

Need to Know Component Administration Guide
10g Release 3 (10.1.3.3.3)

April 2008

Need to Know Component Administration Guide, 10g Release 3 (10.1.3.3.3)

Copyright © 2005, 2007, Oracle. All rights reserved.

Contributing Authors: Karen Johnson

Contributors: Scott Nelson

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents



Chapter 1: Introduction

Overview	1-1
Product Overview	1-1
Features	1-2
Applications	1-3
Requirements	1-3
Component Contents	1-4
About This Guide	1-4

Chapter 2: Installation and Configuration

Overview	2-1
Installing the NTK Component	2-1
Configuring the NTK Component	2-2

Chapter 3: Using the Need to Know Component

Overview	3-1
Security Configuration Customization	3-1
Content Security	3-2
Search Results	3-4
Hit List Roles	3-5
WHERE Clause Calculation	3-6
Content Metadata Security	3-6
Disclosure Query Security Applet	3-6
Query Syntax	3-9
Like Operator	3-9

Boolean Operators	3-10
UserName Variable	3-10
stdSecurity Variable	3-10
User Attribute Fields	3-10
User Roles	3-11
Defining a Content-Level Query	3-11
NTK Administration Interface	3-12
NTK Configuration Information Page	3-13
Content Security Configuration Information Page	3-18
Search Results Configuration Information Page	3-23
Hit List Roles Configuration Information Page	3-26
Test NTK Content Security Page	3-27

Chapter 4: Security Customization Samples

Overview	4-1
Content Security Samples	4-1
Simple Idoc Script Function	4-2
Using stdSecurityCheck	4-2
Using isStrIntersect	4-2
Using allStrIntersect	4-3
Using includeNTKReadSecurityScript	4-3
Search Results Samples	4-4
Disabling Links	4-4
Changing Links	4-4
Changing Images	4-4
Hit List Roles Samples	4-5
Using the Query Hit List Role	4-5
Creating a Black Hole Check In	4-5

Appendix A: Third Party Licenses

Overview	A-1
Apache Software License	A-1
W3C® Software Notice and License	A-2
Zlib License	A-4
General BSD License	A-5
General MIT License	A-5
Unicode License	A-6
Miscellaneous Attributions	A-7

INTRODUCTION

OVERVIEW

This chapter covers the following topics:

- ❖ [Product Overview](#) (page 1-1)
- ❖ [Features](#) (page 1-2)
- ❖ [Requirements](#) (page 1-3)
- ❖ [Component Contents](#) (page 1-4)
- ❖ [About This Guide](#) (page 1-4)
- ❖ (page 1-5)

PRODUCT OVERVIEW

The Need to Know (NtkDocDisclosure or NTK) component supports customization for these Content Server security areas:

- ❖ Content security—Changing user access to content items.
- ❖ Search results—Modifying the display of search results.
- ❖ Hit list roles—Changing user credentials for query and check-in pages.
- ❖ Content metadata security—Altering the behavior of metadata changes for content items.
- ❖ WHERE clause calculation—Modifying use of the WHERE clause in searches.

For example, with standard security, users can only view content for which they have at least Read permission. The Need to Know component can change this in two ways:

- ❖ All users can be allowed to see content items from specified security groups in a search results list, even though they may not be able to view the metadata or document itself.
- ❖ Read and Write permission can be expanded or restricted within specified security groups using a query against content metadata and user attributes.

The Need to Know component provides an HTML administration interface to display security configuration status information, enable editing of security configuration values, and enable viewing and testing of Idoc Script for security configuration values.

FEATURES

The Need to Know function is implemented through the following features:

- ❖ The Need to Know component is applied by security group. You must identify which security groups will use the component. All content in the specified security groups will appear in the search results for all users.
- ❖ This component provides the option of making all accounts visible, so a user can get a search “hit” on a content item regardless of its account.
- ❖ The Security Group list on the Search page will show all specified security groups. If accounts are enabled, all accounts will appear in the Accounts list on the Search page.
- ❖ A new “DocDisclosureQuery” metadata field and new “hit list” role must be created to support the Need to Know function. The hit list role is given read access to all specified security groups.
- ❖ You can create new user attribute fields or use existing ones in Need to Know queries.
- ❖ When a document is checked in, a query can be defined in the “DocDisclosureQuery” metadata field. The query conditions can include content metadata and user attributes, and the query results determine access permission to the document. Queries can be entered manually in Idoc Script, or the Disclosure Query Security applet can be used to build the query.
- ❖ Whenever a user does a search, the hit list role is dynamically applied to the user, giving them read access to all content in the specified security groups. Each content item is then checked for a query in the “DocDisclosureQuery” field, which determines the user’s access to that content item.

- ❖ If the “DocDisclosureQuery” field is empty, standard security applies. Standard security can also be explicitly specified in the query field, or it can be used in a boolean combination with other document and user attributes to expand or refine the read access.
- ❖ If a query is entered for a content item that is not in an NTK security group, the query does not run, and standard security applies.
- ❖ If a user already has more than Write or higher access to the security group, the query in the “DocDisclosureQuery” field does not run, and standard security applies.
- ❖ A global query can be defined for all content, so individual queries do not have to be specified for each content item. You can set up the system to allow the global query to be overridden when a query is entered during check-in.

APPLICATIONS

This component can be used as the starting point for a more complicated security implementation, such as:

- ❖ Providing integrated tracking for downloads of sensitive documents.
- ❖ Controlling Write or higher privileges through custom logic.
- ❖ Implementing view limits and subscription control, where documents within a certain security group may only be downloaded so many times.
- ❖ Controlling access by incorporating entries from a custom database table or results from a custom API. This is a hook for externally controlled authorization.

REQUIREMENTS

The following considerations are important with regard to the Need to Know component:

- ❖ The 7.5 version of the Need to Know component runs on Stellent Content Server versions 6.2 and 7.x.



Note: The 7.5 version of the Need to Know component is not compatible with pre-6.2 versions of Stellent Content Server. You must obtain an earlier version of the Need to Know component to work with an earlier version of SCS. Refer to the Extras link on the Stellent support website for complete listings of available NTK component versions and their compatibility with SCS versions.

COMPONENT CONTENTS

The Need to Know component file, NeedToKnow.zip, is available for download from the Stellent support website and is included with the samples and extras. The Zip file contains the following files:

Description	Filename
Component files	*.hda *.class *.htm *.zip
Class files	idcdisclosure.zip


ABOUT THIS GUIDE




This guide provides instructions to install the Need to Know component on the Content Server. The information contained in this document is subject to change as the product technology evolves and as hardware, operating systems, and third-party software are created and modified.

Conventions

The following conventions are used throughout this guide:

- ❖ The notation *<Install_Dir>/* is used to refer to the location on your system where the content server instance is installed.
- ❖ Forward slashes (/) are used to separate the directory levels in a path name. A forward slash will always appear after the end of a directory name.
- ❖ Notes, technical tips, important notices, and cautions use these conventions:

Symbols	Description
	This is a note. It is used to bring special attention to information.

Symbols	Description
	This is a technical tip. It is used to identify information that can be used to make your tasks easier.
	This is an important notice. It is used to identify a required step or required information.
	This is a caution. It is used to identify information that might cause loss of data or serious system problems.

INSTALLATION AND CONFIGURATION

OVERVIEW

This chapter covers the following topics:

- ❖ [Installing the NTK Component](#) (page 2-1)
- ❖ [Configuring the NTK Component](#) (page 2-2)

INSTALLING THE NTK COMPONENT

Install the component using either Component Wizard or the Component Manager as follows:

Component Wizard Installation

1. Start the Component Wizard by selecting **Start—Programs—Oracle Content Server—<instance>—Utilities—Component Wizard**.

The Component Wizard main screen and the Component List screen are displayed.

2. On the Component List screen, click **Install**.

The Install screen displays.

3. Click **Select**. Navigate to the NeedToKnow.zip file and select it.

4. Click **Open**.

The zip file contents are added to the Install screen list.

5. Click **OK**.
6. The Component Wizard asks if you want to enable the NTK component. Click **Yes**.
The NTK component is listed as enabled on the Component List screen.
7. Continue by following the procedure in [Configuring the NTK Component](#) (page 2-2).

Component Manager Installation

1. Open the Administration tray.
2. Click the Admin Applets option to open the Administration page.
3. Click the Admin Server link.
4. Click the applicable content server instance.
5. Select the Component Manager link.
The Component Manager screen is displayed.
6. Select **Browse** next to the Install New Component box. Navigate to the NeedToKnow.zip file and select it.
7. Click **Install**.
8. After the installation has been successful, highlight the NTK component in the right (disabled) screen.
9. Click **Enable**.
A message will appear prompting you to restart the server.
10. Continue by following the procedure in [Configuring the NTK Component](#) (page 2-2).

CONFIGURING THE NTK COMPONENT

This section describes the procedure to set up a basic security configuration using the Need to Know component. This procedure explains how to set up security configuration variables, a custom metadata field, and a hit list role. After you have set up the basic configuration, you can use the Need to Know component interface to edit, test, and improve the security configuration.



Note: If you used the Component Wizard to install the Need to Know component, you will need to open the Admin Server page for the applicable content server instance before starting the procedure. Otherwise, if you used the Component Manager, the Admin Server page is already open.

1. Select the General Configuration link on the left side bar in the Admin Server page.
2. Under the Additional Configuration Variables heading on the General Configuration page, scroll to the bottom of the text area, and add the following text:

`SpecialAuthGroups=<group1>, <group2>, . . .`

- Replace `<group1>`, `<group2>`,... with the security groups that will use the Need to Know component.
- Security groups must be entered in lower case.
- Any security groups not listed will have standard security applied.



Note: Other products such as Records Management also can use the SpecialAuthGroups configuration variable, so be careful to use unique names for security groups that will use the Need to Know component.

3. If you want to specify content item-level queries, use the Configuration Manager to add a new metadata field. (This is not necessary if you will be using only the global query.) A new metadata field must be added by using the Configuration Manager; it cannot be added from the Need to Know component interface.
 - You can use any field name and title you wish, such as *DocDisclosureQuery* or *NeedToKnow*.
 - The field must be specified as a memo field.
 - After adding the field, you will need to click **Update Database Design**, and then click **Rebuild Search Index**.



Note: If your content server instance already has a large amount of content, rebuilding the search index can take a long time (up to a couple of days). Consider rebuilding during system maintenance periods or at times of non-peak system usage.

4. Use the User Admin administration applet to add a hit list role.
 - You can use any role name you wish, such as *hitlist* or *NTKrole*.
 - Give Read access to all the security groups that were specified in the SpecialAuthGroups configuration entry.
 - If you want the security groups that were specified in the SpecialAuthGroups configuration entry to be listed on the check-in page or update page, you will need to give Write access to this role.
 - You can create two different hit list roles with different names and permissions. One role can be configured with the Need to Know component to be a Query role

in a content search, and the other role can be configured with the Need to Know component to be an Update role in content check-ins and updates.

- Do not assign this role to any users. If the hit list role is configured to be a Query or Update role, it is automatically added to the user's attributes.
5. If you want to set user access permissions that extend the limits of Need to Know security, use the General Configuration page to include extra security configuration settings in the Additional Configuration Variables section. Scroll to the bottom of the text area and enter the configuration settings as necessary.
 6. If you want to add new user attribute fields for use in Need to Know queries, use the User Admin tool to add user attribute fields.
 7. Restart the content server.



Note: When the Need to Know component has been installed, certain security configuration values are stored in the `<Install_Dir>/<instance>/data/needtoknow/ntk_config.hda` file. These values can be edited by using the Need to Know administration interface, described in Chapter 3, or by directly editing the `ntk_config.hda` file.

USING THE NEED TO KNOW COMPONENT

OVERVIEW

This chapter covers the following topics:

- ❖ [Security Configuration Customization](#) (page 3-1)
- ❖ [Disclosure Query Security Applet](#) (page 3-6)
- ❖ [Query Syntax](#) (page 3-9)
- ❖ [Defining a Content-Level Query](#) (page 3-11)
- ❖ [NTK Administration Interface](#) (page 3-12)

SECURITY CONFIGURATION CUSTOMIZATION

The Need to Know component provides additional security configuration support focused on the following areas:

- ❖ [Content Security](#)—Changing user access to content items.
- ❖ [Search Results](#)—Changing the display of search results.
- ❖ [Hit List Roles](#)—Changing user credentials for query and check-in pages.

- ❖ **WHERE Clause Calculation**—Changing use of the WHERE clause in searches.
- ❖ **Content Metadata Security**—Changing the behavior of metadata changes for content items.

Content Security

Standard security uses security roles, groups, and accounts to determine if a user has the appropriate privilege level to access a content item. The Need to Know component enables you to customize the process of determining user privilege. You can use the Need to Know component interface to set configuration fields and create Idoc Script to specify Read, Write, and Delete privilege levels. The Idoc Script can also contain user and content metadata values.

The Need to Know component computes content security using the following process:

1. A user clicks a link to view content information.
2. If the user has the “admin” role, standard security is used and the user can view the content.
3. If the security group of the content item is not a Need to Know authorization group, then standard security is used to evaluate the user’s Read request.
4. If Need to Know security is not enabled at the Read privilege level, then standard security is used to evaluate the user’s Read request.
5. If Need to Know security is not limited at the Read privilege level, and the user has standard security access to the content item, the user is given access to the content.
6. The Need to Know security Idoc Script (in this case the Read security script) is evaluated.
7. The Need to Know access flag (in this case, isNTKReadAccess) is evaluated to determine if the user has access to the content. Access is allowed or denied based on the Need to Know access flag.

The Need to Know component also enables you to test security configuration scripts for each access level: Read, Write, and Delete. For a test you can specify a user and a content ID, and you have the option of specifying roles and accounts. These attributes are used in the test instead of the user’s actual attributes. For example, you could test Idoc Script using an external user whose attributes may not be accessible. After the test is run, the component reports on whether the user has access to the content item, whether Need to Know security was used, and if Need to Know security was not used then the reason why.

For information on using the Need to Know component interface to configure content security, refer to the [NTK Configuration Information Page](#) (page 3-13) and the [Content Security Configuration Information Page](#) (page 3-18). For samples of Idoc Script that can configure content security, refer to [Chapter 4 \(Security Customization Samples\)](#).

The following Idoc Script functions can be used in the Script fields to determine content security. For additional information on Idoc Script refer to the *Idoc Script Reference Manual*.

Idoc Script	Description
allStrIntersect	Takes two required comma-delimited strings and one optional Boolean flag as parameters. If all values in the second string occur in the first string, the function returns true. If the optional parameter is set to true and the second value is an empty string, the function returns true. By default, the optional parameter is false. The comparison of values in the comma-delimited strings are not case sensitive.
includeNTKDeleteSecurityScript	Evaluates the Delete security script and makes the isNTKDeleteAccess variable available for use in the Read or Write security scripts. If this function is used in the Delete security script, it is ignored.
includeNTKReadSecurityScript	Evaluates the Read security script and makes the isNTKReadAccess variable available for use in the Write or Delete security scripts. If this function is used in the Read security script, it is ignored.
includeNTKWriteSecurityScript	Evaluates the Write security script and makes the isNTKWriteAccess variable available for use in the Read or Delete security scripts. If this function is used in the Write security script, it is ignored.

Idoc Script	Description
isDisclosureQuery	Evaluates the query for the disclosure field (if specified) and returns true or false. An optional parameter can be specified to determine if the function should return true or false if the disclosure query is empty. If the disclosure field has not been specified or does not exist, this function always returns false.
isMetaChange	This variable is set if the content security call involves a content update or a check in.
isStrIntersect	Takes two required comma-delimited strings and one optional Boolean flag as parameters. If at least one value in the second string occurs in the first string, the function returns true. If the optional parameter is set to true and the second value is an empty string, the function returns true. By default, the optional parameter is false. The comparison of values in the comma-delimited strings are not case sensitive.
stdSecurityCheck	Checks standard security for the current access level. For example, if the function is in the Read security script, it checks security at the Read access level.

Search Results

The Need to Know component enables you to customize the presentation of the search results that are returned from a search query. Two configuration values can be set using the NTK interface: Hidden Fields, and Script.

The Hidden Fields value is a list of fields that can be hidden from view on the Search Results page. The values are set to empty strings. To hide the fields, the field hideFields must be set in the component search results Idoc Script.

Idoc Script controls the presentation of the search results. Idoc Script is evaluated for each row in the search results. A number of fields can be set in script to alter the presentation of search results. To see the list of fields and how to use the Need to Know component interface to customize script for search results presentation, refer to the [Search Results Configuration Information Page](#) (page 3-23).

The Need to Know component uses the securityCheck Idoc Script function to determine search results presentation. The securityCheck function checks the security against the current content item (standard security or Need to Know security), depending on the configuration values. The function has an option parameter to determine what access level to check:

- 1 = Read
- 2 = Write
- 4 = Delete
- 8 = Admin

If no parameter is used with securityCheck, by default it checks the Read access level.

For examples of Idoc Script that can alter search results presentation, refer to [Chapter 4 \(Security Customization Samples\)](#).

Hit List Roles

Hit list roles enable you to change user credentials for using content Search, Content Check In, and Update pages. Using the User Admin applet, you can add a hit list role with any name you wish. You don't assign the role to a user; when the role is enabled it is automatically added to a user's attributes when doing a search, check in, or update. When creating a hit list role, you need to give Read access to all the security groups that you specify in the SpecialAuthGroups configuration entry. If you want these security groups to be listed on the Content Check In page or Update page, you also need to add Write access to the hit list role.

Using the Need to Know component Hit List Roles Configuration Information page, you can implement hit list roles in two forms: Query and Update. A hit list role used in a query is applied to content searches. A hit list role used in an update is applied to content check-ins and updates.

For additional information about how to use hit list roles, refer to [NTK Administration Interface](#) (page 3-12) and [Hit List Roles Configuration Information Page](#) (page 3-26). For samples of using hit list roles, refer to [Chapter 4 \(Security Customization Samples\)](#).

WHERE Clause Calculation

The Need to Know component provides two filters that enable you to customize the query WHERE clause that is used to retrieve search results:

- ❖ `preDetermineWhereClause`—Overrides the entire WHERE clause.
- ❖ `postDetermineWhereClause`—Appends to the standard security WHERE clause.

The code for these filters is located in the `NTKFilter` Java class. For samples of how these filters work, refer to [Chapter 4 \(Security Customization Samples\)](#).

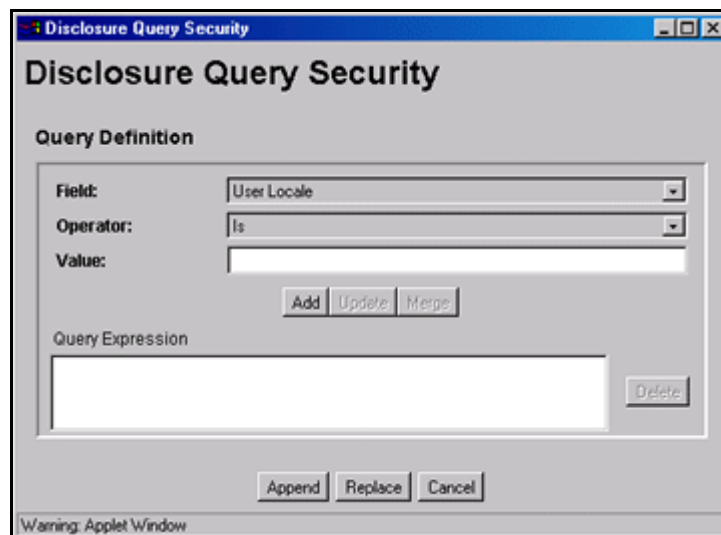
Content Metadata Security

The Need to Know component provides a filter called `checkMetaChangeSecurity` that enables you to alter the behavior of metadata changes when a content item is checked in or updated.


The code for this filter is located in the `NTKFilter` Java class. For an example of how the filter works, refer to [Chapter 4 \(Security Customization Samples\)](#).

DISCLOSURE QUERY SECURITY APPLET

The Disclosure Query Security applet is used to define a query for a particular content item during check-in. To access the applet, click the Update button next to the `DocDisclosureQuery` field on the Content Check In Form page.



Feature	Description
Field field	Select a user attribute field to be specified in the query. This list includes User Locale, User Name, User Role, and all of your custom user attribute fields.
Operator field	<p>Select an operator to apply to the Field and Value. The following operators are used for all fields except User Role:</p> <p>Is—The value in the specified Field matches the specified Value.</p> <p>Is Not—The value in the specified Field does not match the specified Value.</p> <p>Begins With—The value in the specified Field starts with the specified Value.</p> <p>Contains—The value in the specified Field contains the specified Value.</p> <p>The User Role field has only one operator, Has Member, and displays a drop-down list of roles in the Value field.</p>
Value field	<p>Enter the value to be specified in the query.</p> <ul style="list-style-type: none"> • If an option list was specified for the selected field, choose the value from the drop-down list. • If no option list was specified for the selected field, type the value in the text box.
Add button	Enters the query specified by the Field, Operator, and Value fields into the Query Expression text box. Each click of the Add button appends the current settings to the query as an AND clause.
Update button	Updates a selected query clause with the parameters specified in the Field, Operator, and Value fields.

Feature	Description
Merge button	<p>Creates an OR clause (inserts a pipe character) for the selected query clause. This button is enabled under the following conditions:</p> <ul style="list-style-type: none"> • The Field in the drop-down list matches the Field specified in the selected query clause. • The Operator in the selected query clause cannot be “Is Not”. • The Operator in the drop-down list cannot be “Is Not”. <p> Note: The pipe character does not appear in the Query Expression for a User Roles query clause, but it will appear in the DocDisclosureQuery field.</p>
Query Expression	Displays each clause of the query as a single line.
Delete button	Deletes the selected query clause.
Append button	Appends the Query Expression to any existing query in the DocDisclosureQuery field on the Content Check In Form page.
Replace button	Replaces any existing query in the DocDisclosureQuery field on the Content Check In Form page with the Query Expression.
Cancel button	Closes the Disclosure Query Security applet without applying any query changes.

QUERY SYNTAX

The Disclosure Security Query applet creates queries with the correct Idoc Script syntax, but you can also enter your own queries directly in the DocDisclosureQuery field. The following Idoc Script syntax is used in disclosure queries:

- ❖ [Like Operator](#) (page 3-9)
- ❖ [Boolean Operators](#) (page 3-10)
- ❖ [UserName Variable](#) (page 3-10)
- ❖ [stdSecurity Variable](#) (page 3-10)
- ❖ [User Attribute Fields](#) (page 3-10)
- ❖ [User Roles](#) (page 3-11)



Tech Tip: You can learn how to correctly format query clauses for direct entry in the DocDisclosureQuery field by experimenting with the [Disclosure Query Security Applet](#) (page 3-6).

Like Operator

The **like** operator matches substrings and wildcard strings. Enclose all strings in single quotes.

Substrings

Use the **like** operator to match substrings.

Wildcard Strings

Use wildcard strings to match variable characters and options. Wildcard strings use the syntax:

* = Match 0 or more characters

? = Match exactly 1 character

| = Separates multiple options, only one of which needs to match

For example:

```
dDocName like '*MyClient*|199? Reports'
```

would match “MyClient”, “3rd Quarter MyClient Report”, “MyClient Visit”, “Meeting with MyClient”, and “1996 Reports”. This string would not match “My Client”, “All 1996 Reports”, or “1996 Report”.

Boolean Operators

Query clauses can be joined by **and**, **or**, and **not** Boolean operators.

- ❖ The Boolean operators must be lower case.
- ❖ Each clause must be in parentheses. For example:

```
(uRoles like '*:contributor:*') and (uUserLocale like 'hq')
```

UserName Variable

The variable **UserName** is the name of the user who is currently logged in. For example:

```
UserName like 'jgreen|hbrown'
```

would grant privileges only to the users *jgreen* or *hbrown*.

stdSecurity Variable

The variable **stdSecurity** specifies the standard security model; it is mapped to the `stdSecurityCheck` Idoc Script function. This variable can be used in Boolean combination with other query clauses to refine access (using the `and` operator) or expand access (using the `or` operator). For example:

```
stdSecurity or UserName like 'jgreen|hbrown'
```

would grant access to the document if the user would normally be able to access the document or they are *jgreen* or *hbrown*.

User Attribute Fields

When specifying user attribute fields in a query, use the format *uFieldName*. For example:

```
uMyUserField like 'Value'
```


User Roles

User roles require a special form because the UserRoles Idoc Script function returns all the roles for the current user in comma delimited form. (In this example, a *uRoles* shortcut has been defined for this function.) For example, the uRoles value could be:

```
role1,role2,...,role10
```

Therefore, to specify a query string that includes the value *role1*, wildcards must be included so that the query will recognize the value regardless of its position in the role list. For example:

```
uRoles like '*role1*'
```

However, this query string would also grant security access to a user with the role *role10*, which might not be a role you want to include. To limit the uRoles value to only those roles specified in the query, you need to use the DelimitedUserRoles function and syntax, which includes single quotes and colons on each side of the role value as follows:

```
uRoles like '*:role1:*
```

To match either *role1* or *role2*, use this syntax:

```
uRoles like '*:role1:*|*:role2:*
```

DEFINING A CONTENT-LEVEL QUERY

Use the following procedure to define a query for an individual content item:

1. Display the Content Check In Form page (for a new content item) or the Info Update Form page (for an existing content item).
2. Click the Update button next to the DocDisclosureQuery field (the name of this field will be whatever you named it during installation).

The [Disclosure Query Security Applet](#) (page 3-6) is displayed.

3. Choose a Field, an Operator, and a Value to create a query clause.
4. Click **Add**.

The query clause is added to the Query Expression text box.

5. Continue building the query:
 - To add another query clause with an **and** operator, enter the values and click **Add**.
 - To change an existing query clause, enter the new values, select the query line you want to change, and click **Update**.
 - To create an **or** clause, enter the new values, select the query line you want to change, and click **Merge**.
 - To delete a query clause, select the query line and click **Delete**.
6. Enter the query expression in the DocDisclosureQuery field.
 - To replace the existing query in the DocDisclosureQuery field with the query expression in the applet, click **Replace**.
 - To append the query expression in the applet to the existing query in the DocDisclosureQuery field, click **Append**.

The Disclosure Query Security applet converts the query clauses to the appropriate syntax for the query and enters the query in the DocDisclosureQuery field on the Content Check In Form or Info Update Form page.



Tech Tip: You can learn how to correctly format query clauses for direct entry in the DocDisclosureQuery field by experimenting with the Disclosure Query Security applet.

7. After filling out the rest of the fields, click **Check In** or **Update**.

The disclosure query is validated, and if the query is ill-formed, an error message tells you the specific problem with the query.

NTK ADMINISTRATION INTERFACE

After the Need to Know component has been installed, the NTK Configuration Information link is available through the Administration tray or menu. This link provides access to the NTK Configuration Information page, which provides security configuration status information and the capability to edit the security configuration.

The Need to Know component provides the following configuration pages:

- ❖ [NTK Configuration Information Page](#) (page 3-13)
- ❖ [Content Security Configuration Information Page](#) (page 3-18)
- ❖ [Search Results Configuration Information Page](#) (page 3-23)

- ❖ [Hit List Roles Configuration Information Page](#) (page 3-26)
- ❖ [Test NTK Content Security Page](#) (page 3-27)

NTK Configuration Information Page

The NTK Configuration Information page provides information about Need to Know content security configuration, search results configuration, and hit list roles configuration. This page also enables you to edit the security configuration, edit the search results configuration, edit the hit list roles configuration, view Idoc Script and hidden fields for the configuration, and test Idoc Script. To access this page, select **Administration—NTK Configuration Information** from the main menu.

NTK Configuration Information

Content Security Configuration Information

Access Level	Enabled	Limit Access	Script
Read	No	No	View Test
Write	No	No	View Test
Delete	No	No	View Test

Disclosure Field: <none>
 Security Auth Groups: <All Special Auth Groups>
 Debug: No

Search Results Configuration Information

Hidden Fields: [View](#)
 Script: [View](#)

Hit List Roles Configuration Information

Query Role: <none>
 Update Role: <none>
 Allow Hit List Role for Anonymous Users: No

Feature	Description
Content Security Configuration Information	
Access Level column	Displays the permission levels (Read, Write, Delete) for access to content items.
Enabled column	<p>Indicates whether Need to Know security is enabled for Read, Write, or Delete access.</p> <p>No—Need to Know security is disabled for the access level. This is the default.</p> <p>Yes—Need to Know security is enabled for the access level.</p>
Limit Access column	<p>Specifies whether Read, Write, and Delete access is limited by Need to Know security. If Need to Know security is used to limit user access, it does so regardless of whether the user has standard Read, Write, or Delete access to a content item. If Need to Know security is not used to limit user access, the user has standard access to a content item. This feature enables you to create a security model more restrictive than the standard security model.</p> <p>No—Access is not limited by Need to Know security. This is the default.</p> <p>Yes—Access is limited by Need to Know security.</p>

Feature	Description
Script column	<p>Provides links to view or test Idoc Script that is evaluated to determine if a user has Read, Write, or Delete access to a content item. The Need to Know component uses one of three parameters as a flag to determine if access is given:</p> <ul style="list-style-type: none">Read access—<code>isNTKReadAccess</code>Write access—<code>isNTKWriteAccess</code>Delete access—<code>isNTKDeleteAccess</code> <p>Click View in the row for the access level for which you want to view the Idoc Script that the Need to Know component evaluates to determine if a user has Read, Write, or Delete access.</p> <p>Click Test in the row for the access level for which you want to test the Need to Know security configuration. The NTK Test Content Security page is displayed. You can use this page to create and run a test of Idoc Script for security configuration. For more information refer to Test NTK Content Security Page (page 3-27)</p>

Feature	Description
Disclosure Field option	<p>Displays the custom metadata field that is evaluated for the Idoc Script function <code>isDisclosureQuery</code>. The disclosure field can be used to create a content-specific query. The default value is <code><none></code>.</p> <p>Use the Configuration Manager to create this field, and make it a memo field type. For more information refer to Chapter 2 (Installation and Configuration).</p> <p>When the disclosure field exists, an Update button is displayed next to the field where it appears on the Content Check In Form page. Click the button to access the Disclosure Query Security Applet (refer to Disclosure Query Security Applet (page 3-6)). The applet helps you create queries based on the user metadata.</p>
Security Auth Groups option	<p>Displays a list of security groups for which Need to Know security is used. The groups must be a subset of the <code>SpecialAuthGroups</code> configuration variable. If no groups are selected, all <code>SpecialAuthGroups</code> are used. The default value for <code>SpecialAuthGroups</code> is <code><All Special Auth Groups></code>.</p> <p>Use the Configuration Manager to specify a <code>SpecialAuthGroups</code> value in the <code>config.cfg</code> file. For more information refer to Chapter 2 (Installation and Configuration).</p>

Feature	Description
Debug option	<p>Displays the status of the debugging option.</p> <p>Yes—Debugging information is written to a log file for any security check that occurs for a content item. Users with the administrator role are not logged because they always receive access to the content item.</p> <p>No—Debugging information is not written to a log file.</p>
Edit button	Displays the Content Security Configuration Information page, where the content security configuration can be changed.
Search Results Configuration Information	
Hidden Fields field	Click View to display a list of fields that can be hidden on the Search Results page.
Script field	Click View to display the Idoc Script that controls the presentation of the Search Results page.
Edit button	Displays the Search Results Configuration Information page, where the search results security configuration can be changed.
Hit Lit Roles Configuration Information	
Query Role field	Displays the name of the query role, or <none>. This role is applied on the Search query page.
Update Role field	Displays the name of the update role, or <none>. This role is applied on a content check-in or update page.

Feature	Description
Allow Hit List Role for Anonymous Users field	Applies the hit list role for anonymous users. No —The hit list role is not applied for anonymous users. This is the default value. Yes —The hit list role is applied for anonymous users.
Edit button	Displays the Hit List Roles Configuration Information page, where the hit list roles security configuration can be changed.

Content Security Configuration Information Page

The Content Security Configuration Information page enables you to change security and access configuration for Read, Write, Delete, and other options for the Need to Know component. To access this page, click **Edit** in the Content Security Configuration Information area of the NTK Configuration Information page.

Content Security Configuration Information

[NTK Configuration Information](#) --> Content Security Configuration Information

Read Options

Use Security

Limit Access

Script

Write Options

Use Security

Limit Access

Script

Delete Options

Use Security

Limit Access

Script


Other Options


Disclosure Field

Security Auth Groups All Auth Groups

Debug

Feature	Description
Read Options	
Use Security list	Use security as specified in the Script field. No —Do not use Need to Know content security. This is the default value. Yes —Use Need to Know content security.
Limit Access list	Limit access permissions as specified in the Script field. No —Do not limit access permissions. This is the default value. Yes —Limit access permissions.
Script field	Enter IdocScript in this field to specify the Need do Know security configuration for Read permission.
Write Options	
Use Security list	Use security as specified in the Script field. No —Do not use Need to Know content security. This is the default value. Yes —Use Need to Know content security.
Limit Access list	Limit access permissions as specified in the Script field. No —Do not limit access permissions. This is the default value. Yes —Limit access permissions.
Script field	Enter IdocScript in this field to specify the Need to Know security configuration for Write permission.

Feature	Description
Delete Options	
Use Security list	Use security as specified in the Script field. No —Do not use Need to Know content security. This is the default value. Yes —Use Need to Know content security.
Limit Access list	Limit access permissions as specified in the Script field. No —Do not limit access permissions. This is the default value. Yes —Limit access permissions.
Script field	Enter IdocScript in this field to specify the Need to Know security configuration for Delete permission
Other Options	
Disclosure Field field	Select the name of a disclosure field from the list. This field is used to configure security in a content-specific query.  Note: If you create a metadata field for content item-level queries using the Configuration Manager, that field will appear as an option in the list.
Security Auth Groups field	Enter the SpecialAuthGroups to be used in content-specific queries. If you use the General Configuration page to create a specific security group for the Need to Know component, you can specify the group here. If you need to add a security group, you can also edit the Additional Configuration Variables SpecialAuthGroups value in the config.cfg file.

Feature	Description
All Auth Groups check box	<p>Specifies that the Need to Know component use all SpecialAuthGroups instead of a specific group listed in the Security Auth Groups field. This check box is selected by default.</p> <p> Note: Other products such as Records Management can also use the SpecialAuthGroups variable. Be careful to specify only the security groups you want to use the Need to Know security configuration.</p>
Debug list	<p>Select whether to use debugging to view security checking for a content item.</p> <p>Yes—Debugging information is written to a log file for any security check that occurs for a content item. Users with the administrator role are not logged because they always receive access to the content item.</p> <p>When debugging is used, two additional options are visible: View and Clear. Click View to view the log file of debugging information. Click Clear to empty the log file of information.</p> <p>No—Debugging is not used and information is not written to a log file. This is the default value.</p>
Update button	<p>Updates the content security information to use the new settings, restarts the Content Server, and returns you to the NTK Configuration Information page.</p>
Reset button	<p>Returns the Content Security configuration settings to their last saved values.</p>

Search Results Configuration Information Page

The Search Results Configuration Information page enables you to customize the search results that are returned from a search query. This does not affect what content items are returned, just how the results are displayed. To access this page, click **Edit** in the Search Results Configuration Information area of the NTK Configuration Information page.

Search Results Configuration Information

NTK Configuration Information --> Search Results Configuration Information

Hidden Fields

Available Fields

- Standard
- Content ID
- Content Type
- Title
- Author
- Security Group
- Score
- Account
- Release Date
- Expiration Date

<< Add

Remove >>

Script

Update Reset

Feature	Description
Hidden Fields box	Displays the list of fields that are hidden from view in a content search query result. The values are set to empty strings. These fields are hidden if the field <code>hideFields</code> is set in the search results script.
Available Fields box	Displays the list of fields that are included in a content search query result.
Add button	Select a field name and click Add to move the field from the Available Fields list to the Hidden Fields list, making the field hidden in a content search result.
Remove button	Select a field name and click Remove to move the field from the Hidden Fields list to the Available Fields list, making the field visible in a content search result.
Script field	<p>Enter Idoc Script in this field to control the presentation of search results. The Idoc Script is evaluated for each row in the search results. A number of fields can be set to alter the presentation:</p> <ul style="list-style-type: none"> • docInfo:enabled—Set to 0 to disable the content information link. • docInfo:link—Set to alter the content information page link. • docInfo:image_small—Set to alter the small image for the information link. • docInfo:image_large—Set to alter the large image for the information link. (This setting is not applicable for SCS version 7.5.) <p><i>(continued in next row of table)</i></p>

Feature	Description
Script field (continued)	<p><i>(continued from previous row in table)</i></p> <ul style="list-style-type: none"> • url:enabled—Set to 0 to disable the URL link. • url:link—Set to alter the URL link. • url:image—Set to alter the image for the URL link. • revHistory:enabled—Set to 0 to disable the revision history link. (This setting is not applicable for SCS version 7.5.) • revHistory:link—Set to alter the revision history link. (This setting is not applicable for SCS version 7.5.) • checkout:enabled—Set to 0 to disable to checkout link. • checkout:link—Set to alter the checkout link. • actions:enabled—Set to 0 to disable the actions popup link. • checkInSimilar:enabled—Set to 0 to disable the Check In Similar link. • email:enabled—Set to 0 to disable the email link. • dynConv:enabled—Set to 0 to disable the Dynamic Converter link.
Update button	Updates the configuration for search query results, restarts the Content Server, and returns you to the NTK Configuration Information page.
Reset button	Returns the Search Results configuration settings to their last saved values.

Hit List Roles Configuration Information Page

The Hit List Roles Configuration Information page enables you to configure hit list roles for users. To access this page, click **Edit** in the Hit List Roles Configuration Information area of the NTK Configuration Information page.

Hit List Roles Configuration Information

[NTK Configuration Information](#) --> Hit List Roles Configuration Information

Query Role

Update Role

Allow Hit List Role for Anonymous Users

Feature	Description
Query Role field	<p>Select the hit list role to be applied as the query role when the Search page is used. Security group roles with Read access are displayed in the list of selections, including any security group roles for which the user already has Read access.</p> <p>This role is separate from content security. You could have a content item appear in Search results configured for content security, but the user would not be able to view the Content Information page for that item.</p>

Feature	Description
Update Role field	<p>Select the hit list role to be applied as the update role when the Update page is used. Security group roles with Write access are displayed in the list of selections, including any security group roles for which the user already has Write access. When the content item is actually checked in or updated, this role is <i>not</i> applied.</p> <p>This field is probably most useful in conjunction with content security. For examples of using this field, refer to Chapter 4 (Security Customization Samples)</p>
Allow Hit List Role for Anonymous Users field	<p>Applies the hit list roles for anonymous users.</p> <p>No—Do not apply the hit list roles for anonymous users. This is the default value.</p> <p>Yes—Apply the hit list roles for anonymous users.</p>
Update button	Updates the hit list configuration, restarts the Content Server, and returns you to the NTK Configuration Information page.
Reset button	Returns the Hit List Roles configuration settings to their last saved values.

Test NTK Content Security Page

The Test NTK Content Security page enables you to run a test security script for a user. To access this page, click **Test** in the Script column for one of the access permission levels displayed on the NTK Configuration Information page.

Feature	Description
Access Level field	Displays the access level for the permissions level you select to test: Read, Write, or Delete.
Script field	Enter Idoc Script for the content security configuration to be tested.
User field	Enter the user ID for the test.
Set Attributes check box	Select the check box to automatically set the user attributes to match the user's existing attributes.
Roles field	Enter the roles assigned to the user for the test. Use this field if you are testing with external users where attributes may not be accessible.
Accounts	Enter the accounts assigned to the user for the test. Use this field if you are testing with external users where attributes may not be accessible.

Feature	Description
Content ID	Enter the content ID for the test.
Test button	Click Test to test the configuration specified on the Test NTK Content Security page. The Need to Know component test returns results on whether the user has the specified access, whether Need to Know security was used, and if Need to Know security was not used then the reason why.
Reset button	Returns the Test NTK Content Security configuration settings to their last saved values.

SECURITY CUSTOMIZATION SAMPLES

OVERVIEW

This chapter contains samples of security model customization:

- ❖ [Content Security Samples](#) (page 4-1)
- ❖ [Search Results Samples](#) (page 4-4)
- ❖ [Hit List Roles Samples](#) (page 4-5)

CONTENT SECURITY SAMPLES

This section contains samples of content security customization:

- ❖ [Simple Idoc Script Function](#) (page 4-2)
- ❖ [Using stdSecurityCheck](#) (page 4-2)
- ❖ [Using isStrIntersect](#) (page 4-2)
- ❖ [Using allStrIntersect](#) (page 4-3)
- ❖ [Using includeNTKReadSecurityScript](#) (page 4-3)

Simple Idoc Script Function

This sample allows Read access if the user *Color* custom field and the content *Color* custom field match.

```
<$if strEquals(uColor, xColor)$>
<$isNTKReadAccess=1$>
<$endif$>
```

Using stdSecurityCheck

This sample allows Read access if the user *Color* is *Blue* and the user has standard security to the content.

```
<$if stdSecurityCheck() and strEquals(uColor, "Blue")$>
<$isNTKReadAccess=1$>
<$endif$>
```

Using isStrIntersect

This sample returns true because 3 is a member of the first string.

```
<$if isStrIntersect("1,2,3,4", "5,3")$>
<$isNTKReadAccess=1$>
<$endif$>
```

This sample returns false because neither 5 or 6 is a member of the first string.

```
<$if isStrIntersect("1,2,3,4", "5,6")$>
<$isNTKReadAccess=1$>
<$endif$>
```

This sample returns false because the second string is empty and the third parameter is not specified.

```
<$if isStrIntersect("1,2,3,4", "")$>
<$isNTKReadAccess=1$>
<$endif$>
```

This sample returns true because the second string is empty and the third parameter is true.

```
<$if isStrIntersect("1,2,3,4", "", 1)$>
<$isNTKReadAccess=1$>
<$endif$>
```

This sample returns false because the second string is empty and the third parameter is false. Note that the third parameter can be a string (for example, "True" or "T") or a number (for example, 1, 0).

```
<$if isStrIntersect("1,2,3,4", "", 0)$>
<$isNTKReadAccess=1$>
<$endif$>
```

Using allStrIntersect

This sample returns false because 5 is not a member of the first string.

```
<$if allStrIntersect("1,2,3,4", "5,3")$>
<$isNTKReadAccess=1$>
<$endif$>
```

This sample returns true because 3 and 4 are members of the first string.

```
<$if allStrIntersect("1,2,3,4", "3,4")$>
<$isNTKReadAccess=1$>
<$endif$>
```

The samples in [Using isStrIntersect](#) (page 4-2) that use the third parameter would work the same with allStrIntersect.

Using includeNTKReadSecurityScript

Read script:

```
<$if strEquals(dDocType, "ADACCT")$>
<$isNTKReadAccess=1$>
<$endif$>
```

Write script:

```
<$includeNTKReadSecurityScript()$>
<$if isNTKReadAccess and strEquals(uColor, "Red")$>
<$isNTKWriteAccess=1$>
<$endif$>
```

The user has Write access to the content item if they have read access (type is *ADACCT*) and the user's *Color* is *Red*.

SEARCH RESULTS SAMPLES

This section contains samples of search results customization:

- ❖ [Disabling Links](#) (page 4-4)
- ❖ [Changing Links](#) (page 4-4)
- ❖ [Changing Images](#) (page 4-4)

Disabling Links

This sample disables the URL and Content Information link if the user does not have Read access to the content item. This could be used if you set the query role to show extra content items in the search results, but don't want users to see links to them.

```
<$if not securityCheck()$>
<$docInfo:enabled=0$>
<$url:enabled=0$>
<$endif$>
```

Changing Links

This sample alters the Content Information and URL link to another service if the *Color* of the content is *Red*.

```
<$if strEquals(xColor, "Red")$>
<$docInfo:link=HttpCgiPath & "?IdcService=GET_USER_INFO"$>
<$url:link="javascript:alert('Cannot view content.')"$>
<$endif$>
```

Changing Images

This sample alters the Content Information link if the *Color* of the content item is *Green*.

```
<$if strEquals(xColor, "Green")$>
<$docInfo:image_small=HttpImagesRoot &
"stellent/tree_icons/historical.gif"$>
<$endif$>
```


HIT LIST ROLES SAMPLES

This section contains samples of hit list roles customization:

- ❖ [Using the Query Hit List Role](#) (page 4-5)
- ❖ [Creating a Black Hole Check In](#) (page 4-5)

Using the Query Hit List Role

If you set the Query role to be *queryRole*, and *queryRole* has Write access to the security group *NTKGroup*, then *NTKGroup* will appear in the security group option list. You could then limit what content information appears by customizing the Search Results configuration values.

Creating a Black Hole Check In

By using the Update role, you could create a scenario where a user could check in a content item and then not be able to view or edit it. You would need to do the following:

1. Create a role called *updateRole* that has Read/Write access to the security group *NTKGroup*.
2. Update the Write content security script so that if a meta change is occurring and the security group is *NTKGroup*, allow access.

```
<$if isMetaChange and strEquals(dSecurityGroup, "NTKGroup")$>  
<$isNTKWriteAccess=1$>  
<$endif$>
```




THIRD PARTY LICENSES

OVERVIEW

This appendix includes a description of the Third Party Licenses for all the third party products included with this product.

- ❖ [Apache Software License](#) (page A-1)
- ❖ [W3C® Software Notice and License](#) (page A-2)
- ❖ [Zlib License](#) (page A-4)
- ❖ [General BSD License](#) (page A-5)
- ❖ [General MIT License](#) (page A-5)
- ❖ [Unicode License](#) (page A-6)
- ❖ [Miscellaneous Attributions](#) (page A-7)

APACHE SOFTWARE LICENSE

```
* Copyright 1999-2004 The Apache Software Foundation.  
* Licensed under the Apache License, Version 2.0 (the "License");  
* you may not use this file except in compliance with the License.  
* You may obtain a copy of the License at  
* http://www.apache.org/licenses/LICENSE-2.0  
*
```

- * Unless required by applicable law or agreed to in writing, software
- * distributed under the License is distributed on an "AS IS" BASIS,
- * WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
- * See the License for the specific language governing permissions and
- * limitations under the License.

W3C® SOFTWARE NOTICE AND LICENSE

- * Copyright © 1994-2000 World Wide Web Consortium,
- * (Massachusetts Institute of Technology, Institut National de
- * Recherche en Informatique et en Automatique, Keio University).
- * All Rights Reserved. <http://www.w3.org/Consortium/Legal/>
- *
- * This W3C work (including software, documents, or other related items) is
- * being provided by the copyright holders under the following license. By
- * obtaining, using and/or copying this work, you (the licensee) agree that
- * you have read, understood, and will comply with the following terms and
- * conditions:
- *
- * Permission to use, copy, modify, and distribute this software and its
- * documentation, with or without modification, for any purpose and without
- * fee or royalty is hereby granted, provided that you include the following
- * on ALL copies of the software and documentation or portions thereof,
- * including modifications, that you make:
- *
- * 1. The full text of this NOTICE in a location viewable to users of the
- * redistributed or derivative work.
- *
- * 2. Any pre-existing intellectual property disclaimers, notices, or terms

* and conditions. If none exist, a short notice of the following form
* (hypertext is preferred, text is permitted) should be used within the
* body of any redistributed or derivative code: "Copyright ©
* [\$date-of-software] World Wide Web Consortium, (Massachusetts
* Institute of Technology, Institut National de Recherche en
* Informatique et en Automatique, Keio University). All Rights
* Reserved. <http://www.w3.org/Consortium/Legal/>"
*
* 3. Notice of any changes or modifications to the W3C files, including the
* date changes were made. (We recommend you provide URIs to the location
* from which the code is derived.)
*
* THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS
* MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT
* NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR
* PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE
* ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.
*
* COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR
* CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR
* DOCUMENTATION.
*
* The name and trademarks of copyright holders may NOT be used in advertising
* or publicity pertaining to the software without specific, written prior
* permission. Title to copyright in this software and any associated
* documentation will at all times remain with copyright holders.
*

ZLIB LICENSE

* zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied
warranty. In no event will the authors be held liable for any damages
arising from the use of this software.

Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software
in a product, an acknowledgment in the product documentation would be
appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be
misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

GENERAL BSD LICENSE

Copyright (c) 1998, Regents of the University of California

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

"Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

"Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

"Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GENERAL MIT LICENSE

Copyright (c) 1998, Regents of the Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

UNICODE LICENSE

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories <http://www.unicode.org/Public/>, <http://www.unicode.org/reports/>, and <http://www.unicode.org/cldr/data/> . Unicode Software includes any source code published in the Unicode Standard or under the directories <http://www.unicode.org/Public/>, <http://www.unicode.org/reports/>, and <http://www.unicode.org/cldr/data/>.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2006 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in <http://www.unicode.org/copyright.html>.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in

the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

Unicode and the Unicode logo are trademarks of Unicode, Inc., and may be registered in some jurisdictions. All other trademarks and registered trademarks mentioned herein are the property of their respective owners

MISCELLANEOUS ATTRIBUTIONS

Adobe, Acrobat, and the Acrobat Logo are registered trademarks of Adobe Systems Incorporated.

FAST Instream is a trademark of Fast Search and Transfer ASA.

HP-UX is a registered trademark of Hewlett-Packard Company.

IBM, Informix, and DB2 are registered trademarks of IBM Corporation.

Jaws PDF Library is a registered trademark of Global Graphics Software Ltd.

Kofax is a registered trademark, and Ascent and Ascent Capture are trademarks of Kofax Image Products.

Linux is a registered trademark of Linus Torvalds.

Mac is a registered trademark, and Safari is a trademark of Apple Computer, Inc.

Microsoft, Windows, and Internet Explorer are registered trademarks of Microsoft Corporation.

MrSID is property of LizardTech, Inc. It is protected by U.S. Patent No. 5,710,835. Foreign Patents Pending.

Oracle is a registered trademark of Oracle Corporation.

Portions Copyright © 1994-1997 LEAD Technologies, Inc. All rights reserved.

Third Party Licenses

Portions Copyright © 1990-1998 Handmade Software, Inc. All rights reserved.

Portions Copyright © 1988, 1997 Aladdin Enterprises. All rights reserved.

Portions Copyright © 1997 Soft Horizons. All rights reserved.

Portions Copyright © 1995-1999 LizardTech, Inc. All rights reserved.

Red Hat is a registered trademark of Red Hat, Inc.

Sun is a registered trademark, and Sun ONE, Solaris, iPlanet and Java are trademarks of Sun Microsystems, Inc.

Sybase is a registered trademark of Sybase, Inc.

UNIX is a registered trademark of The Open Group.

Verity is a registered trademark of Autonomy Corporation plc

**A**

allStrIntersect function, 3-3

C

checkMetaChangeSecurity filter, 3-6
Component Manager installation, 2-2
Component Wizard installation, 2-1
content security
 Idoc Script functions, 3-3
 Need to Know process, 3-2
 overview, 3-2
Content Security Configuration Information page, 3-18
content security samples
 simple Idoc Script function, 4-2
 using allStrIntersect, 4-3
 using includeNTKReadSecurityScript, 4-3
 using isStrIntersect, 4-2
 using stdSecurityCheck, 4-2

D

define query for check-in
 procedure, 3-11
 using Disclosure Query Security applet, 3-6
 using DocDisclosureQuery field, 3-9
Disclosure Query Security applet, 3-6
DocDisclosureQuery field, 3-9

F

filters
 checkMetaChangeSecurity, 3-6
 postDetermineWhereClause, 3-6
 preDetermineWhereClause, 3-6

H

Hidden Fields configuration value, 3-4
hit list role
 configuring roles, 3-26
 overview, 3-5
Hit List Roles Configuration Information page, 3-26
hit list roles samples
 creating black hole check-in, 4-5
 using query role, 4-5

I

Idoc Script functions, 3-3
includeNTKDeleteSecurityScript function, 3-3
includeNTKReadSecurityScript function, 3-3
includeNTKWriteSecurityScript function, 3-3
installation
 using Component Manager, 2-2
 using Component Wizard, 2-1
isDisclosureQuery function, 3-4, 3-16
isMetaChange function, 3-4
isNTKDeleteAccess parameter, 3-15
isNTKReadAccess parameter, 3-15
isNTKWriteAccess parameter, 3-15
isStrIntersect function, 3-4

N

Need to Know
 features, 1-2
 overview, 1-1
 requirements, 1-3
 security implementation, 1-3
NTK Configuration Page, 3-13
NTK. See Need to Know
NtkDocDisclosure. See Need to Know

NTKFilter Java class, 3-6, 3-6

P

postDetermineWhereClause filter, 3-6
preDetermineWhereClause filter, 3-6

Q

query syntax
 Boolean operators, 3-10
 like operator, 3-9
 stdSecurity variable, 3-10
 substrings, 3-9
 user attribute fields, 3-10
 user roles, 3-11
 UserName variable, 3-10
 wildcard strings, 3-9

R

Records Management
 interaction with NTK, 3-22

S

Search Results Configuration Information page, 3-23

search results presentation
 customizing, 3-4
 settings, 3-24
search results samples
 changing images, 4-4
 changing links, 4-4
 disabling links, 4-4
securityCheck function, 3-5
SpecialAuthGroups
 use in content security, 3-16, 3-21, 3-22
 use in hit list role, 3-5
SpecialAuthGroups variable, 3-22
stdSecurityCheck function, 3-4
Stellent
 support, 1-5
support, 1-5

T

Test NTK Content Security page, 3-27
testing
 configuration scripts, 3-2
 security script, 3-27

W

WHERE clause
 customizing, 3-6