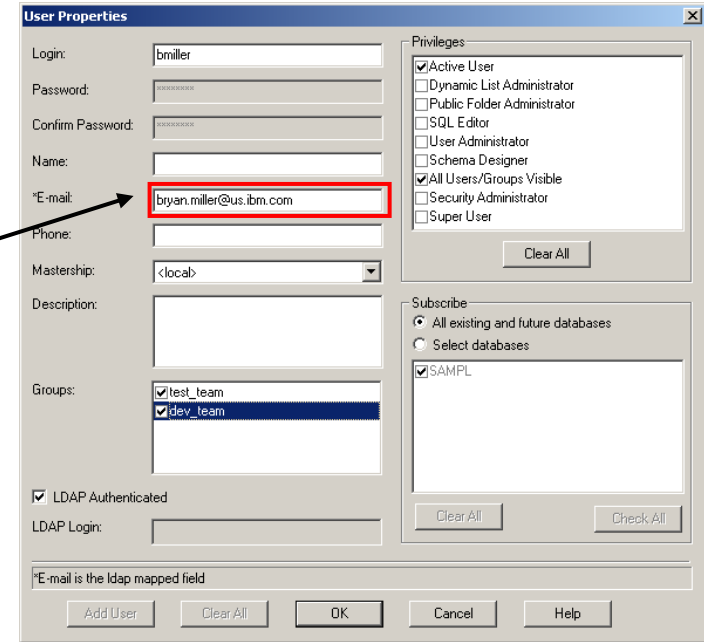
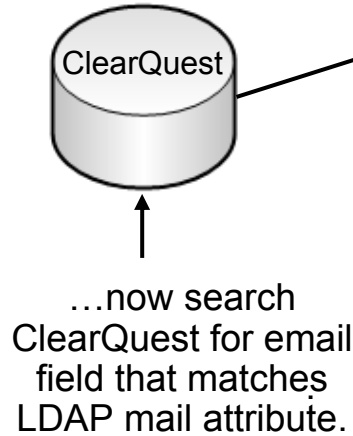
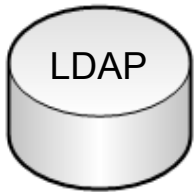
Authentication



ClearQuest to LDAP Mapping



Search LDAP for "user-name" using our defined query...



...a match will return an LDAP record...



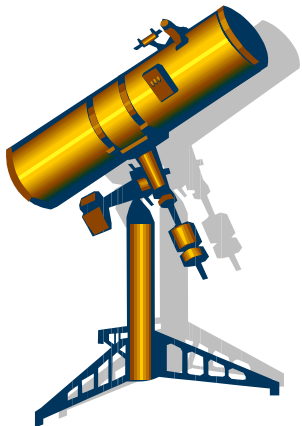
Why Use LDAP?

- Users have the same Login ID as for other Corporate Intranet Services
- LDAP Managed Centrally so:
 - ▶ Password reset requests no longer fall to ClearQuest Administrator
 - ▶ Accounts can be enabled / disabled centrally
 - ▶ Corporate Password Policies can be enforced
 - Strength
 - Aging
- Can be configured to use Secure LDAP for extra Security
- Supports LDAP servers that support protocol Version 3:
 - ▶ IBM® Lotus® Domino® LDAP Server
 - ▶ IBM Tivoli® Directory Server
 - ▶ Microsoft® Active Directory Server
 - ▶ Novell eDirectory Server
 - ▶ Sun Java™ System Directory Server



LDAP Map Lookup

- The User Properties window also contains an **LDAP Login** field. If you enter the user's LDAP login name, and a connection to the LDAP server exists, IBM Rational ClearQuest copies the value of the LDAP mapping attribute to the corresponding Rational® ClearQuest mapping field when you click **OK** or **Add User**

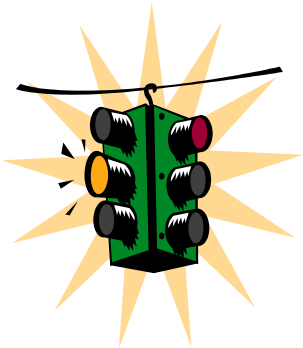
A screenshot of the 'User Properties' dialog box. The dialog is divided into several sections. The 'Login' field contains 'bmiller'. The 'Password' and 'Confirm Password' fields are masked with asterisks. The 'Name' field is empty. The '*E-mail' field contains 'bryan.miller@us.ibm.com' and is highlighted with a red rectangle. The 'Phone' field is empty. The 'Mastership' dropdown is set to '<local>'. The 'Description' field is empty. The 'Groups' list contains 'test_team' and 'dev_team', both checked. The 'LDAP Authenticated' checkbox is checked and circled in red. The 'LDAP Login' field is empty. The 'Privileges' section has several checkboxes: 'Active User' (checked), 'Dynamic List Administrator' (unchecked), 'Public Folder Administrator' (unchecked), 'SQL Editor' (unchecked), 'User Administrator' (unchecked), 'Schema Designer' (unchecked), 'All Users/Groups Visible' (checked), 'Security Administrator' (unchecked), and 'Super User' (unchecked). The 'Subscribe' section has two radio buttons: 'All existing and future databases' (selected) and 'Select databases' (unchecked). Below the 'Subscribe' section is a list box containing 'SAMPL', which is checked. At the bottom of the dialog are buttons for 'Add User', 'Clear All', 'OK', 'Cancel', and 'Help'. A status bar at the bottom of the dialog contains the text '*E-mail is the ldap mapped field'.

Authorisation

User Databases

Groups

The image shows a 'User Properties' dialog box with several fields and sections. A blue callout box labeled 'User Databases' points to the 'Groups' field. Another blue callout box labeled 'Privileges' points to the 'Privileges' section. A red box highlights the 'Groups' field, and another red box highlights the 'Privileges' section. The 'Privileges' section contains a list of checkboxes: Active User (checked), Dynamic List Administrator, Public Folder Administrator, SQL Editor, User Administrator, Schema Designer, All Users/Groups Visible (checked), Security Administrator, and Super User. The 'Subscribe' section contains two radio buttons: 'All existing and future databases' (selected) and 'Select databases'. Below the 'Select databases' radio button is a list of checkboxes: SAMPL (checked), ENTR (checked), foo (checked), tsamp (checked), and pct (checked). The 'Groups' field is empty. The 'LDAP Authenticated' checkbox is checked. The 'LDAP Login' field is empty. The 'E-mail' field contains 'engineer@company.com'. The 'Login' field contains 'engineer'. The 'Password' and 'Confirm Password' fields are masked with asterisks. The 'Name' field is empty. The 'Mastership' field is a dropdown menu with 'Admin' selected. The 'Description' field is empty. The 'Add User' button is highlighted. The 'Clear All' button is also highlighted. The 'OK', 'Cancel', and 'Help' buttons are also visible.



Role Based Access

- **Use Case:**
 - ▶ Some teams are building reusable assets. Everyone should have access to view and comment on their defects and RFEs. They can submit defects and RFEs, but cannot transition them. Only specific roles within the organization can transition records.
- **Security Requirement:**
 - ▶ Action level security
- **Implementation: 2 Possible Approaches**
 - ▶ Create users/groups and define basic roles through User Administration tool
 - Roles Based on ClearQuest Privileges
 - ▶ Define roles for the users/groups in the context of actions using designer tool
 - Define roles through group membership
 - Programmatically through hooks



RFE – Request for Enhancement



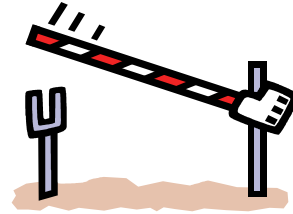
Role Based Access

Implementation Details



- **Create users and groups and define their basic roles**
 - ▶ Define users and groups with appropriate privileges through user administration tool
- **Graphically define roles for action level security**
 - ▶ Grant or revoke permissions on **actions** to all users or specific groups
- **Programmatically define roles for action level security**
 - ▶ Grant or revoke permission on **actions** to a single user
 - ▶ Grant or revoke permission on **actions** to a whole group or a part of the group
 - ▶ Grant or revoke permission on **actions** to users and groups based on any criteria





Role Based Access Example

Create users and define their roles

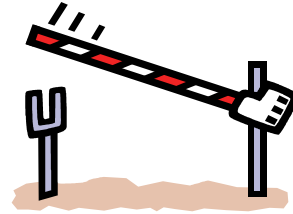
- Create user 'customer' without all user/groups visible privilege

'Customer' cannot see information about other users or group memberships

IBM Rational ClearQuest

ERROR! Access denied for retrieving record, 'engineer', record type 'users'.

OK



Role Based Access Example

Create additional users

- Create users 'Developer' and 'Tester' with *All Users/Groups Visible* Privilege

Add User

Login: Developer

Password:

Confirm Password:

Name:

E-mail:

Phone:

Mastership: <local>

Description:

Groups: Everyone

LDAP Authenticated

LDAP Login:

Privileges

- Active User
- Dynamic List Administrator
- Public Folder Administrator
- SQL Editor
- User Administrator
- Schema Designer
- All Users/Groups Visible
- Security Administrator
- Super User

Clear All

Subscribe

All existing and future databases

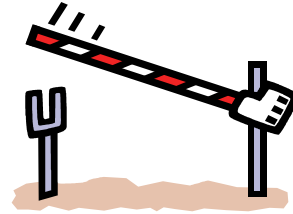
Select databases

- SAMPL

Clear All Check All

Add User Clear All OK Cancel Help

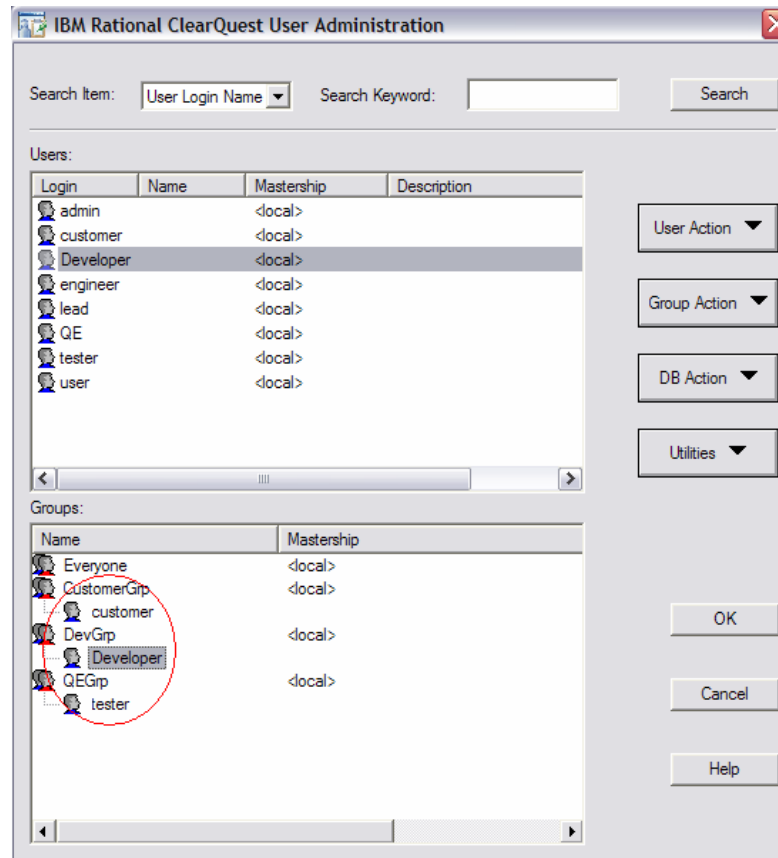


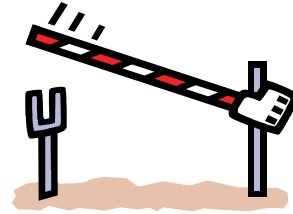


Role Based Access Example

Create additional groups

- Create CustomerGrp , DevGrp and QEGrp for their respective users





Role Based Access Example

Graphically define roles for action level security

- Restrict “Resolve” actions to “DevGrp” Members only

Action Name	Type	Access Control	Initialization	Validation	Commit	Notification	Record Scripts
Submit	SUBMIT	All Users					
Assign	CHANGE_STATE	All Users					
Open	CHANGE_STATE	All Users					
Resolve	CHANGE_STATE	User Groups					
Validate	CHANGE_STATE	All Users					
Reject	CHANGE_STATE	All Users					
Re_open	CHANGE_STATE	All Users					
Close	CHANGE_STATE	All Users					
Duplicate	DUPLICATE	All Users					
Unduplicate	UNDUPLICATE	All Users					
Postpone	CHANGE_STATE	All Users					
Modify	MODIFY	All Users					
Delete	DELETE	All Users					
Import	IMPORT	All Users					
Init_Note_Entry	BASE	All Users		PERL			
Send_Email_Notif	BASE	All Users				BASIC,PERL	

User Groups

Select User Groups:

CustomerGrp

DevGrp

Everyone

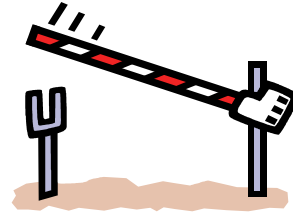
QEGrp

Ok Cancel Help

Access Control



What keeps me Rational?



Role Based Access Example

Graphically define roles for action level security

- Restrict “Close” action to Members of the group “QEGrp”

Action Name	Type	Access Control	Initialization	Validation	Commit	Notification	Record Scripts
Submit	SUBMIT	All Users					
Assign	CHANGE_STATE	All Users					
Open	CHANGE_STATE	All Users					
Resolve	CHANGE_STATE	User Groups					
Validate	CHANGE_STATE	All Users					
Reject	CHANGE_STATE	All Users					
Re_open	CHANGE_STATE	All Users					
Close	CHANGE_STATE	User Groups ▾					
Duplicate	DUPLICATE	All Users					
Unduplicate	UNDUPLICATE	All Users					
Postpone	CHANGE_STATE						
Modify	MODIFY						
Delete	DELETE						
Import	IMPORT						
Init_Note_Entry	BASE			PERL			
Send_Email_Notif	BASE					BASIC,PERL	

User Groups [X]

Select User Groups:

CustomerGrp

DevGrp

Everyone

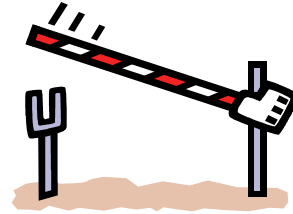
QEGrp

Ok Cancel Help



Role Based Access Example

Programmatically define roles for action level security



- Allow only "Developer" to execute Resolve action

IBM Rational ClearQuest Designer - [Resolve: Action Perl Script Editor]

Hook Types: ACTION_ACCESS_CONTI

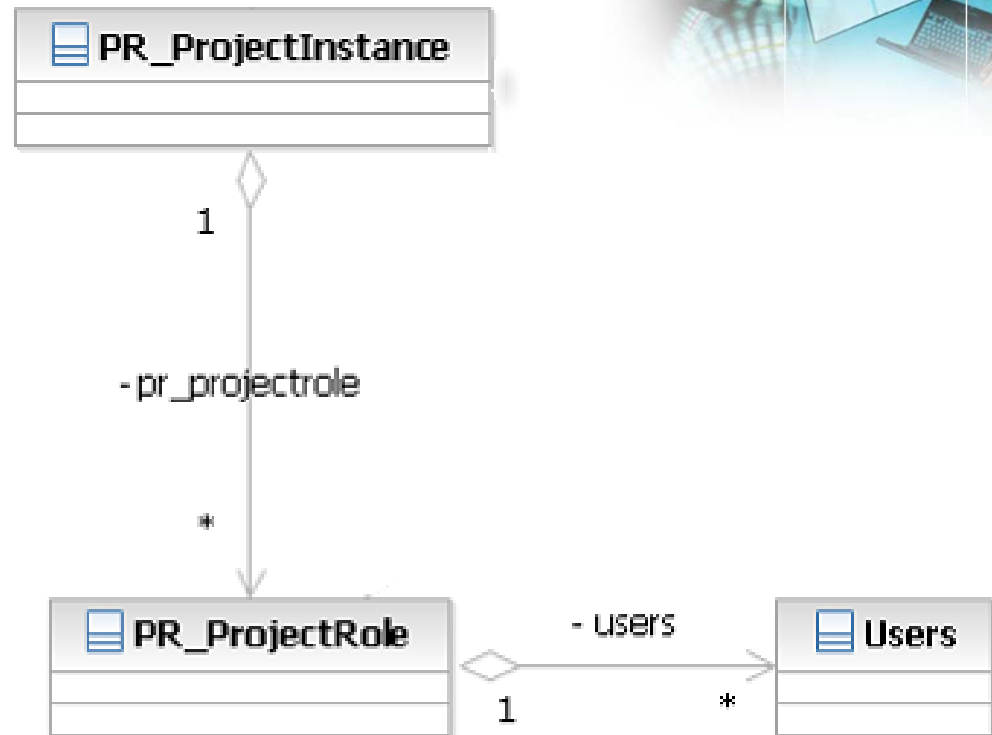
```
sub Defect_AccessControl {  
    my($actionname, $actiontype, $username)  
    my $result;  
    # $actionname string scalar  
    # $actiontype as long scalar  
    # $username as string scalar  
    # action is Resolve  
    # record type name is Defect  
  
    # Set $result to 1 if the user has permission to perform  
    # this action, otherwise set it to 0.  
  
    if ($username eq "Developer") {  
        $result = 1;  
    } else {  
        $result = 0;  
    }  
  
    return $result;  
}
```

For Simplicity, test for specific user is shown. In reality you would have a more complex test.



Project Role Example

- Uses Stateless Records to Define
 - ▶ List of Possible Roles
 - ▶ List of Projects
 - ▶ Roles Associated with a project
 - ▶ Members of a Role for a Project
- Useful in Environments where
 - ▶ Many Projects
 - ▶ Individuals work on one or more projects



Confidentiality Between Projects and Project Teams

■ Use Case:

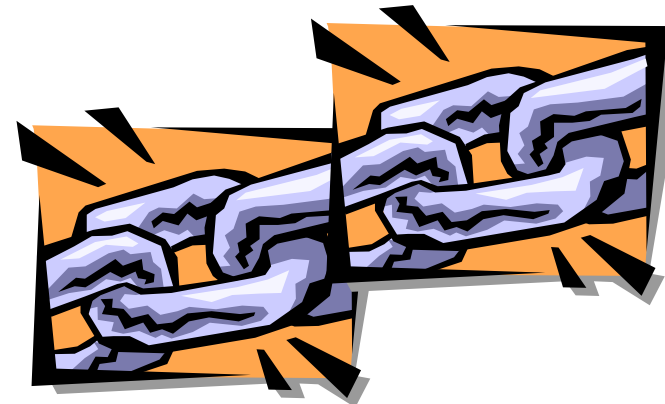
- ▶ Team X manages the corporate portal, their work is confidential and requires a highly secure and auditable environment. Defects and RFEs cannot be seen by other project teams and Customers can only see their own.

■ Security Requirements:

- ▶ Record Hiding
- ▶ Workspace ACLs
- ▶ Audit Trail and e-Signature

■ Implementation:

- ▶ Security context
- ▶ Set ACLs on project folders
- ▶ Apply Audit Trail and e-Signature packages

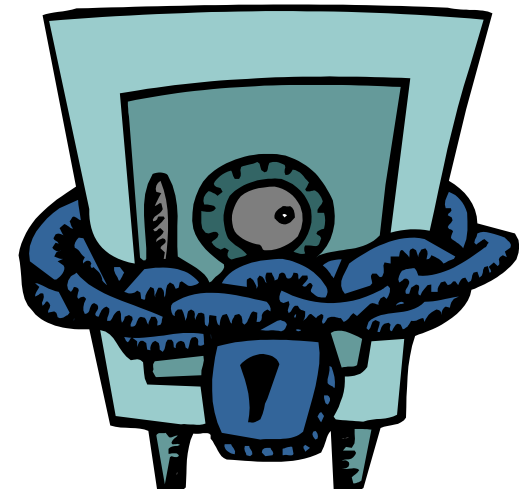


Confidentiality Between Projects and Project Teams

Implementation Details

■ **Security Context:**

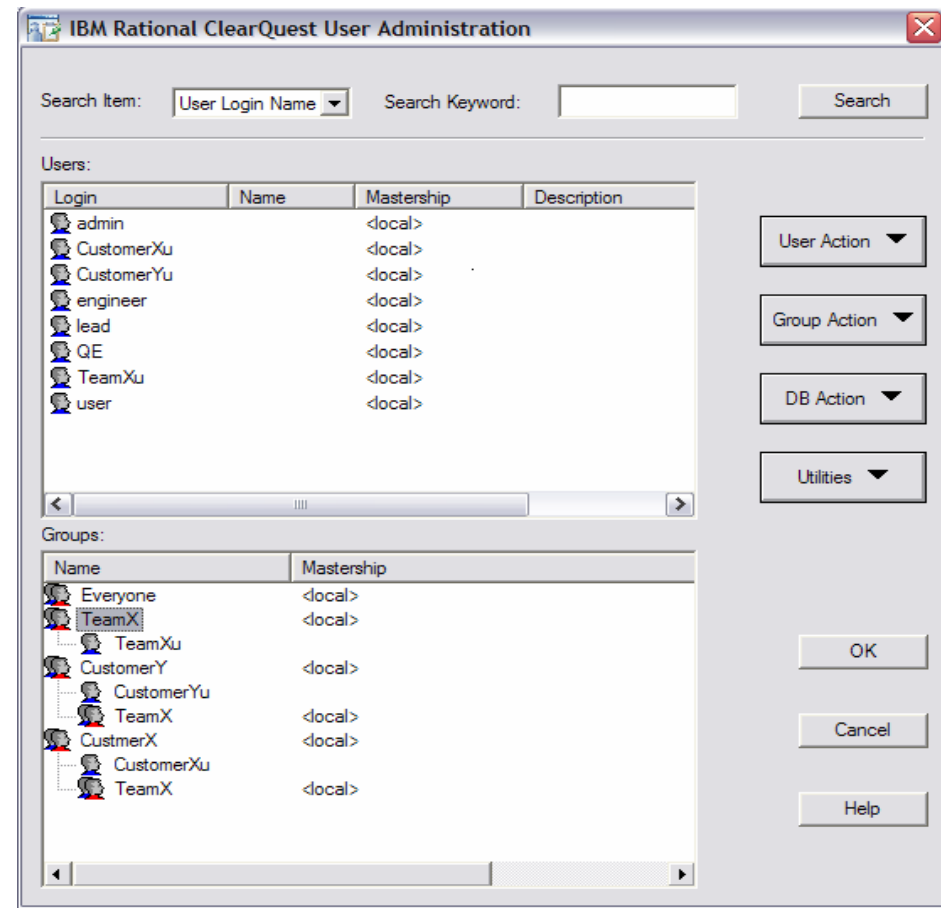
- ▶ Enables record hiding:
 - Decide which record types to control
 - Create user groups that align with your user access privileges
 - Decide which record type to use as the security context
 - The security context field must be a Reference field type
 - Submit records for each security context
 - Editing records to allow user access



Confidentiality Between Projects and Project Teams

Security Context Example

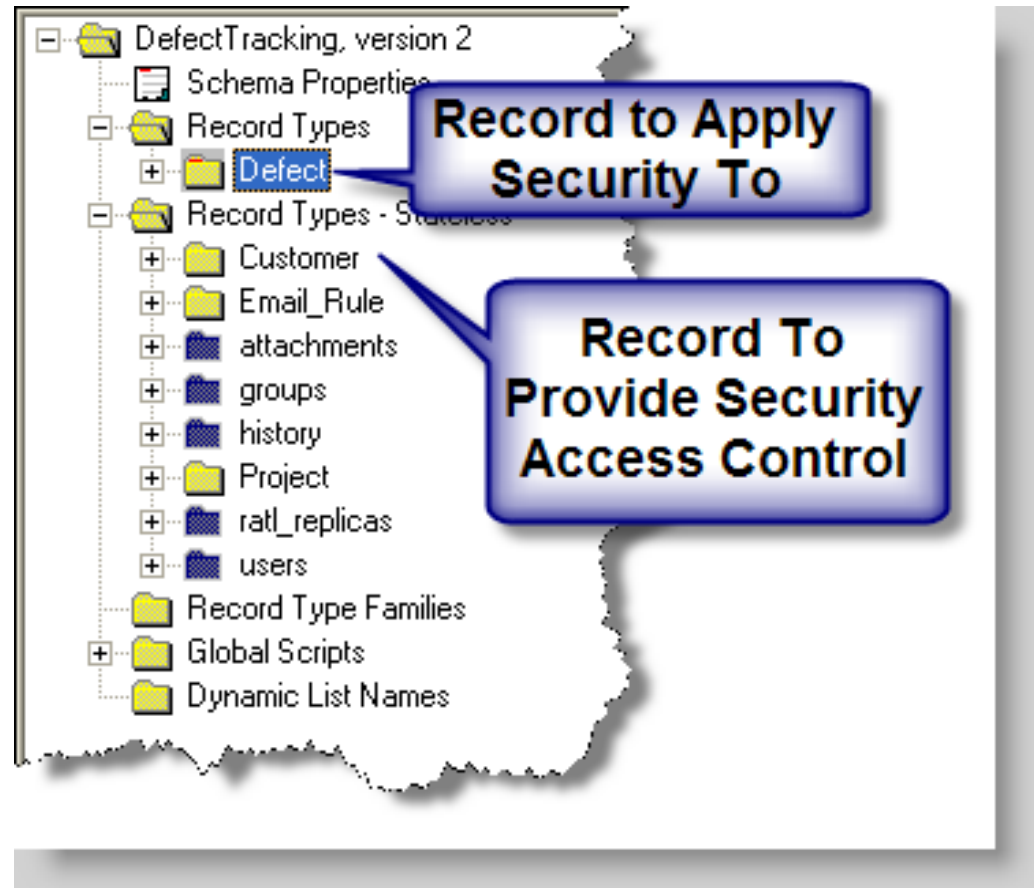
- **Create Groups**
 - **TeamX**
 - **CustomerX**
 - **CustomerY**
- **Create Users and make group members**
 - **TeamXu,**
 - **CustomerXu**
 - **CustomerYu**



Confidentiality Between Projects and Project Teams

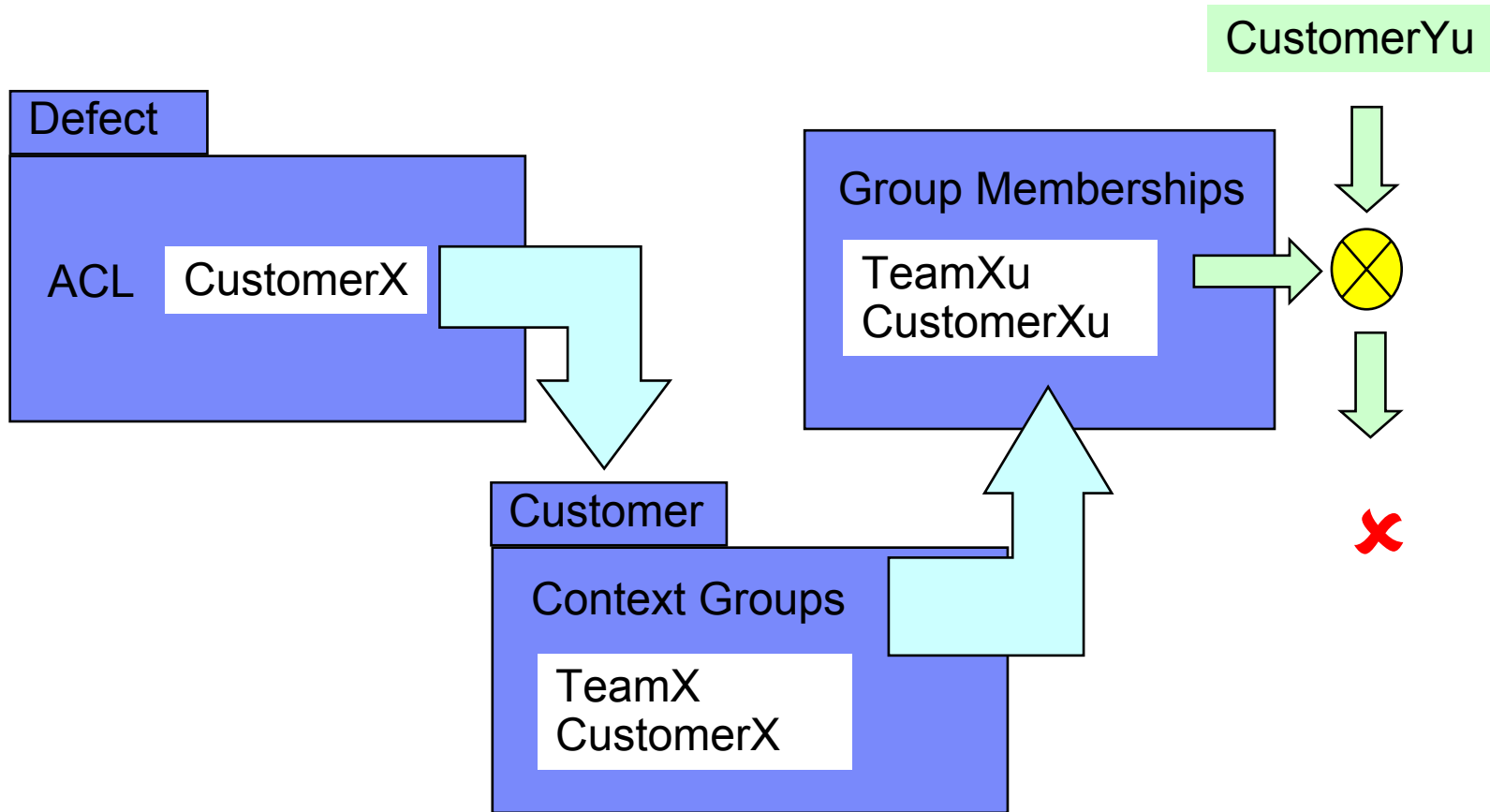
Security Context Example

- **Select Record type defect to be controlled by security context record of type customer**



Confidentiality Between Projects and Project Teams

Security Context Example



Confidentiality Between Projects and Project Teams

Security Context Example

- Create a security context field of type REFERENCE which refers to Customer record type

IBM Rational ClearQuest Designer - [Defect: Fields]

Field Name	Type	Default Value	Permission	Value Change
ratl_mastership	REFERENCE			
record_type	RECORDTYPE			
dbid	DBID			
is_active	INT			
id	ID			
State	STATE			
version	INT			
lock_version				
locked_by				
history				
is_duplicate				
unduplicate_state				
Headline				
Description				
Priority				
Severity				
Submitter				
Submit_Date				
Owner				
old_id				
Keywords				
Symptoms				
Note_Entry				
Notes_Log				
Resolution_Staty				
Resolution				
Attachments	ATTACHMENT_LIST			
Project	REFERENCE			
customer_severity	SHORT_STRING			
customer	REFERENCE_LIST			
ACL	REFERENCE			

Defect Fields - ACL

This dialog box contains properties for the selected field .

General | Help Text

Field Name: ACL

DB Column Name: acl

Type: REFERENCE

Visible in Query Security Context

Owned By: None

Reference To: Customer

Back Reference



Confidentiality Between Projects and Project Teams

Security Context Example



- Submit a 'Customer' Record
- Associate the 'CustomerX' Group with the Security Context for the record

IBM Rational ClearQuest - SAMPL :

File Edit View Actions Query Window Help

Run Query New Defect Defect Email_Rule Project

Workspace: Queries, Charts, Reports

- Personal Queries
- Public Queries
 - Aging Charts
 - Customers
 - Distribution Charts
 - Email Rules
 - PrintReportFormats
 - Report Formats
 - Reports
 - Trend Charts
 - All Defects
 - Keyword Search
 - My Hot List
 - My To Do List
 - Needs Verification

Submit Customer

Customer Rat_Security

Context Groups

name
CustomerX

Add Remove

OK Cancel Values

Browse Record Type groups

Search key:

Search Build Query... Browse...

Results:

	name
1	CustomerX
2	CustomerY
3	Everyone
4	TeamX
5	
6	
7	
8	
9	

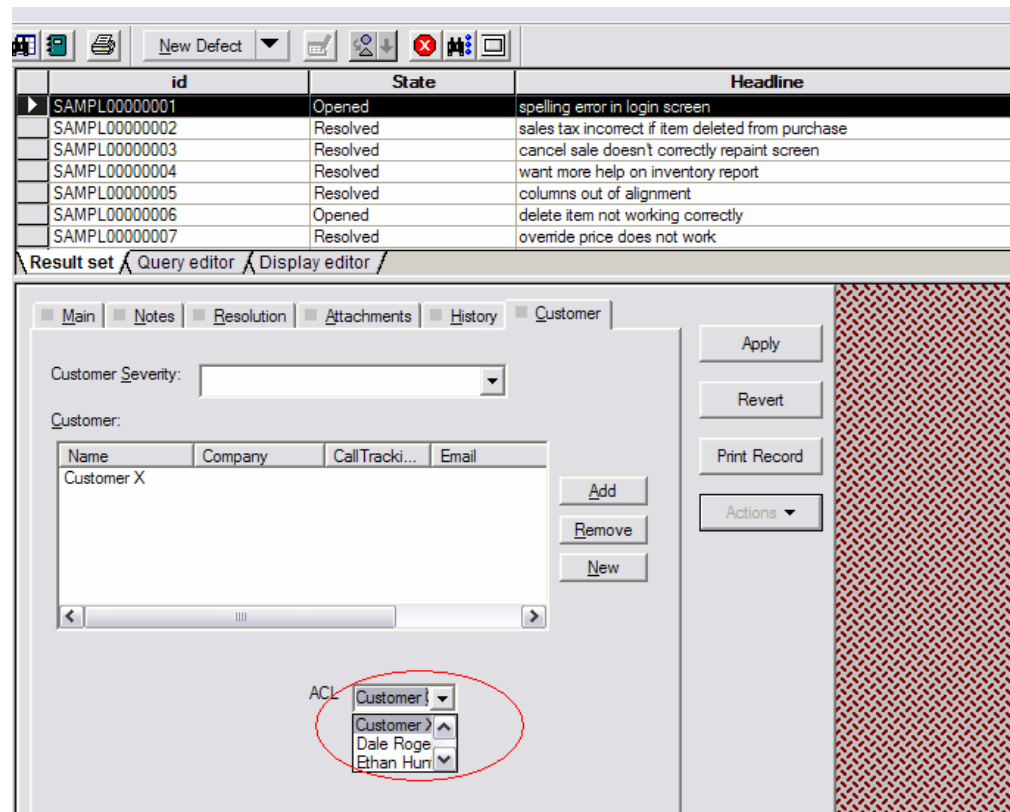
Select records to be added to the list in the form

OK Cancel Help

Confidentiality Between Projects and Project Teams

Security Context Example

- Edit Existing Records to Identify which Customer they belong to



id	State	Headline
SAMPL00000001	Opened	spelling error in login screen
SAMPL00000002	Resolved	sales tax incorrect if item deleted from purchase
SAMPL00000003	Resolved	cancel sale doesn't correctly repaint screen
SAMPL00000004	Resolved	want more help on inventory report
SAMPL00000005	Resolved	columns out of alignment
SAMPL00000006	Opened	delete item not working correctly
SAMPL00000007	Resolved	override price does not work

Result set Query editor Display editor

Main Notes Resolution Attachments History Customer

Customer Severity: [Dropdown]

Customer:

Name	Company	CallTrack...	Email
Customer X			

Add Remove New

ACL: Customer [Dropdown]

Customer Dale Roge Ethan Hunt

Apply Revert Print Record Actions

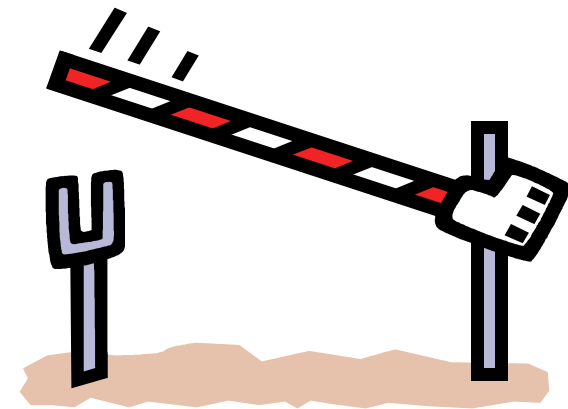


Confidentiality Between Projects and Project Teams

Implementation Details

■ Public Queries (Folder) ACLs:

- ▶ Sets CRUD permissions to:
 - Limit access/visibility to Public Queries (folders)
 - Limit cross-group/project visibility
 - Restrict customer access within Public Queries
 - Enable folder management by individual groups
 - Hiding existence of other group folders
 - Cleanups Workspace



New in ClearQuest 7.0.1

Privacy + Access Control



What keeps me **Rational**?

Confidentiality Between Projects and Project Teams

Limit access/visibility to Public Queries (folders)

- TeamX wants to share one of its private folders “AllCommonInfo” with CustomerX and CustomerY granting limited access.
- TeamX will have complete access to the content of folder “AllCommonInfo”

IBM Rational ClearQuest - [SAMPL : (commoninfo (Defect))]

Workspace: Queries, Charts, Reports

Public Queries

- Aging Charts
- AllCommonInfo
- Customers
- Distribution Charts
- Email Rules
- PrintReportFormats
- Report Formats
- Reports
- Trend Charts
- All Defects
- Keyword Search
- My Hot List
- My To Do List
- Needs Verification

ClearQuest Permissions

Filter by Group: []

Filter by User: []

Public Queries/AllCommonInfo
You can modify the permission on this folder
Your Effective Permission is Read-Write

Groups	Permissions	Effective Permissions	Change Permissions
CustomerX		Read-Only	No
CustomerY		Read-Only	No
Everyone	Read-Only	Read-Only	No
TeamX	Read-Write	Read-Write	No
	No-Access		
	Read-Only		
	Read-Write		
	Read-Limited		

Show Effective Permission Above
 Show Change Permission Above

Save Report Preview Apply Revert

Help OK Cancel

New in ClearQuest 7.0.1



What keeps me **Rational**?

Confidentiality Between Projects and Project Teams

Limit cross-group/project visibility

- TeamX wants to create a folder “TeamPrivate” whose contents should be only visible to TeamX where other groups can see the folder but not its content

ClearQuest Permissions

Filter by Group:
 Filter by User:

Public Queries/TeamPrivate
 You can modify the permission on this folder.
 Your Effective Permission is Read-Write

TeamPrivate

	Groups	Permissions	Effective Permissions	Change Permissions
	CustomerX		No-Access	No
	CustomerY		No-Access	No
	Everyone	No-Access	No-Access	No
	TeamX	Read-Write	Read-Write	No
		No-Access		
		Read-Only		
		Read-Write		
		Read-Limited		

New in ClearQuest 7.0.1



Confidentiality Between Projects and Project Teams

Enable folder management for individual groups

- Administrator wants to enable CustomerX and CustomerY to be able to Manage their own folders themselves

ClearQuest Permissions

Filter by Group: Public Queries/CustomerFolder/CustomerX
 You can modify the permission on this folder
 Your Effective Permission is Read-Write

Filter by User:

Public Queries

- Aging Charts
- AllCommonInfo
- CustomerFolder
 - Everyone:Read-Limited
 - CustomerX
 - CustomerY
- Customers
- Distribution Charts
- Email Rules
- PrintReportFormats
- Report Formats
- Reports
- TeamPrivate
- Trend Charts

Groups	Permissions	Effective Permissions	Change Permissions
CustomerX	Read-Only	Read-Only	No
CustomerXAdmi	Read-Write	Read-Write	Yes
CustomerY	No-Access	No-Access	No
Everyone	No-Access	No-Access	No
TeamX	No-Access	No-Access	No

Show Effective Permission Above
 Show Change Permission Above

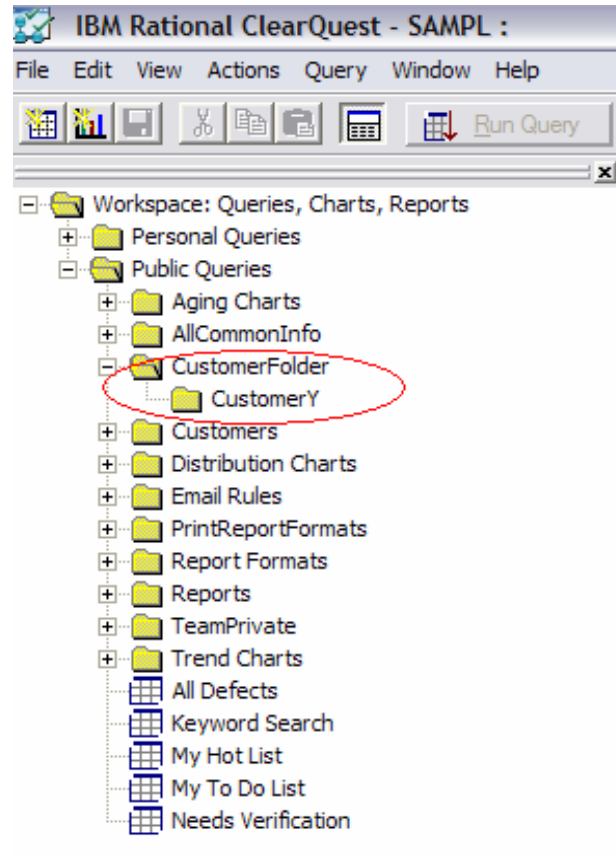
New in ClearQuest 7.0.1



Confidentiality Between Projects and Project Teams

Hiding existence of other group folders

- **Hide CustomerX folders from CustomerY and vice versa**



New in ClearQuest 7.0.1



Ensuring Process Traceability & Auditability

- ▶ **Apply AuditTrail and eSignature packages:**
- ▶ **AuditTrail:**
 - Specifies that certain records are to be audited when they are created or changed
 - Can be configured to determine what fields to audit
- ▶ **eSignature:**
 - Requires users to add their electronic signatures to records when certain State Transitions occur
 - Can be configured to determine actions/state transitions that need to be signed and who can sign.



Ensuring Process Traceability & Auditability

Audit Trail Example

- ▶ After applying the AuditTrail package and enabling a record type An Audit Trail tab will be added to the record form
- ▶ Content of Audit Trail can be Customised
 - ▶ Can Choose which fields to audit
 - ▶ Can Choose format of audit trail content

Record History:

```

====START====
Time      : 2007-05-02 19:23:54 +06:00
Schema Rev : 5
User Name  : admin
User Login : admin
User Groups : Everyone
Action     : Modify
State      : Submitted
==Fields==
Headline   (27:37)
Old        : Testing Audit Trail package
New        : Testing Audit Trail package completed
Severity   (7:9)
Old        : 4-Minor
New        : 3-Average
====END====

====START====
Time      : 2007-05-02 19:22:40 +06:00
Schema Rev : 5
User Name  : CustomerYu
User Login : CustomerYu
User Groups : Everyone CustomerY
  
```

ID: 00000041



Ensuring Process Traceability & Auditability

e-Signature Example

- After applying the package to schema, you must configure it

Submit eSig_Config

■ eSignature Configuration Record

Record Type: Defect

Sign by State:

States: Sign When: Entering State

Sign by Action

OK

Cancel

Values ▾





Ensuring Process Traceability & Auditability

e-Signature Example

- During a *Modify* operation it prompts for user name and password

id	State	Headline
SAMPL00000001	Opened	spelling error in login screen
SAMPL00000002	Resolved	sales tax incorrect if item deleted from purchase
SAMPL00000003	Resolved	cancel sale doesn't correctly repaint screen
SAMPL00000004	Resolved	want more help on inventory report
SAMPL00000005	Resolved	columns out of alignment
SAMPL00000006	Opened	delete item not working correctly
SAMPL00000007	Resolved	override price does not work

Result set / Query editor / Display editor /

Main
Notes
Resolution
Attachments

History
Customer
Audit Trail
eSignature

Enter eSignature Here:

User Name:

Password:

eSignature Log:


```

**START** e-Signature - 2007-05-02 19:33:46 +05:00
Fullname:
Login: admin
Groups: Everyone
State: Opened
Purpose/Action: Modify
**END** e-Signature
          
```



Vendor/Contractor/Customer Access to ClearQuest

■ Use Case:

- ▶ Team Y is working with external vendors. Team Y needs to file Defects and RFEs for the vendors. The vendors require access to submit Defects and RFEs

■ Security Requirements:

- ▶ Record Hiding
- ▶ Workspace ACLs
- ▶ External IDs not in corporate LDAP directory

■ Implementation:

- ▶ Leverage ClearQuest Web client
 - Restricted mode



Vendor/Contractor/Customer Access to ClearQuest Implementation Details

- **Restricted Mode:** Provides a layer of user privilege control in addition to that provided in the underlying schema
 - ▶ Configuring Restricted Mode access:
 - Restrict Site: All users run in restricted mode
 - Restricted Users: Specific users are restricted
 - Restricted User Groups: Specific user groups are restricted
 - Restricted Query: Users in restricted mode can access only one Query predefined by the administrator
 - Administrator can choose whether to Allow Find Record When Restricted: Users in restricted mode can use the Find Record feature (subject to s enforcement rules)
 - Administrator can choose whether to allow restricted users to Modify Records



New!



Vendor/Contractor/Customer Access to ClearQuest Restricted Mode Example

- Configuring restricted mode access

Rational - Windows Internet Explorer

http://localhost/cqweb/main?command=GenerateMainFrame&rmsessionId=aaa4c161-1

File Edit View Favorites Tools Help

Rational

Rational ClearQuest® Web Home **Site Configuration** Logon Statistics User Profile Help About Log Out IBM

- Select a database - Go

Site Configuration
Defect and Change Tracking

Restore Defaults Save Cancel

Site Configuration: Defect and Change Tracking

Security Options Reporting Options Application Options Email Options

Restrict Site:
(default: no selection)

Restricted Users:
(default: none)

Restricted Usergroups:
(default: none)

Restricted Query:
(default: none)

Allow Find Record When Restricted:
(default: no selection)

* Required Fields



Enhanced Web Security Improvements!

The screenshot shows the 'Site Configuration: Defect and Change Tracking' page in Rational ClearQuest Web. The 'Security Options' tab is active, displaying several settings:

- Restrict Site:** (default: no selection)
- Restricted Users:** (default: none)
- Restricted Usergroups:** (default: none)
- Restricted Query:** (default: none)
- Allow Find Record When Restricted:** (default: no selection)
- Allow Modify Record When Restricted:** (default: no selection)
- Disable Persistent Cookies:** (default: no selection)

Two blue callout boxes highlight new features:

- Left Callout:** "New Site Configuration setting allowing Restricted Users to modify records when in restricted mode" (points to the 'Allow Modify Record When Restricted' checkbox).
- Right Callout:** "New Site Configuration setting allowing admins to disable persistent cookies" (points to the 'Disable Persistent Cookies' checkbox).

At the bottom of the interface, there is a note: "* Required Fields".

New in ClearQuest 7.0.1

Vendor/Contractor/Customer Access to ClearQuest Restricted Mode Example

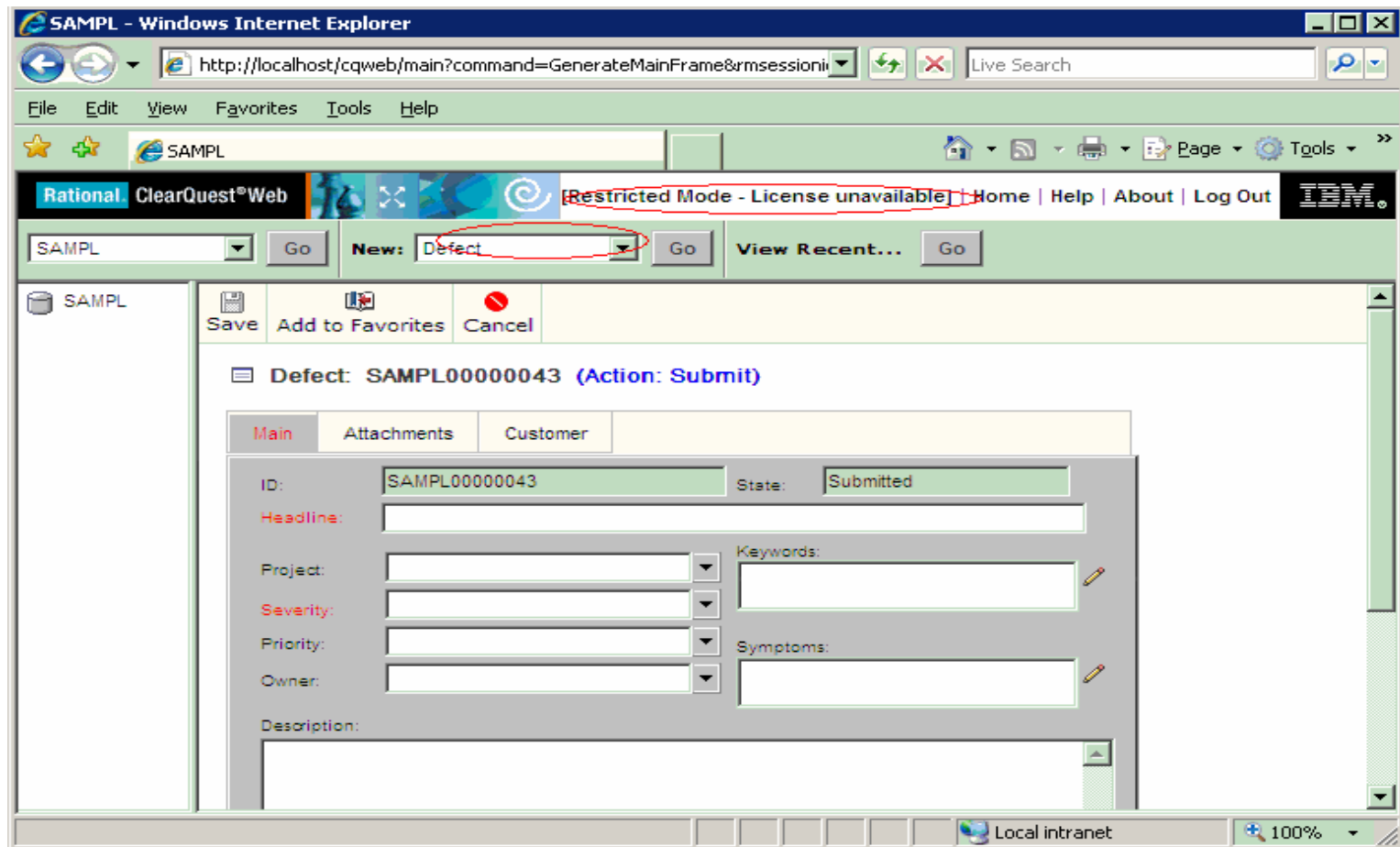
- Before applying Restricted mode

The screenshot shows the ClearQuest web interface in a browser window. The URL is `http://localhost/cqweb/main?command=GenerateMainFrame&rmssid=acf1ac42-c`. The interface includes a navigation menu on the left with categories like 'Personal Queries', 'Public Queries', 'Aging Charts', 'Customers', 'Distribution Charts', 'Email Rules', 'PrintReportFormats', 'Report Formats', 'Reports', and 'Trend Charts'. The 'Reports' and 'All Defects' items are circled in red. The main content area displays 'Results for Query "Public Queries/All Defects"' and a list of defects. The selected defect is 'Defect: SAMPL00000001'. The defect details are shown in a form with fields for ID, State, Headline, Project, Severity, Priority, Owner, and Description. The 'Change' button is circled in red, and a context menu is open over it, showing options like 'Resolve' and 'Postpone'. The status bar at the bottom indicates 'Local intranet' and '100%' zoom.



Vendor/Contractor/Customer Access to ClearQuest Restricted Mode Example

- After enabling Restrict Site for All users/groups



Vendor/Contractor/Customer Access to ClearQuest Restricted Mode Example

- Example after enabling Restrict Site with Restricted Query

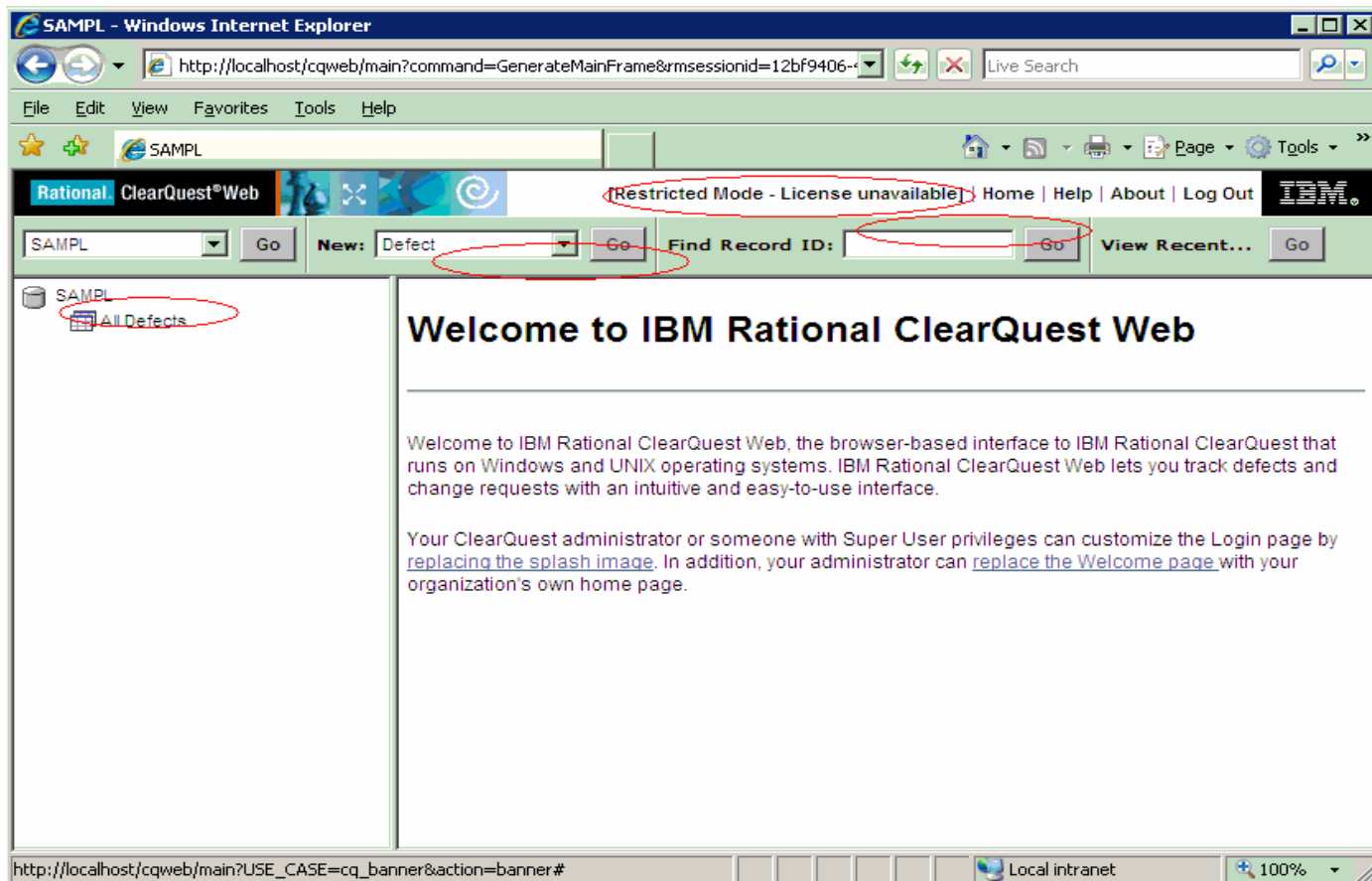
The screenshot displays the ClearQuest web interface in a restricted mode. Key elements include:

- Browser Window:** SAMPL - Windows Internet Explorer, URL: `http://localhost/cqweb/main?command=GenerateMainFrame&rmssessionid=b946dd12-`
- Page Header:** Rational. ClearQuest® Web. A red circle highlights the text "[Restricted Mode - License unavailable]".
- Navigation:** Home | Help | About | Log Out
- Search Bar:** SAMPL, Go, New: Defect, Go, View Recent... Go
- Left Sidebar:** SAMPL, All Defects (circled in red)
- Main Content Area:**
 - Buttons: Refresh, Export Grid, Printable Version
 - Section: Results for Query "Public Queries/All Defects"
 - Buttons: Refresh, Printable Version
 - Defect: SAMPL00000001 (1/40)
 - Tabs: Main, Notes, Resolution, Attachments, History, Customer
 - Form Fields:
 - ID: SAMPL00000001, State: Opened
 - Headline: spelling error in login screen
 - Project: Classics
 - Severity: 3-Average
 - Priority: 3-Normal Queue
 - Owner: lead
 - Description: option2
- Bottom Left:** A red circle highlights the text "All Actions disabled".
- Bottom Status Bar:** Local intranet, 100%



Vendor/Contractor/Customer Access to ClearQuest Restricted Mode Example

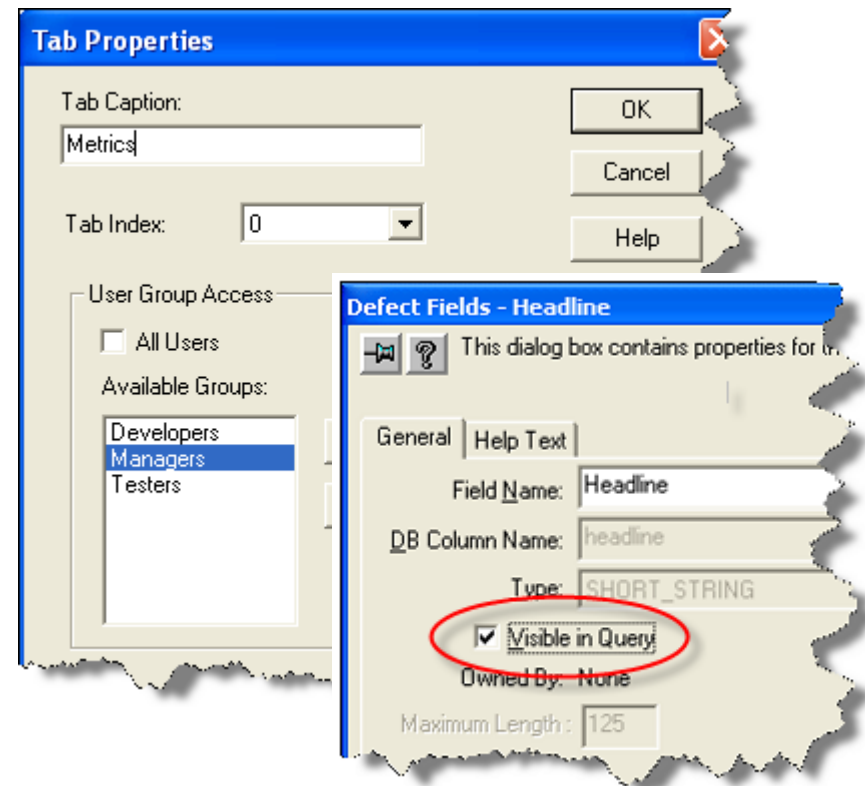
- Example after enabling Restrict Site with Find Record and Restricted Query



Miscellaneous Security Features in ClearQuest

- In Addition to above security features ClearQuest provides the following features which can be applied to ClearQuest change management system

- ▶ Restricting Access to Fields
- ▶ Hiding fields in a Query
- ▶ Restricting Access to Actions
- ▶ Restrict Access to Dialog Tabs
- ▶ Password Fields
- ▶ Granular Folder level Permissions in Workspace ACL





Server-Side SMTP Email Notification

- The existing client-side email notification approach is executed on client desktops
 - ▶ This approach tends to be problematic for many customers due to increased IT infrastructure security rules
 - Many IT organizations only permit SMTP mail to be sent via a select set of IP addresses
 - MAPI 'Broken' by Security Patches requesting user confirmation for all emails
- The answer – Rational Field Services!
 - ▶ Greatly enhanced email notification reliability and audit capabilities
 - ▶ Full replacement of client-side email notification
 - ▶ Adds a “Postoffice” stateless record to any existing schema
 - ▶ No client-side / Web server configuration or maintenance required
 - ▶ Completely flexible email content generation
 - ▶ For further info contact: Alan Murphy or David J. Trent
(alan.murphy@uk.ibm.com or djtrent@us.ibm.com)





Questions





Thank You

Alan Murphy
IT Specialist - IBM Rational Brand Services
IBM Certified Rational ClearQuest Administrator
alan.murphy@uk.ibm.com

