

# **Configure the Rational ClearQuest Web and Rational DOORS Web Access integration with SSL**

Joan Morgan  
November 1, 2012

<b>INTRODUCTION</b> .....	<b>3</b>
<b>SUPPORTED FEATURES</b> .....	<b>4</b>
<b>PREPARATION FOR THE INTEGRATION</b> .....	<b>5</b>
PREREQUISITES.....	5
SOFTWARE INSTALLATION.....	5
IMPORTANT NOTES.....	6
<b>CONFIGURE RATIONAL DOORS WEB ACCESS WITH SSL</b> .....	<b>7</b>
IDENTIFYING THE DATABASE URN.....	7
ADDING THE URN TO THE FESTIVAL.XML FILE.....	8
GET THE KEYSTORE FILE AND NEW SELF-SIGNED CERTIFICATE.....	9
CREATING ONE KEYSTORE FILE AND CERTIFICATE FOR BOTH PRODUCTS.....	9
CREATING SEPARATE KEYSTORE FILES AND CERTIFICATES FOR EACH PRODUCT.....	11
CONFIGURE SSL AND KEYSTORE FILE ATTRIBUTES FOR DOORS WEB ACCESS.....	11
CONFIGURE SSL AND KEYSTORE FILE ATTRIBUTES FOR CLEARQUEST WEB.....	12
SETUP THE RATIONAL DOORS DATABASE SERVER.....	12
CONFIGURE THE REDIRECTOR SERVICE WITH SSL.....	13
CONFIGURE THE FESTIVAL.XML FILE.....	13
RUN THE DBADMIN COMMAND.....	14
START RATIONAL DOORS WEB ACCESS WITH SSL.....	14
<b>PREPARE THE CLEARQUEST SCHEMA FOR THE INTEGRATION</b> .....	<b>16</b>
APPLY THE REQUIREMENTSCHANGEREQUEST PACKAGE TO THE SCHEMA.....	16
CONFIGURE AN EXISTING CLEARQUEST RECORD TYPE.....	18
<b>CONFIGURE CROSS-SERVER COMMUNICATION</b> .....	<b>20</b>
ESTABLISH CROSS-SERVER COMMUNICATION IN CLEARQUEST WEB.....	20
CONFIGURE PROJECT RELATIONSHIPS.....	21
REGISTER DOORS WEB ACCESS OAUTH CONSUMER IN CLEARQUEST WEB.....	22
REGISTER CLEARQUEST WEB SERVICES IN THE RATIONAL DOORS CLIENT.....	23
ADD CLEARQUEST WEB CONNECTION TO COLLABORATION LINKS.....	24
<b>DEFINING A TEMPLATE FOR THE INTEGRATION</b> .....	<b>25</b>
CONFIGURE RATIONAL CHANGE MANAGEMENT SERVER.....	25
REQUIREMENTS CHANGE MANAGEMENT.....	26
REQUIREMENTS IMPLEMENTATION.....	27
REQUIREMENTS GATHERING.....	28
FINISH TEMPLATE CONFIGURATION.....	28
<b>ENABLING THE INTEGRATION FROM THE DOORS CLIENT</b> .....	<b>29</b>
CREATE THE DOORS PROJECT AND MODULE FOR CONFIGURATION.....	29
ENABLE REQUIREMENTS IMPLEMENTATION.....	30
ENABLE REQUIREMENTS CHANGE MANAGEMENT.....	30
ENABLE REQUIREMENTS GATHERING.....	31
<b>CONCLUSION</b> .....	<b>32</b>
<b>REFERENCES</b> .....	<b>32</b>

## Introduction

This white paper instructs on how to configure the integration of IBM Rational ClearQuest Web and IBM Rational DOORS Web Access (DWA) with Secure Sockets Layer (SSL) enabled. The integration supports Requirements Implementation, Requirements Change Management, and Requirements Gathering features. These features create links between a Rational DOORS requirement and a Rational ClearQuest (CQ) change request to enable traceability between the two records. Open Services Lifecycle Collaboration (OSLC) provides the integration between the two products.

With this white paper you learn how to apply the **RequirementsChangeRequest** and **OSLCLinks** packages to your ClearQuest schema. These packages enable you to use the integration of the ClearQuest change request workflow to manage changes to the requirements within the DOORS interface.

You must have an understanding of these topics:

- ClearQuest schemas
- Rational DOORS and Rational DOORS Web Access
- Open Services Lifecycle Collaboration technology

This white paper provides you with the knowledge to perform these activities:

- Configure Rational DOORS Web Access with SSL enabled
- Configure SSL for Rational ClearQuest Web
- Start Rational DOORS Web Access
- Configure the Rational ClearQuest and Rational DOORS integration

This white paper does not target information specific to tools development.

## Supported features

- **Requirements gathering**

Requirements gathering automates the start of the product definition phase. As such, you can gather requirements suggestions and proposals by using a change management tool and review them through configurable work flows. Once approved, change management records are pulled into a Rational DOORS module for further analysis and propagation.

- **Requirements implementation**

Brings comprehensive, round-trip traceability through business requirements, change requests, and code. The interface reduces scope creep (uncontrolled changes in project scope), streamlines development, and provides real-time visibility relationships between requirements and development activities.

- **Requirements Change Management**

Provides flexibility to implement any process for managing, tracking, and reporting on all proposed changes against critical requirements, links, requirements structures, specifications, test plans, and other information maintained in the change management database.

## Preparation for the integration

To setup the OSLC-based integration between Rational ClearQuest and Rational DOORS you must install and configure the products on a Microsoft Windows computer.

The basis of the integration is to apply the **OSLCLinks** V1.1 and **RequirementsChangeRequest** V1.0 packages to your Rational ClearQuest schema as explained in later topics of this white paper. You must install the Rational ClearQuest administration tools to apply the packages to your schema.

To enable “rich-hover” capability and to support creating links from the Rational ClearQuest Web client, install and configure the Rational DOORS Web Access client.

### Prerequisites

- Rational ClearQuest V7.1.2, V8.0, or above
- Rational DOORS V9.3 or above
- Rational DOORS Web Access V1.4 or above
  - Node locked licenses are not available
- You must have valid Rational DOORS licenses for the integration to work

**Note:** You can find information on the required licensing for both products in the Rational Common Licensing Information Center:

[http://publib.boulder.ibm.com/infocenter/rational/v0r0m0/topic/com.ibm.rational.license.doc/topics/t\\_define\\_lic\\_types.html](http://publib.boulder.ibm.com/infocenter/rational/v0r0m0/topic/com.ibm.rational.license.doc/topics/t_define_lic_types.html)

### Software installation

1. Install the Rational DOORS components in this order:
  - a) Install the Rational DOORS Database Server V9.3 or above
  - b) Install DWA V1.4 or above
  - c) Install the Rational DOORS Client

**Note:** If you require an upgrade of Rational DOORS to a higher version, you must first stop the processes and then uninstall in the following order:

- a) Uninstall the Rational DOORS client
- b) Uninstall DOORS Web Access
- c) Uninstall Rational DOORS server

After uninstalling, you can reinstall using the order in step 1.

2. Install Rational ClearQuest Web. Make sure you also select Administration Tools and ClearQuest Web applications during ClearQuest installation.

### ***Important notes***

- When configuring the Rational ClearQuest and Rational DOORS Web Access integration, you must use lower case characters for host name even if the server name includes upper case characters. Otherwise, some integration operation will fail.
- When configuring the integration between Rational ClearQuest and Rational DOORS, you must specify a consistent URL format. All URLs must use either the fully qualified domain name or just the host name. The URL format must be consistent in the **doorsRedirector.properties** and **festival.xml** configuration files as well. You will find more information on those two configuration files in this white paper.

The DOORS Web Access server cannot connect to the ClearQuest Web server if you specify the URLs in mixed formats, resulting in a **"GET failed with http code 401"** error.

- The DOORS Information Center has more information on DOORS Web Access tasks:
  - Installation on Microsoft Windows  
[http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.install.doc/topics/c\\_introinstallwin.html](http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.install.doc/topics/c_introinstallwin.html)
  - Uninstall on Windows  
[http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.install.doc/topics/c\\_removedwawindows.html](http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.install.doc/topics/c_removedwawindows.html)
  - Running DOORS Web Access (includes start and stop operations)  
[http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.install.doc/topics/c\\_rundoorswebaccess.html](http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.install.doc/topics/c_rundoorswebaccess.html)

## Configure Rational DOORS Web Access with SSL

This configuration enables DOORS Web Access to use SSL and enabling the Hypertext Transfer Protocol Secure (HTTPS) connector in the included Tomcat server. You require a **security certificate** to proceed. You can make a certificate manually for testing purposes or you can purchase one from a trusted certificate authority. You also require a **keystore** that contains the server certificate.

The default HTTPS port for the Tomcat server and DOORS Web Access is 8443. To use a different HTTPS port, define the custom port in the **server.xml** file and all of the DOORS Web Access configuration files with reference to 8443 as the HTTPS port.

Before you make any changes, you must stop DOORS Web Access. This document assumes that that DOORS Web Access is in a stopped state. Before you update your configuration files, back them up.

**Note:** At the end of this procedure, you must restart Rational DOORS and DOORS Web Access.

### *Identifying the database URN*

You must have a database uniform resource name (URN) before you can configure the Rational DOORS Web Access server to communicate with the broker, the license server, and the Rational DOORS database server.

1. Start the Rational DOORS database server if it is not already running.
2. Start the Rational DOORS client and log into the database.
3. Select the menu option **Tools > Edit DXL**.
4. Type this DXL script into the DXL input pane:

```
print getDatabaseIdentifier()
```

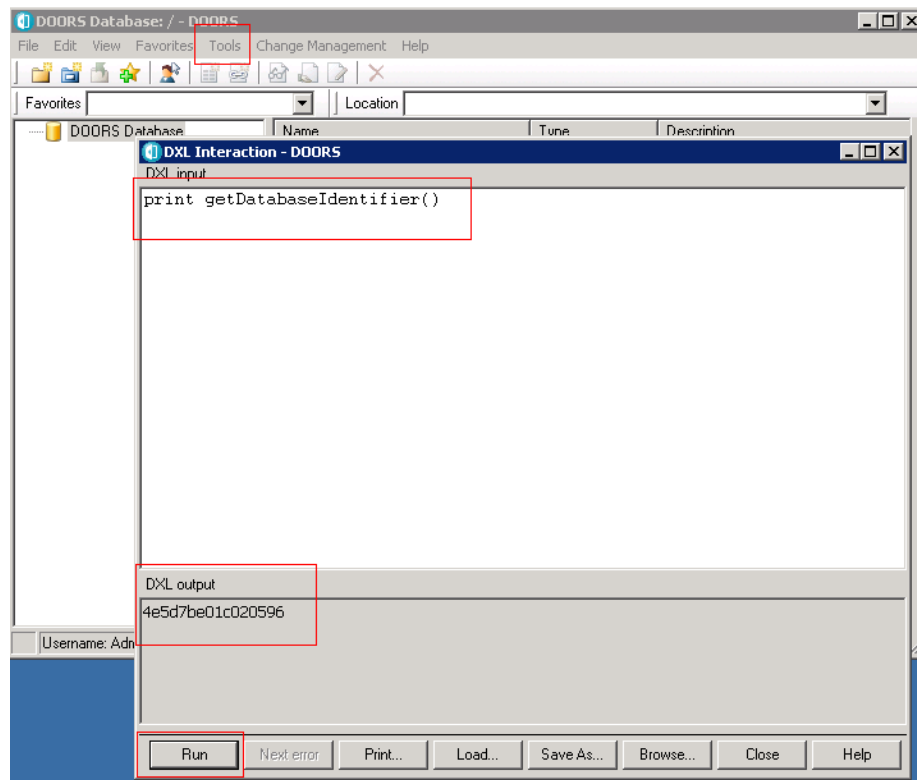
5. Click **Run**.

Clicking **Run** results in a 16-digit, hexadecimal number in the **DXL output** field. For example:

```
38f5c98719f27b6d
```

This number forms part of the database URN. In this example, the database URN is:

```
urn:rational:ers-4e5d7be01c020596:
```



6. Take note of the database URN. You must have the URN when modifying the DOORS Web Access configuration files.

### ***Adding the URN to the festival.xml file***

The **festival.xml** file is one of the core configuration files for the DOORS Web Access server, along with the **doorsRedirector.properties** file. You can find the files in this directory by default:

**C:\Program Files\IBM\Rational\DOORS Web Access\<<version>\server\festival\config**

You must modify entries in the **festival.xml** file to set up the DOORS Web Access server to communicate with the broker and the license server. You must also add the URN you gathered from the DXL output in the Rational DOORS client.

Modify the entries for **f:broker**, **f:repository-mapping**, and **f:properties** in the file to match your broker, repository, and license server setup respectively.

1. Open the **festival.xml** file in a text editor.
2. Modify the **repositoryUrn** attribute of the **f:repository-mapping** tag using the URN value that you gathered earlier.



For example:

```
<f:repository-mapping
  enabled="true"
  endpoint="RMSERVICES"
  name="DOORS ERS Repository"
  repositoryUrn="urn:rational:ers-4e5d7be01c020596:" />
```

## Get the keystore file and new self-signed certificate

When configuring SSL for DOORS Web Access and ClearQuest Web, you can create a key store and certificate for both using IBM Key Management Utility. Alternatively, you can create separate key stores and certificates for DOORS Web Access and ClearQuest Web.

**Note:** If you are generating your own certificate for testing purposes, you can create and manage the keystore using the standard Java key tool facilities as documented on the Sun web site. In addition to the Sun documentation, there are resources available on the Internet that can help you with creating your own certificate and installing it into Tomcat.

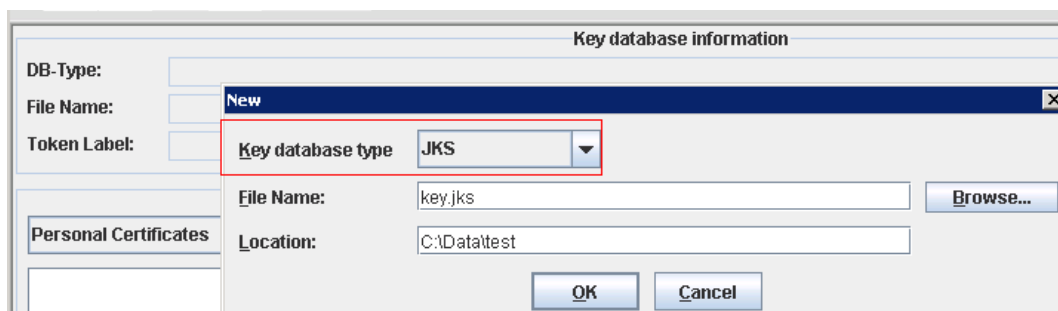
## Creating one keystore file and certificate for both products

Use the IBM Key Management Utility to generate the a key of the database type "JKS". The IBM HTTP Server packaged with Rational ClearQuest Web includes that tool. To generate this key:

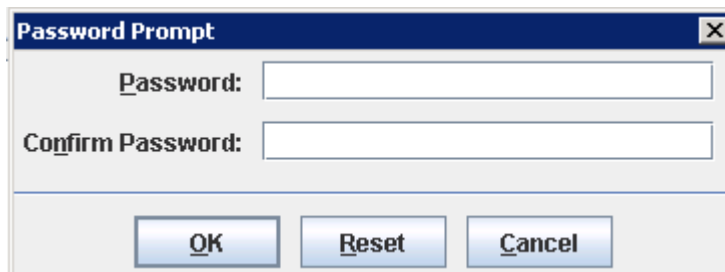
1. On the Rational ClearQuest Web server machine, open the IBM Key Management Utility in the Windows Start menu path:

**All Programs > IBM HTTP Server > Start Key Management Utility**

2. In the **Key Database File** menu of the tool, select **New**.
3. Select "JKS" as **Key database type**. Provide a location to store the key. Click **OK**.

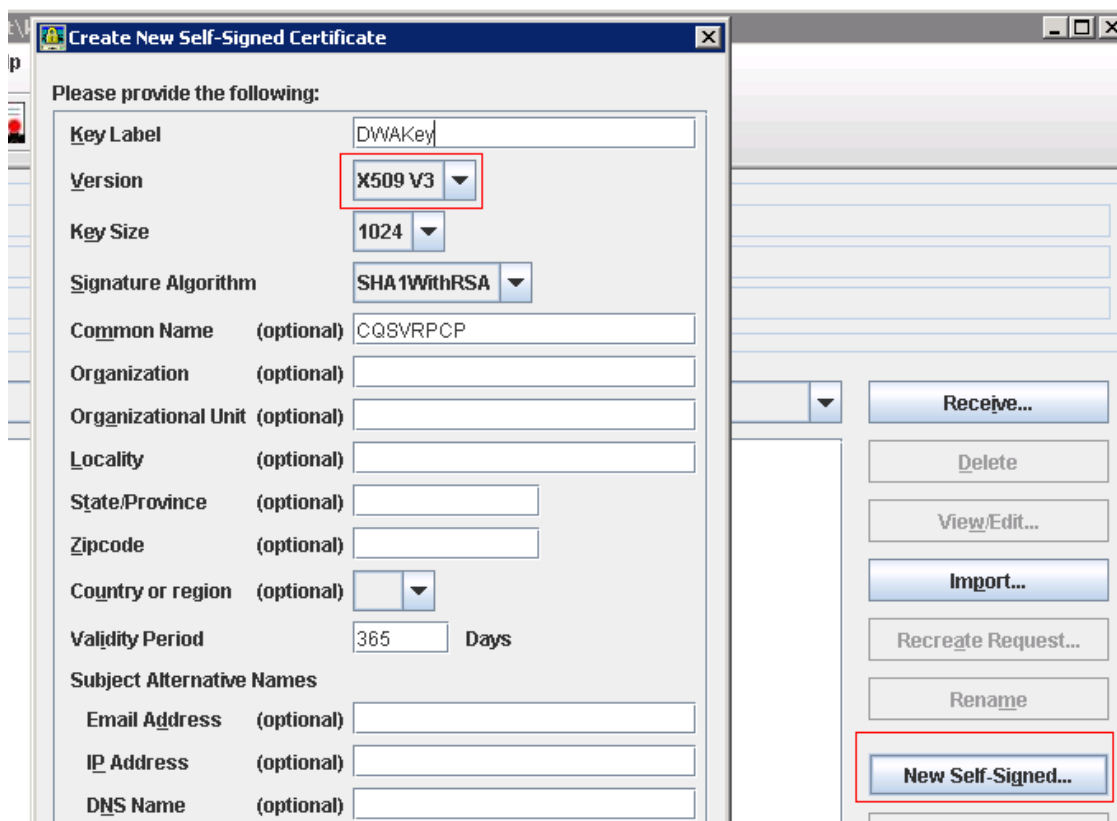


4. Type a password for the key and click **OK**.



A dialog box titled "Password Prompt" with a close button (X) in the top right corner. It contains two text input fields: "Password:" and "Confirm Password:". Below the fields are three buttons: "OK", "Reset", and "Cancel".

5. After saving the key, click **New Self Signed**.
6. Select "**X509 V3**" as version.



A dialog box titled "Create New Self-Signed Certificate" with a close button (X) in the top right corner. It contains the following fields and options:

- Key Label:** DWAKey
- Version:** X509 V3 (highlighted with a red box)
- Key Size:** 1024
- Signature Algorithm:** SHA1WithRSA
- Common Name (optional):** CQSVRPCP
- Organization (optional):**
- Organizational Unit (optional):**
- Locality (optional):**
- State/Province (optional):**
- Zipcode (optional):**
- Country or region (optional):**
- Validity Period:** 365 Days
- Subject Alternative Names:**
  - Email Address (optional):**
  - IP Address (optional):**
  - DNS Name (optional):**

On the right side of the dialog, there is a list of buttons: "Receive...", "Delete", "View/Edit...", "Import...", "Recreate Request...", "Rename", and "New Self-Signed..." (highlighted with a red box).

7. Click **OK**. Close the IBM Key Management Utility.
8. Find the generated key and copy it into a location on the Rational DOORS Web Access server. The **KeystoreFile** value in the **server.xml** file points to this file.

## Creating separate keystore files and certificates for each product

Creating the keystore file and certificate for ClearQuest Web generally occurs with IBM Key Management Utility. However, there is another process available for DOORS Web Access if you require it to have a separate keystore and certificate.

1. Go to **server** folder in the DOORS Web Access installation location. For example:

**C:\Program Files\IBM\Rational\DOORS Web Access\<version>\server**

2. Create a folder called "ssl".

3. Open a command prompt and change to this directory:

**<DOORS Web Access Installation>\win32\ibm-java2-i386-50\jre\bin**

4. Run this command, replacing the parameter values as required. The password is "ibm-team". The **alias** is the name of the server where tomcat runs without the domain details.

```
keytool -genkey -keyalg RSA -keysize 1024 -dname "CN=<Fully Qualified Hostname>, OU=DWA, O=IBM, L=English, C=US" -validity 365 -storepass ibm-team -keystore <DOORS Web Access Installation>\server\ssl\ibm-team-ssl.keystore -keypass ibm-team -alias <host name>
```

## Configure SSL and keystore file attributes for DOORS Web Access

1. Open the **server.xml** file in this directory of the DOORS Web Access server:

**C:\Program Files\IBM\Rational\DOORS Web Access\<version>\server\conf**

2. Find this line in the file:

**<!-- Define a SSL HTTP/1.1 Connector on port 8443**

3. Delete the beginning and ending comment indicators (<!--) from this section. Make and save the changes the changes listed highlighted in **bold**:

```
<Connector port="8443" SSLEnabled="true" maxHttpHeaderSize="8192"
  maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
  enableLookups="false" disableUploadTimeout="true"
  acceptCount="100" scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="<directory>\<keystore file name>"
  keystorePass="ProvideThePassword" algorithm="IbmX509"/>
```

**Note:** The **keystoreFile** parameter must match the location of the keystore file you created for use with DOORS Web Access.

## Configure SSL and keystore file attributes for ClearQuest Web

1. Open the **httpd.conf** file in this directory of the ClearQuest Web server:

**C:\Program Files\IBM\Rational\HTTPServer\conf**

2. Find this line in the file:

**# LoadModule ibm\_ssl\_module modules/mod\_ibm\_ssl.so**

3. Delete the comment indicators (**#**) from this line. Make and save the changes the changes listed highlighted in **bold**:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 443
<VirtualHost *:443>
SSLEnable
</VirtualHost>
KeyFile <directory>\keystorefilename.kdb
SSLDisable
```

**Note:** The **KeyFile** parameter must match the location of the keystore file you created for use with ClearQuest Web.

## Setup the Rational DOORS database server

1. From the command prompt, go to this directory:

**IBM\Rational\DOORS\<version>\bin**






2. Run this **dbadmin** command:

```
dbadmin -data 36677@host -dcnEnable -dcnBrokerUrl "tcp://host:61616"
-dcnChannelName "dcn" -dwaProtocol https -dwaHost host -dwaPort port
```

For example:

```
C:\Program Files (x86)\IBM\Rational\DOORS\9.3\bin>dbadmin -data 36677@doorsserver
-dcnEnable -dcnBrokerUrl "tcp://DOORSserver:61616" -dcnChannelName "dcn"
-dwaProtocol https -dwaHost DOORSserver -dwaPort 8443
```

3. Restart the Rational DOORS Database Server service.

	Distributed Transac...	Coordinate...	Started	Automatic (D...	Network S...
	DNS Client	The DNS Cl...	Started	Automatic	Network S...
	<b>DOORS DB Server 9.3</b>		<b>Started</b>	<b>Automatic</b>	<b>Local System</b>
	Encrypting File Syst...	Provides th...		Manual	Local System
	Extensible Authenti...	The Extens...		Manual	Local System

## Configure the Redirector Service with SSL

The Rational DOORS Redirector Service gives you the option to open DOORS URLs in a standard Rational DOORS client or in a web client. The **doorsRedirector.properties** file is in the "server\festival\config" directory. If you do not configure the Redirector Service Rational DOORS URLs open in the standard client.

1. Open the **doorsRedirector.properties** file from this directory:

**<Rational Directory>\DOORS Web Access\<version>\server\festival\config**

2. Modify the values of **dwa.url.prefix** and **doors.url.prefix** for the **<properties>** tag:

```
<properties>
  <comment>Configuration for DOORS Redirector.</comment>
  <entry key="dwa.url.prefix">https://DOORSserver:8443/dwa</entry>
  <entry key="doors.enable"></entry>
  <entry key="doors.url.prefix">doors://DOORSserver:36677/</entry>
  <entry key="dwa.enable"></entry>
</properties>
```

## Configure the festival.xml file

The **festival.xml** file is the core configuration file of Rational DOORS Web Access. The file is in the "server\festival\config" directory. You must edit the file to enable SSL for the Rational DOORS Web Access server to communicate with the broker and license server.

1. Open the **festival.xml** file from this directory:

**<Rational Directory>\DOORS Web Access\<version>\server\festival\config**

2. Modify the **license.server.location**, **display.redirector.urls**, **published.url.prefix**, **ForceHttpsForAuthenticationForOAuth** and **oauth.domain** values for the **<f:properties>** tag:

For Example:

```
<f:properties>
  <f:property name="license.server.location" value="19353@server"/>
  <f:property name="display.redirector.urls" value="true"/>
  <f:property name="published.url.prefix"
    value="https://DOORSserver:8443/doors/redirector"/>
  <f:property name="ForceHttpsForAuthenticationForOAuth" value="true"/>
  <f:property name="oauth.domain" value="https://DOORSserver:8443/dwa"/>
  <f:property name="interop.version" value="9.3.0.6"/>
</f:properties>
```

**Note:** If you want DWA V1.4.0.4 to run with the Rational DOORS client V9.3.0.5 or greater, you must add an **interop.version** property with your Rational DOORS version as the value.

## Run the dbadmin command

Run the **dbadmin** command to configure the Rational DOORS database server so that the generated URLs point to the Redirector Service.

1. From the command prompt, go to this directory:

**IBM\Rational\DOORS\\bin**

- a) If your environment is Rational DOORS V9.3 and DWA V1.4, run this **dbadmin** command:

```
dbadmin -data port@host -urlPrefix https://server:port/doors/redirector
```

For example:

```
C:\Program Files (x86)\IBM\Rational\DOORS\9.3\bin> dbadmin -data  
36677@DOORSserver -urlPrefix https://DOORSserver:8443/doors/redirector
```

- b) If your environment is Rational DOORS V9.4 and DWA V1.5, run this **dbadmin** command:

```
dbadmin -data port@host -urlPrefix "" -dwaProtocol https -dwaHost host -dwaPort  
port
```

For example:

```
C:\Program Files (x86)\IBM\Rational\DOORS\9.4\bin> dbadmin -data  
36677@DOORSserver -urlPrefix "" -dwaProtocol https -dwaHost DOORSserver  
-dwaPort 8443
```

2. Restart the Rational DOORS Database Server service in Control Panel on the server machine hosting the database..

## Start Rational DOORS Web Access with SSL

To start the Rational DOORS server and Rational DOORS Web Access, you must start the processes in this order:

1. Start the broker by running **broker.start.bat** located in the Rational DOORS Web Access directory:

**C:\Program Files (x86)\IBM\Rational\DOORS Web Access\**

2. Restart the Rational DOORS Database Server service in Control Panel on the server machine hosting the database.

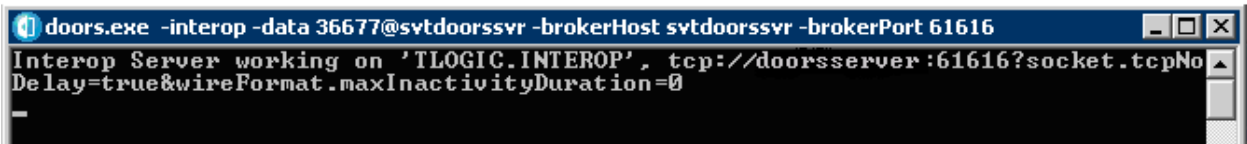
3. Run the Interoperation Server on the machine hosting DOORS Database Server from the command prompt in this format:

```
doors.exe -interop -data port@myserver -brokerHost myBroker -brokerPort brokerport
```

For example:

```
C:\Program Files (x86)\IBM\Rational\DOORS\9.3\bin> doors.exe -interop -data  
36677@doorsserver -brokerHost doorsserver -brokerPort 61616
```

After you run the **-interop** command successfully, this window opens:



```
doors.exe -interop -data 36677@sytdoorssvr -brokerHost sytdoorssvr -brokerPort 61616  
Interop Server working on 'TLOGIC.INTEROP', tcp://doorsserver:61616?socket.tcpNo  
Delay=true&wireFormat.maxInactivityDuration=0
```

4. Start the Rational DOORS Web Access server by running **server.start.bat**, located in the in DOORS Web Access directory. For example:

```
C:\Program Files (x86)\IBM\Rational\DOORS Web Access\1.4.0.4\server.start.bat
```

5. Access Doors Web Access Client using this URL:

```
https://<host>:8443/dwa
```

## Prepare the ClearQuest schema for the integration

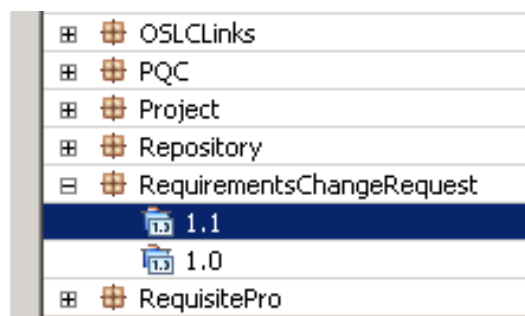
You have two avenues to take when preparing the ClearQuest schema for this integration.

- Apply the packages to the schema to create new record types for the integration
- Configure an existing record type for the integration

### ***Apply the RequirementsChangeRequest package to the schema***

The first option is to apply the **RequirementsChangeRequest** package to your ClearQuest schema. This adds new record types to the schema.

1. Log into the ClearQuest Designer tool.
2. Select the schema and schema version to which you will apply the package. Select the menu option **Packages > Apply Package**.
3. In the Package Wizard, select the latest **RequirementsChangeRequest** package. Click **Finish** to apply.



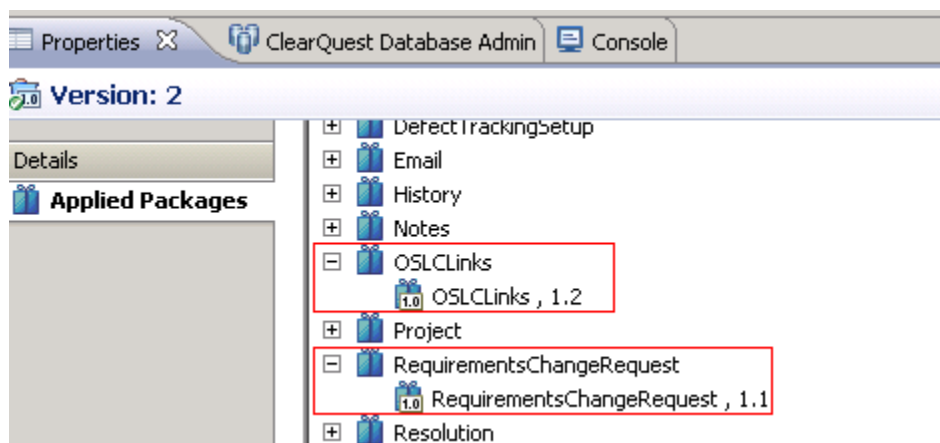
4. Check in this schema version.

Once you apply the **RequirementsChangeRequest** package, the **OSLCLinks** package will apply to the schema automatically. The inclusion of this package occurs to support these features of the integration:

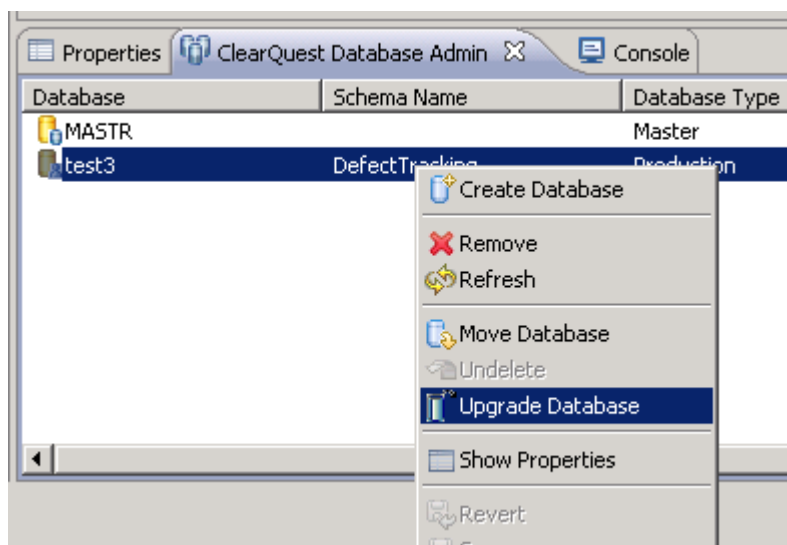
- Requirements Implementation
- Requirements Change Management with non-**RequirementsChangeRequest** enabled ClearQuest record types.
- Requirements Gathering feature.



5. Verify the application of the packages in the schema properties:



6. Upgrade the ClearQuest user database to apply the changes for the schema version. Right click the database and select **Upgrade Database**.



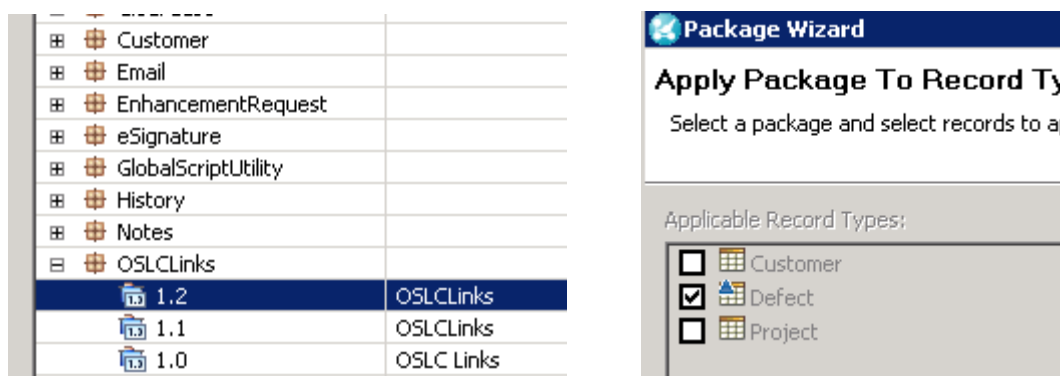
7. Log into a Rational ClearQuest client.
8. Try to submit a record. You should now see **RequirementsChangeRequest** as one of the record types.

## Configure an existing ClearQuest record type

The alternative option for preparing a ClearQuest schema for integration is configuring an existing record type for use with **RequirementsChangeRequest**.

**Note:** Use this method only on schemas that do not have the RequirementsChangeRequest record type and Requirements Change Management feature. The integration uses a "OSLC\_CQ\_State\_Mapping" global script. You cannot modify this script to support two different record types.

1. Log into the ClearQuest Designer tool.
2. In a checked out schema version, choose an existing record type. For example, "Defect".
3. Apply the latest version of the OSLCLinks package to your schema. Select "Defect" as the specific



4. Check in the schema and upgrade the user database.
5. Log into the ClearQuest client to verify the package installation.
6. Open a submission form for the target record type. There is now a **Links** tab. You can cancel the submission of the record.

The next step is to map the ClearQuest record type states to the OSLC Change Management states. In this example, you add a script for the **Defect** record type.

7. Check out the a new schema version.
8. Right click **Global Script** under the Defect record type. Select **Perl > New Script**.
9. Name the script "OSLC\_CQ\_State\_Mapping".

Here is an example of an `OSLC_CQ_State_Mapping` global script implemented in Perl. The subroutine maps the ClearQuest states (Assigned, Opened, Resolved and Closed) of a Defect record type to the corresponding `oslc_cm` states. These are the mappings defined in the global script:

- Assigned --> `oslc_cm:inprogress` is "1" (all other `oslc_cm-*` fields are "0")
- Opened --> `oslc_cm:fixed` is "1" (all other `oslc_cm-*` fields are "0")
- Resolved --> `oslc_cm:approved` is "1" (all other `oslc_cm-*` fields are "0")
- Closed --> `oslc_cm:closed` is "1" (all other `oslc_cm-*` fields are "0")

Here is the full script:

```

sub OSLC_CQ_State_Mapping
{
  my ($myentity, $hook_type) = @_;
  my $state = $myentity->GetFieldStringValue("State");

  if ($hook_type eq "Validation") {
    if ($state eq "Assigned") {
      $myentity->SetFieldValue("oslc_cm-inprogress","1");
    } else {
      $myentity->SetFieldValue("oslc_cm-inprogress","0");
    }
    if ($state eq "Opened") {
      $myentity->SetFieldValue("oslc_cm-fixed","1");
    } else {
      $myentity->SetFieldValue("oslc_cm-fixed","0");
    }
    if ($state eq "Resolved") {
      $myentity->SetFieldValue("oslc_cm-approved","1");
    } else {
      $myentity->SetFieldValue("oslc_cm-approved","0");
    }
    if ($state eq "Closed") {
      $myentity->SetFieldValue("oslc_cm-closed","1");
    } else {
      $myentity->SetFieldValue("oslc_cm-closed","0");
    }
  }
}

```

10. Save the script.

11. Check in the schema and upgrade the user database.

## Configure cross-server communication

Starting in ClearQuest V7.1.2.1 and Rational DOORS V9.3.0.1, there is support for cross-server communication and Open Authorization (OAuth) authentication. You must configure cross-server communication on both the ClearQuest Web server and the DOORS Web Access server.

### Establish cross-server communication in ClearQuest Web

1. Log into ClearQuest Web with an account that has Super User privilege.
2. Select the menu option **Site Administration > Cross-Server Communication** in the ClearQuest Web toolbar.
3. In the Cross-Sever Communication page, specify this information about the target server with which you require established communication:
  - Title: The target DOORS Web Access server
  - Root Services URI: The URI for the target root services of the application to add as a "friend" in this format:

**https://<friend-server>:<port-number>/<context>/rootservices**

**friend-server** - Host name of the friend server. Must be a public URL with a fully qualified domain name. Do not specify the IP address.

**port-number** - Port number for access the server.

**Context** - Application context. This is a configurable parameter.

**Note:** Verify that port 8443 is open on the Rational DOORS server using Microsoft Windows Firewall. In **Advanced Security**, left menu click **Inbound Rule**. If port 8443 is not open, click **New Rule**. Use the wizard to create the inbound rule for the port.

**Cross-Server Communication**

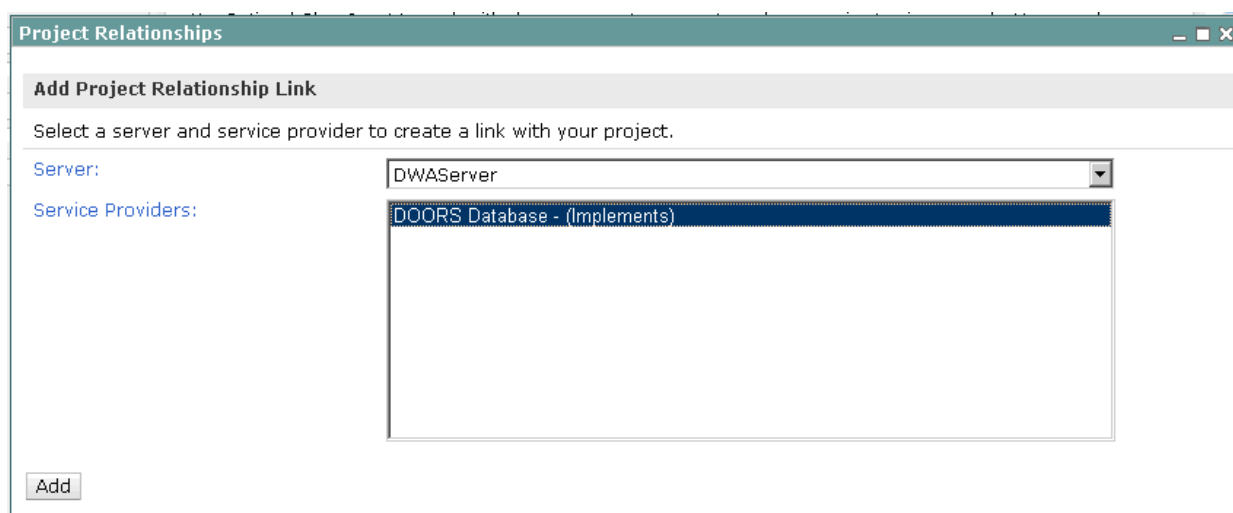
Specify other servers with which you want to establish server-to-server communication. Enter the location information of another server and a code phrase to use as the OAuth secret. Then request access to that server to create an OAuth consumer key and store the information in the friends list. Once the OAuth key is authorized by the other server, this server will be able to interact with the other server.

Property	Value
Title:	DWAServer
Root Services URI:	https://doorsserver:8443/dwa/rdm/discovery/rootservices Format: https://<hostname>:<port-number>/<context>/rootservices
OAuth Secret:	••••
Re-type secret:	••••
Trusted:	<input checked="" type="checkbox"/>

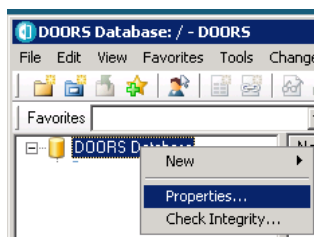
**Request Access**

## Configure Project Relationships

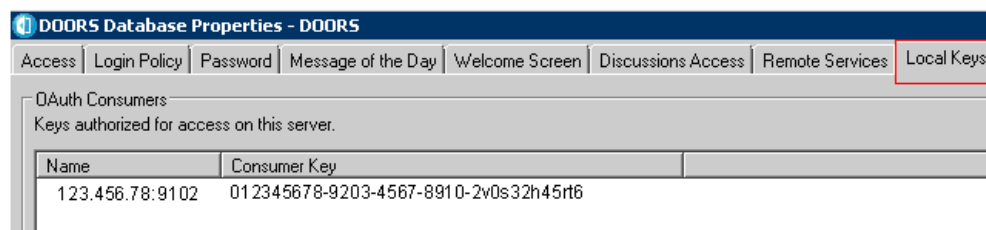
1. Log into ClearQuest Web with an account that has Super User privilege.
2. Select **Site Administration > Project Relationships** on the ClearQuest Web toolbar.
3. Select the DOORS server from the **Server** list. A DOORS Web Access authentication window might open, prompting you for credentials for the remote service. Enter your DOORS administrative user name and password. Click **OK**.
4. Select the **DOORS Database - (Implements)** service provider in the **Service Providers** list



5. In the Rational DOORS client, right click the DOORS Database and select **Properties**.



6. Check the **Local Keys** tab to verify the authorization for ClearQuest Web.

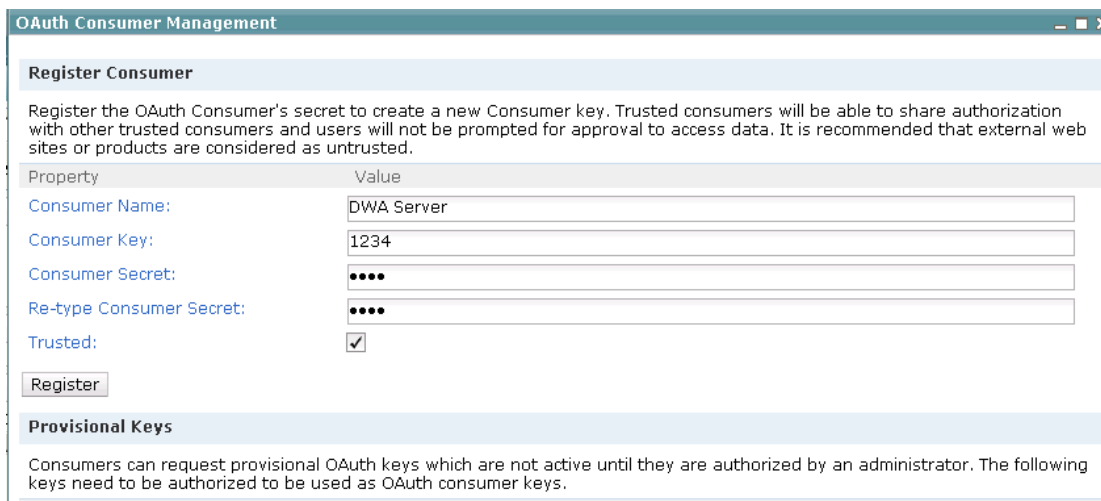


## Register DOORS Web Access OAuth Consumer in ClearQuest Web

1. Log into ClearQuest Web with an account that has Super User privilege.
2. Select **Site Administration > OAuth Consumer Management** on the ClearQuest Web toolbar.
3. In the **Consumer Name** field, enter the name of the consumer that uses the consumer key.
4. In the **Consumer Key** field, enter the OAuth key value to be associated with the consumer.
5. In the **Consumer Secret** and **Re-type Consumer Secret** fields, enter the consumer secret provided by the Jazz Team Server administrator.

**Note:** You must keep the **Consumer Key** and **Consumer Secret** in this page consistent with **Consumer Key** and **OAuth Key** when configuring remote server in the Rational DOORS client.

6. Click **Register**. You see the new key in the **Authorized Keys** section of the page.



The screenshot shows a web browser window titled "OAuth Consumer Management". The main heading is "Register Consumer". Below the heading is a descriptive paragraph: "Register the OAuth Consumer's secret to create a new Consumer key. Trusted consumers will be able to share authorization with other trusted consumers and users will not be prompted for approval to access data. It is recommended that external web sites or products are considered as untrusted." Below this is a table with two columns: "Property" and "Value". The table contains the following entries: "Consumer Name:" with the value "DWA Server", "Consumer Key:" with the value "1234", "Consumer Secret:" with masked characters "....", and "Re-type Consumer Secret:" with masked characters "....". There is a "Trusted:" checkbox which is checked. At the bottom of the form is a "Register" button. Below the form is a section titled "Provisional Keys" with a descriptive paragraph: "Consumers can request provisional OAuth keys which are not active until they are authorized by an administrator. The following keys need to be authorized to be used as OAuth consumer keys."

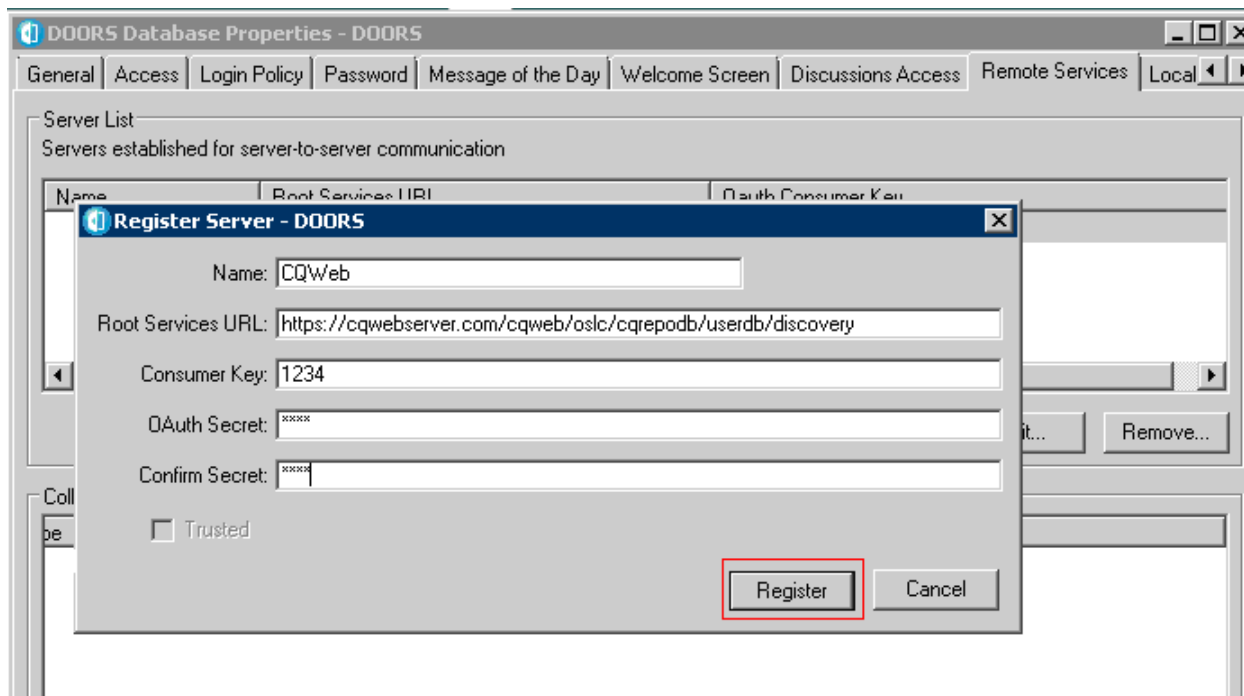
Property	Value
Consumer Name:	DWA Server
Consumer Key:	1234
Consumer Secret:	....
Re-type Consumer Secret:	....
Trusted:	<input checked="" type="checkbox"/>

### Provisional Keys

Consumers can request provisional OAuth keys which are not active until they are authorized by an administrator. The following keys need to be authorized to be used as OAuth consumer keys.

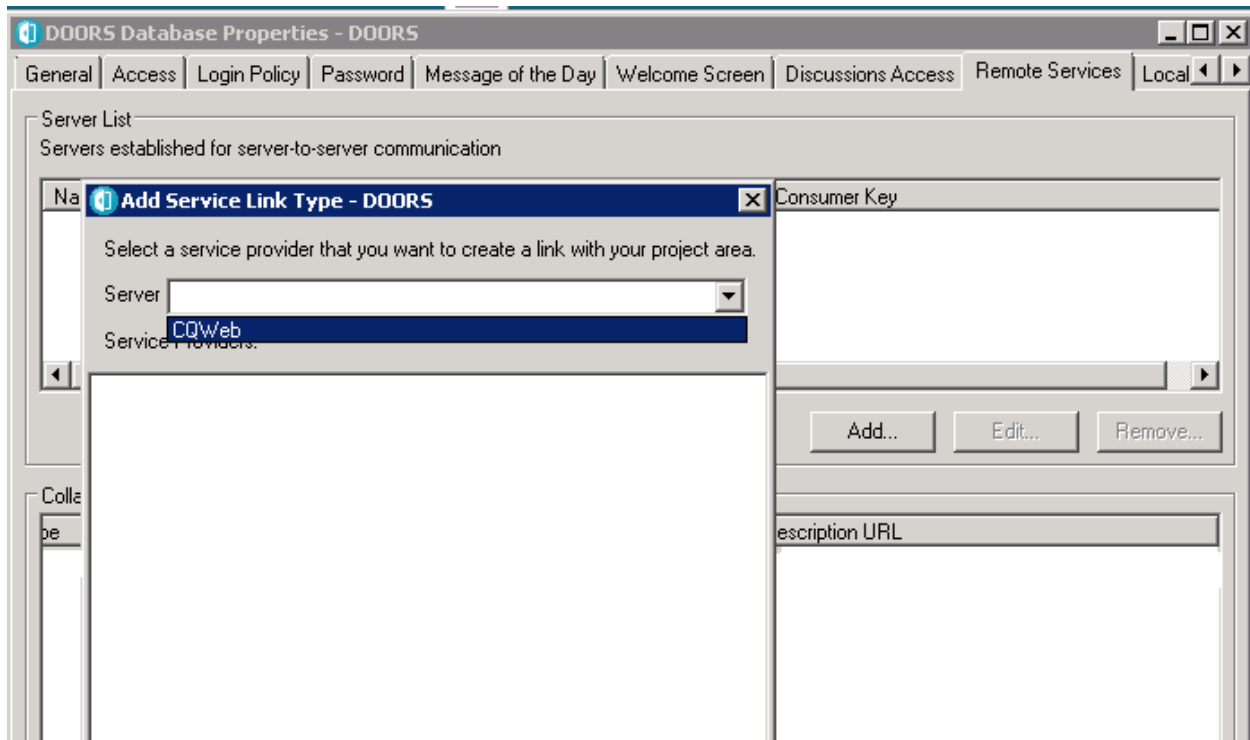
## Register ClearQuest Web services in the Rational DOORS client

1. Log into the Rational DOORS native client with administrator privilege.
2. Right click DOORS Database and select **Properties**.
3. Go to the **Remote Services** tab and click **Add**. The Register Server window opens.
4. In the **Name** field, enter a name to identify the Rational ClearQuest Web server.
5. In the **Root Services URI** field, enter the application context URI for the ClearQuest Web server:  
**https://<ClearQuest Web host>/cqweb/oslc/repo/dbset/discovery**
6. In the **Consumer Key** field, enter the OAuth key value to associate with the consumer.
7. In the **OAuth Secret** and **Confirm Secret** fields, enter an OAuth secret code to associate with the new OAuth consumer key.
8. Click **Register**



## Add ClearQuest Web connection to Collaboration Links

1. Log into the Rational DOORS native client with administrator privilege.
2. Right click DOORS Database and select **Properties**.
3. Go to the **Remote Services** tab.
4. Click **Add** in the **Collaboration Links** section.
5. In the **Server** field, select your Rational ClearQuest Web server.
6. Provide your ClearQuest login and password.
7. Select your ClearQuest user database and click **Add**. The ClearQuest user database is now in the **Collaboration Links** list of the DOORS database properties.
8. Click **OK** to close DOORS database properties.

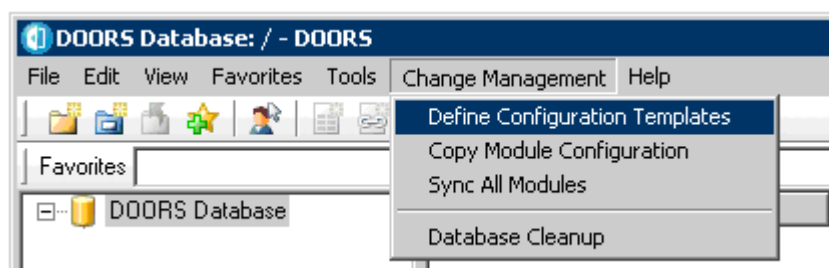




## Defining a template for the integration

Define a template in Rational DOORS. Note the Requirement Change Management feature supports the ClearQuest record type "RequirementsChangeRequest". Your ClearQuest schema requires the **RequirementsChangeRequest** package for that record type. You can also use the feature with another, existing record type (such as Defect) if you prepared your schema in that way.

1. Log into the Rational DOORS client with administrator privilege.
2. Select the menu option **Change Management > Define Configuration Templates**.

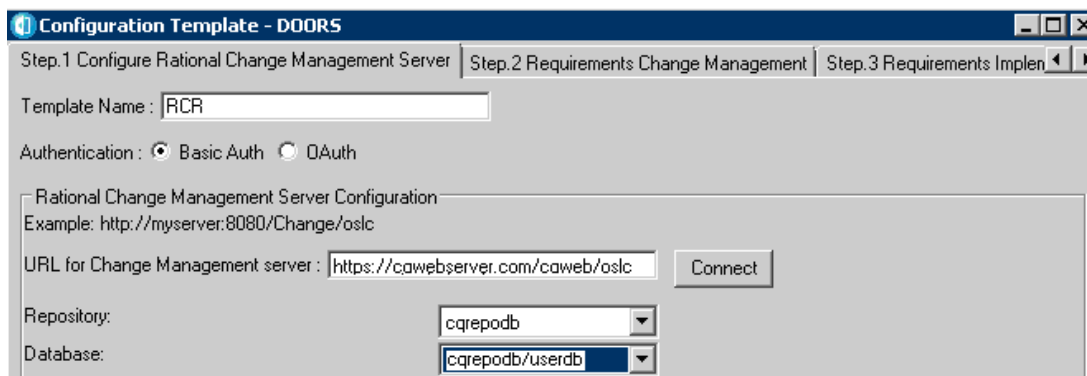


### Configure Rational Change Management Server

1. In the **Template Name** field, type the template name.
2. Select the method of authentication, either basic authentication or OAuth.
  - a) For basic authentication:
    - i. Enter the OSLC URL for the ClearQuest Web server. For example:

**https://server:port/change/oslc**

Note that the server URL might not need a port value.



- ii. Click **Connect**.
  - iii. Log into the ClearQuest system.
  - iv. Select the ClearQuest user database.
- b) For OAuth mode:
- i. Make sure you complete the steps to **Configure cross-server communication** in advance.
  - ii. If this is complete, you can select the ClearQuest user database right away.

3. Click **Next** to move to the **Step.2 Requirements Change Management** tab.

## **Requirements Change Management**

1. Enter the states in the **Values** section
  - a) If you are using the **RequirementsChangeRequest** record type, define these values: **Assigned, Review, Approved, Applied**.
  - b) If you are using an existing record type, enter the ClearQuest states that are appropriate for that record type. Use the state name as defined in the ClearQuest schema state transition matrix rather than the form label.
2. Check the **For ClearQuest** option.
  - a) If you are using the **RequirementsChangeRequest** record type: Enter "Apply" in the **Apply Action Attribute** field and "Review" in the **Review Action Attribute** field.

- b) If you are using an existing record type, enter the ClearQuest actions that are appropriate for that record type in the ClearQuest schema state transition matrix.

**Configuration Template - DOORS**

Step.1 Configure Rational Change Management Server | Step.2 Requirements Change Management | Step.3 Requirements Implemen

Values:

Assigned State:

Review State:

Approved State:

Applied State:

For ClearQuest

Apply Action Attribute:  Review Action Attribute:

For Rational Team Concert

Apply Action Attribute:  Review Action Attribute:

State Attribute:

RCR Submit Form:

Conflicting Proposal Behavior:

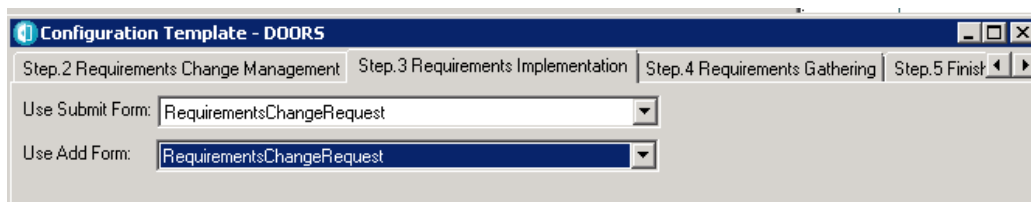
Show RCR Recording Report  Enable Reject button in DWA

3. Select the record type in the **RCR Submit Form** field.
4. In the **Conflicting Proposal Behavior** field, select the option **Take no action**.
5. Check the **Show RCR Recording Report** option to show the RCR Recording report.
6. To enable the **Reject** button on the Rational DOORS Web Access Requirement Change Management page, check **Enable Reject button in DWA**.
7. Click **Next** to display the **Step.3 Requirements Implementation** tab.

## Requirements Implementation

1. Enter the the appropriate forms for the appropriate ClearQuest record type in the **Use Submit Form** and **Use Add Form fields**.

**Note:** For all fields, select the options that are applicable to your schema and the record type chosen for implementation requests.



2. Click **Next** to display the **Step 4 Requirements Gathering** tab.

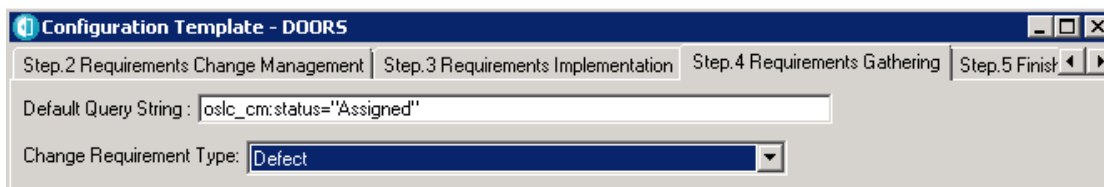
## Requirements Gathering

**Note:** Skip this step if you are not using the requirements gathering feature.

1. In the **Default Query String** field, enter the OSLC style query string used during requirements gathering. For example:

**oslc:cm:status="Assigned"**

2. Select your **Change Requirement Type**.



3. Click **Next** to display the **Step.5 Finish** tab.

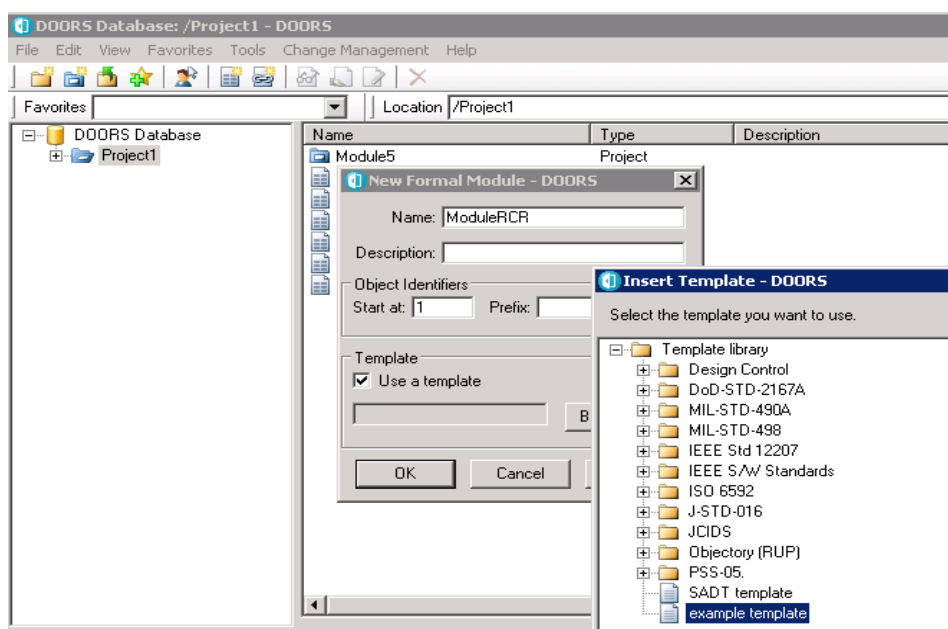
## Finish template configuration

1. In the **Template Summary**, review your selections. After your review, you can perform one of these actions:
  - a) If the information is correct, click **Finish** to save your configuration template.
  - b) If you need to correct the information, click **Back** to return to the correct tab and make the necessary corrections.

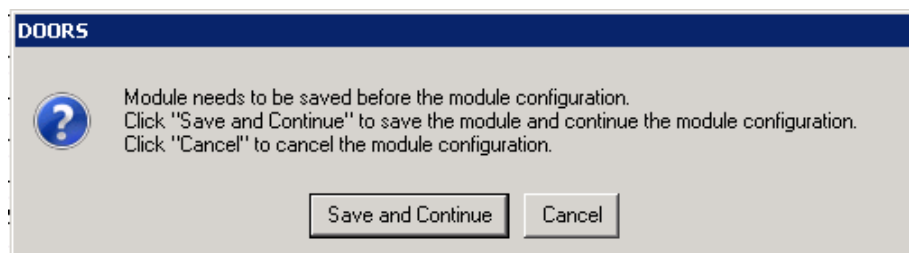
## Enabling the integration from the DOORS client

### Create the DOORS project and module for configuration

1. Log into the DOORS native client as Administrator.
2. Right click the DOORS Database and select **New > Project**.
3. Right click the created Project and select New > Formal Module.



4. Open the module.
5. Select the menu option **Change Management > Configure Module**.
6. Click **Save and Continue** when prompted.



## Enable Requirements Implementation

1. In the **Template Name** field, select the configuration template to use for this module.
2. To show the change management menus, select **ON** for the **Integration Status**.
3. Check the **Enable Requirements Implementation** option.
4. Check the **Create IR Attrs View** option.
5. Click **Save**

Configure Module for Change Management - DOORS

Use the following configuration template:

Template Name  
DefectRCM  
RCR

Integration Status :  ON  OFF

Enable Requirements Change Management

DOORS Attributes Managed by RCRs

Create RCR Attrs View

Manage External Links  Manage Internal DOORS Links

Enable Requirements Implementation

Map Attributes for CM IR Submission

Create IR Attrs View

Enable Requirements Gathering

Show Template Details

Save Close

## Enable Requirements Change Management

1. In the **Template Name** field, select the configuration template to use for this module.
2. To show the change management menus, select **ON** for the **Integration Status**.
3. Check the **Enable Requirements Change Management** option.
4. Check the **Create RCR Attrs View** option.
5. Check the **Manage External Links** option.
6. Check the **Manage Internal DOORS Links** option.

## 7. Click **Save**

Configure Module for Change Management - DOORS

Use the following configuration template:

Template Name: DefectRCM, RCR

Integration Status:  ON  OFF

Enable Requirements Change Management

DOORS Attributes Managed by RCRs

Create RCR Attrs View

Manage External Links  Manage Internal DOORS Links

Enable Requirements Implementation

Map Attributes for CM IR Submission

Create IR Attrs View

Enable Requirements Gathering

Show Template Details

Save Close

### ***Enable Requirements Gathering***

1. In the **Template Name** field, select the configuration template to use for this module.
2. To show the change management menus, select **ON** for the **Integration Status**.
3. Check the **Enable Requirements Gathering** option.
4. Click **Save**

Configure Module for Change Management - DOORS

Use the following configuration template:

Template Name: DefectRCM, RCR

Integration Status:  ON  OFF

Enable Requirements Change Management

DOORS Attributes Managed by RCRs

Create RCR Attrs View

Manage External Links  Manage Internal DOORS Links

Enable Requirements Implementation

Map Attributes for CM IR Submission

Create IR Attrs View

Enable Requirements Gathering

Show Template Details

Save Close

## Conclusion

This concludes the configuration for integrating Rational ClearQuest Web and Rational DOORS Web Access. You can now use the integration to carry out activities include requirements implementation, requirements change management, and requirements gathering. Use the steps in this white paper, the configuration provides you with extra security by taking advantage of SSL technology.

## References

Rational ClearQuest RequirementsChangeRequest Package:

<http://www.ibm.com/support/docview.wss?uid=swg24028401>

Configuring and using the OSLC-based Rational ClearQuest and Rational DOORS integration:

<http://www.ibm.com/support/docview.wss?uid=swg21456993>

Configuring Rational DOORS Web Access to use SSL:

[http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.inSTALL.doc/topics/t\\_configureSSL.html](http://publib.boulder.ibm.com/infocenter/doorshlp/v9/topic/com.ibm.rational.dwa.inSTALL.doc/topics/t_configureSSL.html)

DOORS Web Access secure (HTTPS) configuration instructions:

<http://www.ibm.com/support/docview.wss?uid=swg21574687>



## Copyrights, trademarks, and disclaimers

IBM, the IBM logo, ibm.com, WebSphere, and Rational are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS DOCUMENT, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS DOCUMENT OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS DOCUMENT IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REDOCUMENTS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2012. All rights reserved.