

**IBM® Content Analytics with Enterprise Search**

**Exploring the Security Dashboard**

**© Copyright IBM Corporation 2012**

## Exploring the Security Dashboard

The screenshot shows the IBM Content Analytics with Enterprise Search interface. The top navigation bar includes the IBM logo, the product name, and links for Search Customizer, Analytics Customizer, Log Out, Help, and About. Below this is a secondary navigation bar with tabs for Collections, System, and Security. The main content area displays three security categories: Application Login Security, Collection-Level Security, and System-Level Security, each with an 'Actions' dropdown menu. A blue tooltip box is overlaid on the System-Level Security section, providing a summary of the dashboard's capabilities and links to specific configuration pages.

IBM IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security Actions ▾

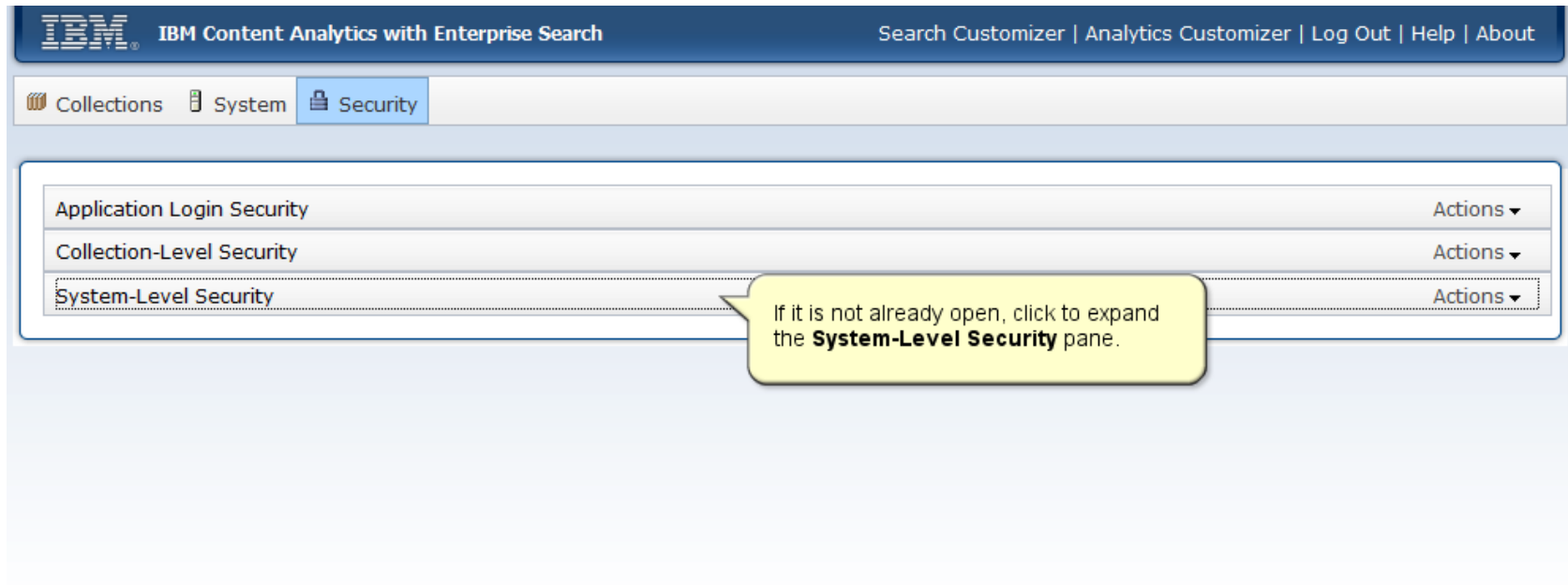
Collection-Level Security Actions ▾

System-Level Security Actions ▾

In the **Security** dashboard, you can:

- Control access to **applications** by configuring the embedded web application server to authenticate users when they log in to administer the system or query collections. [Skip to Application Login Security](#)
- Control access to **collections** by restricting connections to specific applications and by configuring document-level security controls. [Skip to Collection-Level Security](#)
- Control access to the **system** by assigning administrative roles, assigning privileges to specific users, and configuring connections between the system servers and your data source servers. [Skip to System-Level Security](#)

## Exploring the Security Dashboard



IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security	Actions ▾
Collection-Level Security	Actions ▾
System-Level Security	Actions ▾

If it is not already open, click to expand the **System-Level Security** pane.

# Exploring the Security Dashboard

The screenshot displays the IBM Content Analytics Security Dashboard. At the top, the IBM logo and 'IBM Content Analytics with Enterprise Search' are visible on the left, and navigation links for 'Search Customizer', 'Analytics Customizer', 'Log Out', 'Help', and 'About' are on the right. Below the header, there are tabs for 'Collections', 'System', and 'Security', with 'Security' being the active tab.

The main content area is divided into three sections: 'Application Login Security', 'Collection-Level Security', and 'System-Level Security'. The 'System-Level Security' section is expanded and contains three sub-tables:

- Administrative roles:** A table with columns for 'User ID' and 'Role'. It lists roles such as 'Default administrator', 'Master administrator', 'Operator', 'Monitor', 'Collection administrator', 'Content analytics administrator', 'Facet tree administrator', and 'Rule-based category administrator'.
- Application user privileges:** A table with columns for 'User or Group ID', 'Privileges', and 'Applicati ID'. It lists users like 'user 0' through 'user 4' with various privileges such as 'Save searches', 'Export documents', 'Create deep inspection reports', 'Add rules to categories', and 'Rebuild the category index'.
- Connection Credentials:** A table with columns for 'Name', 'Description', and 'Credentials'. It lists connections like 'Content Manager', 'DB2', 'Exchange Server', 'FileNet P8', 'Content Integrator', and 'JDBC'.

On the right side of the dashboard, there are three 'Actions' dropdown menus. A yellow callout bubble points to the top 'Actions' menu with the text: 'Click **Actions** to add users, groups, or connection credentials to the system.' A red circle highlights the middle 'Actions' menu, which has a dropdown menu open showing options: 'Add an administrative user', 'Add an application user or group', 'Specify default application user privileges', and 'Specify data source connection credentials'.

# Exploring the Security Dashboard

IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security Actions ▾

Collection-Level Security Actions ▾

System-Level Security Actions ▾

**Administrative roles**

User ID	Role	
esadmin	Default administrator	✎ 🗑
esadmin	Master administrator	✎ 🗑
cadmin	Operator	✎ 🗑
operator	Monitor	✎ 🗑
monitor	Collection administrator	✎ 🗑
taadmin	Content analytics administrator	✎ 🗑
facetadmin	Facet tree administrator	✎ 🗑
catadmin	Rule-based category administrator	✎ 🗑

**Application user privileges**

User or Group ID	Privileges	Applicati ID	
user 0	Save searches	0	✎ 🗑
user 1	Export documents	1	✎ 🗑
user 2	Create deep inspection reports	2	✎ 🗑
user 3	Add rules to categories	3	✎ 🗑
user 4	Rebuild the category index	0	✎ 🗑

**Connection credentials**

Data source	Connection ID	
Agent for Windows file systems	agent for windows fs	✎ 🗑
Content Manager	content manager	✎ 🗑
DB2	db2	✎ 🗑
Exchange Server	exchangeAdapt	✎ 🗑
FileNet P8	filenetp8	✎ 🗑
Content Integrator	iice	✎ 🗑
JDBC	jdbc	✎ 🗑

You can limit different administrative users to specific functions.

**Attention:** If you use WebSphere Application Server instead of the embedded application server, ensure that all users that you add are registered in the WebSphere LDAP server, including the default IBM Content Analytics with Enterprise Search administrator.

# Exploring the Security Dashboard

The screenshot displays the IBM Content Analytics Security Dashboard. At the top, the IBM logo and 'IBM Content Analytics with Enterprise Search' are on the left, and navigation links for 'Search Customizer | Analytics Customizer | Log Out | Help | About' are on the right. Below this is a navigation bar with 'Collections', 'System', and 'Security' tabs. The main content area is titled 'System-Level Security' and contains three tables: 'Administrative roles', 'Application user privileges', and 'Connection credentials'. A yellow callout box points to the 'Default administrator' role in the 'Administrative roles' table, stating: 'You cannot delete the default IBM Content Analytics with Enterprise Search administrator ID.'

Administrative roles	
User ID	Role
esadmin	Default administrator
esadmin	Master administrator
cadmin	Operator
operator	Monitor
monitor	Collection administrator
taadmin	Content analytics administrator
facetadmin	Facet tree administrator
catadmin	Rule-based category administrator

Application user privileges		
User or Group ID	Privileges	Application ID
user 0	Save searches	0
		1
		2
user 3	categories	3
user 4	Rebuild the category index	0

Connection credentials	
Data source	Connection ID
Agent for Windows file systems	agent for windows fs
Content Manager	content manager
DB2	db2
Exchange Server	exchangeAdapt
FileNet P8	filenetp8
Content Integrator	iice
JDBC	jdbc

# Exploring the Security Dashboard

IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security Actions ▾

Collection-Level Security Actions ▾

System-Level Security Actions ▾

You can grant advanced privileges to all users or to specific users and user groups, such as allowing all users to save searches or allowing specific users to export documents.

If you use WebSphere Application Server instead of the embedded application server, you must map the users to specific roles in the WebSphere administration console. For example, you must map users who can save searches to the SAVE\_SEARCH role.

Administrative roles		Application user privileges			Connection credentials	
User ID	Role	User or Group ID	Privileges	Applicati ID	Data source	Connection ID
esadmin	Default administrator	user 0	Save searches	0	Agent for Windows file systems	agent for windows fs
esadmin	Master administrator	user 1	Export documents	1	Content Manager	content manager
cadmin	Operator	user 2	Create deep inspection reports	2	DB2	db2
operator	Monitor	user 3	Add rules to categories	3	Exchange Server	exchangeAdapt
monitor	Collection administrator	user 4	Rebuild the category index	0	FileNet P8	filenetp8
taadmin	Content analytics administrator				Content Integrator	iice
facetadmin	Facet tree administrator				JDBC	jdbc
catadmin	Rule-based category administrator					

## Exploring the Security Dashboard

**IBM** IBM Content Analytics with Enterprise Search

☰ Collections
☰ System
☰ Security

Application Login Security

Collection-Level Security

System-Level Security

**Administrative roles**

User ID	Role	
esadmin	Default administrator	✎ 🗑
esadmin	Master administrator	✎ 🗑
cadmin	Operator	✎ 🗑
operator	Monitor	✎ 🗑
monitor	Collection administrator	✎ 🗑
taadmin	Content analytics administrator	✎ 🗑
facetadmin	Facet tree administrator	✎ 🗑
catadmin	Rule-based category administrator	✎ 🗑

**Application user privileges**

User or Group ID	Privileges	Applicati ID	
user 0	Save searches	0	✎ 🗑
user 1	Export documents	1	✎ 🗑
user 2	Create deep inspection reports	2	✎ 🗑
user 3	Add rules to categories	3	✎ 🗑
user 4	Rebuild the category index	0	✎ 🗑

**Connection credentials**

Data source	Connection ID	
Agent for Windows file systems	agent for windows fs	✎ 🗑
Content Manager	content manager	✎ 🗑
DB2	db2	✎ 🗑
Exchange Server	exchangeAdapt	✎ 🗑
FileNet P8	filenetp8	✎ 🗑
Content Integrator	iice	✎ 🗑
JDBC	jdbc	✎ 🗑

Configure connection credentials to allow crawlers to collect content from data sources.

Search servers can also use the credentials to determine whether an application user's permissions are still valid.

**Hint:** You can create the connection credentials here, or create them when you configure a crawler and specify information that allows the crawler to access a data source.



## Exploring the Security Dashboard

IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security	Actions ▾
Collection-Level Security	Actions ▾
System-Level Security	Actions ▾

If it is not already open, click to expand the **Collection-Level Security** pane.

Configure user validation preferences, associate applications with the collections they can access, and specify security preferences for documents in specific collections.

# Exploring the Security Dashboard

The screenshot displays the IBM Content Analytics Security Dashboard. At the top, the navigation bar includes the IBM logo, the text "IBM Content Analytics with Enterprise Search", and links for "Search Customizer", "Analytics Customizer", "Log Out", "Help", and "About". Below this, a secondary navigation bar contains "Collections", "System", and "Security" (the active tab).

The main content area is titled "Application Login Security" and is divided into three sections:

- Collection-Level Security**: This section is further divided into:
  - Identity management settings**: Shows a lock icon and "Enabled", a "Refresh interval: 6 days", and a list of "All crawler types that support SSO": Content Integrator, Domino Document Manager, Notes, Quickr for Domino, and IBM Connections.
  - Application associations**: A list of application boxes including "app1", "All collections", "app2", "app3", and "app4".
  - Security**: A list of settings: "Pre-filtering enabled", "Post-filtering disabled", and "Edit document-level security".
- System-Level Security**: Located at the bottom of the main content area.

On the right side of the "Collection-Level Security" section, there are two "Actions" dropdown menus. A yellow callout bubble points to the top "Actions" menu with the text: "Click **Actions** to configure identity management settings for secure search or to associate applications with the collections that they can access." The bottom "Actions" menu is open, showing options: "Configure identity management", "Associate applications with collections", "Pre-filtering enabled", "Post-filtering disabled", and "Edit document-level security".

## Exploring the Security Dashboard

**IBM** IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System **Security**

**Identity management settings**

Enabled  
Refresh interval: 6 days

**All crawler types that support SSO**  
Content Integrator  
Domino Document Manager  
Notes  
Quickr for Domino  
IBM Connections

Configure identity management settings if your collections include crawlers that support the ability to validate current credentials when users query collections.

For example, you can refresh the stored credential data every time the user logs in or according to a specified interval.

**Application-Level Security**

app1  
All collections  
app2  
app3  
app4

**Secure search settings**

Kiso collection

Pre-filtering enabled  
 Post-filtering disabled  
 Edit document-level security

System-Level Security

## Exploring the Security Dashboard

IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

To control which collections your users query, you can allow your applications to access all collections, all enterprise search collections, all content analytics collections, or specific collections.

Application Login Security Actions ▾

Collection-Level Security Actions ▾

**Identity management settings**

- Enabled
- Refresh interval: 6 days
- All crawler types that support SSO**
- Content Integrator
- Domino Document Manager
- Notes
- Quickr for Domino
- IBM Connections

**Application associations**

Application	Associations
app1	All collections
app2	
app3	
app4	

**Secure search settings**

Kiso collection

- Pre-filtering enabled
- Post-filtering disabled
- Edit document-level security

System-Level Security Actions ▾

## Exploring the Security Dashboard

The screenshot displays the IBM Content Analytics Security Dashboard. At the top, the navigation bar includes the IBM logo, the text "IBM Content Analytics with Enterprise Search", and links for "Search Customizer", "Analytics Customizer", "Log Out", "Help", and "About". Below the navigation bar, there are tabs for "Collections" and "System".

The main content area is divided into several sections:

- Application Login Security**
- Collection-Level Security**
  - Identity management set**
    - Enabled
    - Refresh interval: 6 days
    - All crawler types that support SSO**
      - Content Integrator
      - Domino Document Manager
      - Notes
      - Quickr for Domino
      - IBM Connections
  - Secure search settings**
    - Kiso collection
      - Pre-filtering enabled
      - Post-filtering disabled
      - Edit document-level security** (highlighted with a red oval)
- System-Level Security**

A yellow callout box is overlaid on the dashboard, providing the following information:

If security is enabled for the collection, you can see how user validation is enforced:

- When **pre-filtering** is enabled, the user's credentials are compared to ACL data that is stored with documents in the index.
- When **post-filtering** is enabled, the system verifies the user's credentials with the data source server before returning results.

To change these settings for a collection, click **Edit document-level security**.

At the bottom of the dashboard, there is a list of applications: app2, app3, and app4.

## Exploring the Security Dashboard

The screenshot displays the IBM Content Analytics with Enterprise Search interface. At the top, the IBM logo is followed by the text "IBM Content Analytics with Enterprise Search". To the right of this header are links for "Search Customizer", "Analytics Customizer", "Log Out", "Help", and "About". Below the header is a navigation bar with three tabs: "Collections", "System", and "Security". The "Security" tab is currently selected. The main content area shows three security configuration panes: "Application Login Security", "Collection-Level Security", and "System-Level Security". Each pane has an "Actions" dropdown menu to its right. A yellow callout box with a speech bubble pointing to the "Application Login Security" pane contains the following text: "If it is not already open, and you use the embedded web application server instead of WebSphere Application Server, click to expand the **Application Login Security** pane. **Attention:** If you use WebSphere, user authentication must be configured and enforced through WebSphere Application Server global security settings."

## Exploring the Security Dashboard

The screenshot displays the IBM Content Analytics with Enterprise Search Security Dashboard. The top navigation bar includes the IBM logo, the product name, and links for Search Customizer, Analytics Customizer, Log Out, Help, and About. Below this, a breadcrumb trail shows Collections, System, and Security. The main content area is divided into sections for Application Login Security, Collection-Level Security, and System-Level Security. The Application Login Security section is expanded to show 'Application login settings' and 'LTPA token and key file settings'. The 'Application login settings' section is 'Enabled' and includes 'Authentication preferences' (The default administrator can access all applications) and 'LDAP server configuration' (LDAP server host name: ldap.ibm.com, LDAP server port number: 389, Base DN: CN=ldap user, Use credentials to access to the LDAP server: Yes, LDAP user name: bind dn). The 'LTPA token and key file settings' section is also 'Enabled' and includes 'LTPA token for single sign-on login' (Token timeout value: 150, Cookie domain name: ltpa.ibm.com, LTPA interoperability mode: Yes, LTPA key file path: /home/esadmin/ltpa.key, Additional domain: (empty), Additional user name suffix: (empty)). Callout boxes provide instructions on using the 'Actions' menu and explain the LTPA settings. The 'Actions' menu is visible in the top right of the settings panels.

IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security

**Application login settings**

Enabled

Authentication preferences  
The default administrator can access all applications

LDAP server configuration

LDAP server host name	ldap.ibm.com
LDAP server port number	389
Base DN	CN=ldap user
Use credentials to access to the LDAP server	Yes
LDAP user name	bind dn

Collection-Level Security

System-Level Security

LTPA token and key file settings

Enabled

LTPA token for single sign-on login

Token timeout value	150
Cookie domain name	ltpa.ibm.com
LTPA interoperability mode	Yes
LTPA key file path	/home/esadmin/ltpa.key
Additional domain	
Additional user name suffix	

Click **Actions** to enable, disable, add, or change authentication settings.

Configure application login settings

Configure ap

If you previously configured a connection to your Lightweight Directory Access Protocol (LDAP) server, or configured a Lightweight Third-Party Authentication (LTPA) token file to support single sign-on authentication, the **Security** dashboard shows your configured settings.

**IBM Content Analytics with Enterprise Search** Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System **Security**

Security : System Security > **Configure application login settings**

### Configure Application Login Settings

[Learn more](#)

You can control access to administration, enterprise search, and content mining applications by authenticating users who log in. If you installed an LDAP server, wizards can discover possible DN attributes and help you validate user and group entries. If the collection includes crawlers...

For your changes to become effective...

- Require users to log in

Configure login settings

Authentication preferences  
You can enable the default IRM settings. To authenticate users through your LDAP server, you must first configure the LDAP server connection.

- The default administrator can access all applications
- Use the LDAP server to authenticate users

Configure the LDAP server connection

LDAP server host name:

LDAP server port number:

Credentials:

- Do not use credentials to access the LDAP server
- Use credentials to access to the LDAP server

LDAP user name:

LDAP password:

Validate the LDAP server connection configuration

Server connection test results:

Before you begin, collect information about your LDAP server, such as:

- The server host name and port
- A user name and password for accessing the LDAP user registry
- The base distinguished name (DN) and attributes for finding user names and group names in the registry, and
- The names of object classes for user and group entries in the registry



**IBM Content Analytics with Enterprise Search** Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System **Security**

Security : System Security > Configure application login settings

### Configure Application Login Settings

[Learn more](#)

You can control access to administration, enterprise search, and content mining applications by authenticating users who log in. If you installed an LDAP server, wizards can discover possible DN attributes and help you validate user and group entries. If the collection includes crawlers that support SSO authentication, configure the LTPA token and key file.

If you do not want to allow the default Content Analytics with Enterprise Search administrator to access the content analytics miner and all enterprise search applications, clear this check box.

Allow the default Content Analytics with Enterprise Search administrator to access applications regardless of other authentication

If you want to authenticate users through your LDAP server, enable the system to use LDAP.

The default administrator can access all applications

Use the LDAP server to authenticate users

Configure the LDAP server connection

LDAP server host name:

LDAP server port number:

Credentials:

Do not use credentials to access the LDAP server

Use credentials to access to the LDAP server

LDAP user name:

LDAP password:

Validate the LDAP server connection configuration

[Test LDAP Server Connection](#)

Server connection test results:

## Exploring the Security Dashboard

Administration Console for IBM Content Analytics with Enterprise Search - Windows Internet Explorer

http://masala1.yamato.ibm.com:8390/ESAdmin/security.do?command=displaySearchAppsLo

For your changes to become effective, restart the IBM Content Analytics with Enterprise Search system.

Require users to log in

Configure login settings

Authentication preferences

You can enable the default IBM Content Analytics authentication settings.

To authenticate users through your LDAP server, you must:

- Require users to log in
- Indicate that you want to use the LDAP server
- Specify the LDAP server host name and port, and specify credentials that allow the system to access the server.

The default administrator can access all applications

Use the LDAP server to authenticate users

Configure the LDAP server connection

LDAP server host name:  
ldap.ibm.com

LDAP server port number:  
389

Credentials:

Do not use credentials to access the LDAP server

Use credentials to access to the LDAP server

LDAP user name:  
uid=wasadmin,o=omnifind

LDAP password:  
●●●●●●●●

Validate the LDAP server connection configuration

[Test LDAP Server Connection](#)

Server connection test results:

Done

Internet | Protected Mode: Off

## Exploring the Security Dashboard

Administration Console for IBM Content Analytics with Enterprise Search - Windows Internet Explorer

http://masala1.yamato.ibm.com:8390/ESAdmin/security.do?command=displaySearchAppsLo

For your changes to become effective, restart the IBM Content Analytics with Enterprise Search system.

Require users to log in

Configure login settings

Authentication preferences

You can enable the default IBM Content Analytics with Enterprise Search administrator to access applications regardless of other authentication settings.  
To authenticate users through your LDAP server, enable the system to use LDAP.

The default administrator can access all applications  
 Use the LDAP server to authenticate users

Configure the LDAP server connection

LDAP server host name:  
ldap.ibm.com

LDAP server port number:  
389

Credentials:

Do not use credentials to access the LDAP server  
 Use credentials to access to the LDAP server

LDAP user name:  
uid=wasadmin,o=omnifind

LDAP password:  
●●●●●●●●

Click to test the system's ability to connect to the LDAP server.

Validate the LDAP server connection configuration

[Test LDAP Server Connection](#)

Server connection test results:

Done

Internet | Protected Mode: Off

100%

## Exploring the Security Dashboard

Administration Console for IBM Content Analytics with Enterprise Search - Windows Internet Explorer

http://masala1.yamato.ibm.com:8390/ESAdmin/security.do?command=displaySearchAppsLo

For your changes to become effective, restart the IBM Content Analytics with Enterprise Search system.

Require users to log in

Configure login settings

Authentication preferences

You can enable the default IBM Content Analytics with Enterprise Search authentication settings. To authenticate users through your LDAP server, enable the following options:

The default administrator can access all applications regardless of other authentication settings.

Use the LDAP server to authenticate users

Configure the LDAP server connection

LDAP server host name:  
ldap.ibm.com

LDAP server port number:  
389

Credentials:

Do not use credentials to access the LDAP server

Use credentials to access to the LDAP server

LDAP user name:  
uid=wasadmin,o=omnifind

LDAP password:  
●●●●●●●●

If the connection is successful, you can continue with the configuration steps. Otherwise, verify that the server information and credentials are correct, and test the connection again.

Validate the LDAP server connection configuration

[Test LDAP Server Connection](#)

Server connection test results:  
✔ Successful

Done

Internet | Protected Mode: Off

100%

## Exploring the Security Dashboard

**Discover Entries**

**User entries**

Base DN:

User ID attribute:

Object class for user entries:

**Group entries**

Base DN for group entries:

Group ID attribute:

Member attribute in group entries:

Object class for group entries:

Validate the LDAP configuration for user entries.  
User entry test results:

Validate the LDAP configuration for group entries.  
Group entry test results:

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

LTPA key  
LTPA key file name:

If you are knowledgeable about your LDAP configuration data, specify the LDAP properties for user and group entries, and then test that you can log in to the LDAP server.

## Exploring the Security Dashboard

**Discover Entries**

User entries

Base DN:

User ID attribute:

Object class for user entries:

---

Group entries

Base DN for group entries:

Group ID attribute:

Member attribute in group entries:

Object class for group entries:

Validate the LDAP configuration for user entries.

**Test User Entries**

User entry test results:

Click **Test User Entries**.

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

## Exploring the Security Dashboard

The screenshot shows the LDAP configuration interface. On the left, there are sections for 'User entries' and 'Group entries'. The 'User entries' section has fields for 'Base DN' (uid=wasadmin,o=omnifind), 'User ID attribute' (uid), and 'Object class for user entries' (person). The 'Group entries' section has fields for 'Base DN for group entries' (o=omnifind), 'Group ID attribute' (cn), 'Member attribute in group entries' (member), and 'Object class for group entries' (groupOfNames). A 'Discover Entries' button is at the top left. On the right, there is a 'Test User Entries' button and a 'Validate the LDAP configuration for user entries.' instruction. A yellow callout bubble points to the 'Test Login' button in the dialog box, containing the text: 'Enter a valid ID and password for a user in the LDAP registry and click **Test Login**.' The dialog box, titled 'Validate User Entry Attributes', contains the following text: 'To validate settings, enter an example user ID and password. If the login test succeeds, the LDAP configuration is likely valid.' It has input fields for 'Test user ID' (wasadmin) and 'Password for the test user ID' (masked with dots), a 'Test Login' button, and a 'Login test results:' label. A 'Close' button is at the bottom right of the dialog. Below the dialog, there is a checkbox for 'Use LTPA tokens for application single sign on' and a section for 'Configure LTPA token parameters' with fields for 'Token timeout value' (minutes), 'Cookie domain name', and 'LTPA interoperability mode'. At the bottom, there is a section for 'LTPA key' with a field for 'LTPA key file name'.

## Exploring the Security Dashboard

**Discover Entries**

User entries

Base DN:  
uid=wasadmin,o=omnifind

User ID attribute:  
uid

Object class for user entries:  
person

Group entries

Base DN for group entries:  
o=omnifind

Group ID attribute:  
cn

Member attribute in group entries:  
member

Object class for group entries:  
groupOfNames

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

Validate the LDAP configuration for user entries.

**Test User Entries**

User entry test results:  
✔ Successful

If the login is not successful, verify the LDAP user entry properties and verify that the user ID and password are valid, and test again.

**Validate User Entry Attributes**

To validate settings, enter an example user ID and password. If the login test succeeds, the LDAP configuration is likely valid.

Test user ID:  
wasadmin

Password for the test user ID:  
●●●●●●

**Test Login**

Login test results:  
✔ Successful

**Close**



## Exploring the Security Dashboard

**Discover Entries**

User entries

Base DN:

User ID attribute:

Object class for user entries:

---

Group entries

Base DN for group entries:

Group ID attribute:

Member attribute in group entries:

Object class for group entries:

Validate the LDAP configuration for user entries.

**Test User Entries**

User entry test results:  
✔ Successful

Validate the LDAP configuration for group entries.

**Test Group Entries**

Group entry test results:

Click **Test Group Entries**.

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

## Exploring the Security Dashboard

**Discover Entries**

User entries

Base DN:  
uid=wasadmin,o=omnifind

User ID attribute:  
uid

Object class for user entries:  
person

Group entries

Base DN for group entries:  
o=omnifind

Group ID attribute:  
cn

Member attribute in group entries:  
member

Object class for group entries:  
groupOfNames

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

Validate the LDAP configuration for user entries.

**Test User Entries**

User entry test results:  
✔ Successful

Enter a valid DN for a user in the LDAP registry and test to see whether information about groups that the user belongs to can be retrieved.

**Validate Group Entry Attributes**

To validate settings, enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics) and test to see whether group information can be retrieved.:

uid=wpsadmins,o=omnifind

**Retrieve Group Information**

Group information test results (if no results are shown, the group attributes are incorrect):

**Close**

## Exploring the Security Dashboard

**Discover Entries**

User entries

Base DN:  
uid=wasadmin,o=omnifind

User ID attribute:  
uid

Object class for user entries:  
person

Group entries

Base DN for group entries:  
o=omnifind

Group ID attribute:  
cn

Member attribute in group entries:  
member

Object class for group entries:  
groupOfNames

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

Validate the LDAP configuration for user entries.

**Test User Entries**

User entry test results:  
✔ Successful

In some cases, the test results might show that the user is valid, but the user does not belong to any groups.

**Validate Group Entry Attributes**

To validate settings, enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics) and test to see whether group information can be retrieved.:

uid=wpsadmins,o=omnifind

**Retrieve Group Information**

Group information test results (if no results are shown, the group attributes are incorrect):

✔ The following groups were found. Verify that the list includes groups that the user belongs to.

*No entries are found.*

Close

## Exploring the Security Dashboard

**Discover Entries**

User entries

Base DN:

User ID attribute:

Object class for user entries:

Group entries

Base DN for group entries:

Group ID attribute:

Member attribute in group entries:

Object class for group entries:

**Test User Entries**

Validate the LDAP configuration for user entries.

User entry test results:  
✔ Successful

**Test Group Entries**

Validate the LDAP configuration for group entries.

Group entry test results:  
✔ The following groups were found. Verify that the list includes groups that the user belongs to.  
*No entries are found.*

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

If you are not knowledgeable about your LDAP configuration data, you can use a wizard to discover possible attributes and then test to see if they are valid.

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base

uid=w

User I

uid

Objec

perso

Group entri

Base

o=om

Group

cn

Memb

memb

Objec

group

Use LTPA to

Configure L

Token time

Cookie don

LTPA inte

LTPA key

LTPA key file name:

**Discover User and Group Attributes** x

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

**Possible user entries**  
After you select an entry, you can select possible DN attributes a

---

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

**Possible group entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Enter a user DN, and then click **Discover User Entries** to see potentially valid attributes.

## Exploring the Security Dashboard

The screenshot displays the Security Dashboard interface. At the top, there are buttons for 'Discover Entries' and 'Test User Entries'. The 'Discover User and Group Attributes' dialog box is open, showing instructions for discovering user and group entries. The dialog has a title bar with a close button (x). The 'User entries' section contains a text input field with the value 'uid=wasadmin,o=omnifind' and a 'Discover User Entries' button. Below this, it lists 'Possible user entries' with a dropdown menu. The 'Group entries' section contains a text input field and a 'Discover Group Entries' button. Below this, it lists 'Possible group entries' with a dropdown menu. The background shows a sidebar with various configuration options like 'Use LTPA token', 'Configure LTPA token time', 'Cookie domain', 'LTPA integration', and 'LTPA key file name'.

Discover Entries

Validate the LDAP configuration for user entries.

Test User Entries

Discover User and Group Attributes

User entries

Base

uid=w

User I

uid

Objec

perso

Group entri

Base

o=om

Group

cn

Memb

memb

Objec

group

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

uid=wasadmin,o=omnifind

Discover User Entries

**Possible user entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

Discover Group Entries

**Possible group entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Use LTPA token

Configure LTPA token time

Token time

Cookie domain

LTPA integration

LTPA key file name:

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base

uid=w

User I

uid

Objec

perso

Group entri

Base

o=om

Group

cn

Memb

memb

Objec

group

Use LTPA to

Configure L

Token time

Cookie don

LTPA inte

LTPA key

LTPA key file name:

**Discover User and Group Attributes** x

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

uid=wasadmin,o=omnifind Discover User Entries

✔ 1 entry or entries found.

**Possible user entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

---

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

Discover Group Entries

**Possible group entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base

uid=w

User

uid

Object

person

Group entries

Base

o=om

Group

cn

Membr

memb

Object

group

### Discover User and Group Attributes

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

✔ 1 entry or entries found.

**Possible user entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

If more than one potential DN entry is available, select the one that you want to use to test the LDAP server.

---

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

**Possible group entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Use LTPA to

Configure L

Token time

Cookie don

LTPA inte

LTPA key

LTPA key file name:



## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base

uid=w

User

uid

Object

person

Group entries

Base

o=om

Group

cn

Membr

memb

Object

group

Use LTPA to

Configure L

Token time

Cookie don

LTPA inte

LTPA key

LTPA key file name:

**Discover User and Group Attributes** x

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

✔ 1 entry or entries found.

**Possible user entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

---

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

**Possible group entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

## Exploring the Security Dashboard

Discover Entries

Validate the LDAP configuration for user entries.

Test User Entries

Discover User and Group Attributes

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

uid=wasadmin,o=omnifind Discover User Entries

✓ 1 entry or entries found.

**Possible user entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:  
uid=wasadmin,o=omnifind

Continue to select attributes from the lists of potential user entry attributes.

Base DN:  
User ID attribute:  
Object class for user entries:

Validate the LDAP configuration for user entries.  
Test User Entries  
User entry test results:

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

Discover Group Entries

**Possible group entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Use LTPA token  
Configure LTPA token  
Token time  
Cookie domain  
LTPA integrity  
LTPA key  
LTPA key file name:

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base DN: uid=wasadmin,o=omnifind Discover User Entries

uid=wasadmin,o=omnifind

Object class for user entries: Test User Entries

Group entries

Base DN: Test User Entries

o=omnifind

cn=administrators,o=analytics

Member DN: Test User Entries

membership: Test User Entries

Object class for group entries: Test User Entries

group entries

Use LTPA tokens Test User Entries

Configure LTPA tokens Test User Entries

Token time Test User Entries

Cookie domain Test User Entries

LTPA interop Test User Entries

LTPA key Test User Entries

LTPA key file name: Test User Entries

### Discover User and Group Attributes

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

uid=wasadmin,o=omnifind Discover User Entries

✔ 1 entry or entries found.

**Possible user entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

uid=wasadmin,o=omnifind

Base DN: Test User Entries

o=omnifind

uid=wasadmin,o=omnifind

Object class for user entries: Test User Entries

Validate the LDAP configuration for user entries.  
Test User Entries

User entry test results:

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

Discover Group Entries

**Possible group entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Test User Entries

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base DN: uid=wasadmin,o=omnifind Discover User Entries

uid=wasadmin,o=omnifind

✓ 1 entry or entries found.

**Possible user entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:  
uid=wasadmin,o=omnifind

Group entries

Base DN: o=omnifind Validate the LDAP configuration for user entries.  
Test User Entries

o=omnifind

Group ID attribute:

User ID attribute:

Object class for user entries:

User entry test results:

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

Discover Group Entries

**Possible group entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Use LTPA token

Configure LTPA token time:

Token time:

Cookie domain:

LTPA integrity

LTPA key file name:

# Exploring the Security Dashboard

The screenshot shows a web interface for LDAP configuration. A modal dialog box titled "Discover User and Group Attributes" is open. It contains the following elements:

- Discover Entries** button (top left)
- Text: "Validate the LDAP configuration for user entries." (top right)
- Test User Entries** button (top right)
- Text: "Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:"
- Text input: "uid=wasadmin,o=omnifind" (with a dropdown arrow)
- Discover User Entries** button
- Text: "1 entry or entries found." (with a green checkmark icon)
- Possible user entries** section:
  - Text: "After you select an entry, you can select possible DN attributes and then test the LDAP configuration:"
  - Text input: "uid=wasadmin,o=omnifind" (with a dropdown arrow)
  - Base DN:** "o=omnifind" (with a dropdown arrow)
  - User ID attribute:** "uid" (text input)
  - Object class for user entries:** (empty dropdown menu with a hand cursor pointing to it)
  - Validate the LDAP configuration for user entries.** (text)
  - Test User Entries** button
  - User entry test results:** (text)
- Possible group entries** section:
  - Text: "Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:"
  - Text input: (empty)
  - Discover Group Entries** button

The background interface shows a sidebar with a tree view containing "User entries" and "Group entries" sections, and a main content area with various configuration options like "Use LTPA token", "Configure LTPA", "Token time", "Cookie domain", "LTPA internal", "LTPA key", and "LTPA key file name".

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base DN: uid=wasadmin,o=omnifind Discover User Entries

uid=wasadmin,o=omnifind

✓ 1 entry or entries found.

**Possible user entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:  
uid=wasadmin,o=omnifind

Group entries

Base DN: o=omnifind Validate the LDAP configuration for user entries.  
Test User Entries

o=omnifind

Group ID attribute: uid User entry test results:

Object class for user entries:

top

person

organizationalPerson

inetOrgPerson

ePerson

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries: Discover Group Entries

Use LTPA token

Configure LTPA token time

Cookie domain

LTPA integrity

LTPA key file name:

## Exploring the Security Dashboard

Discover Entries Validate the LDAP configuration for user entries.  
Test User Entries

User entries

Base DN: uid=wasadmin,o=omnifind Discover User Entries

uid=wasadmin,o=omnifind

✓ 1 entry or entries found.

**Possible user entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

uid=wasadmin,o=omnifind

Base DN: o=omnifind Validate the LDAP configuration for user entries.  
Test User Entries

User ID attribute: uid User entry test results:

Object class for user entries: person

Group entries

Base DN: Discover Group Entries

Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:

Use LTPA tool Discover Group Entries

**Possible group entries**  
After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

Configure LTPA tool

Token time

Cookie domain

LTPA interactive

LTPA key file name:

## Exploring the Security Dashboard

Discover Entries

Validate the LDAP configuration for user entries.

Test User Entries

Discover User and Group Attributes

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible user entries:

uid=wasadmin,o=omnifind Discover User Entries

1 entry or entries found.

**Possible user entries**

After you select an entry, you can select possible DN attributes and then test the LDAP configuration:

uid=wasadmin,o=omnifind

Base DN: o=omnifind

User ID attribute: uid

Object class for user: person

To validate settings, enter an example user ID and password. If the login test succeeds, the LDAP configuration is likely valid.

Test user ID: wasadmin

Password for the test user ID: ●●●●●●

Test Login

Login test results:

Close

Enter a fully qualified Distinguished Name for an example user (such as uid=admin,o=analytics), and then click to discover possible group entries.

Discover Group Entries

Use LTPA token

Configure LTPA token

Token time

Cookie domain

LTPA integrity

LTPA key

LTPA key file name:



## Exploring the Security Dashboard

The screenshot displays the Security Dashboard interface with two overlapping dialog boxes. The background window shows the 'Discover Entries' section with a 'Discover User and Group Attributes' dialog box open. This dialog box contains a text input field with the value 'uid=wasadmin,o=omnifind' and a 'Discover User Entries' button. Below the input field, it indicates '1 entry or entries found' and lists 'Possible user entries' with the same DN. A 'Validate User Entry Attributes' dialog box is also open, showing fields for 'Base DN' (o=omnifind), 'User ID attribute' (uid), and 'Object class for user' (person). It includes a 'Test Login' button and displays 'Login test results: Successful'. A yellow callout bubble points to the 'Test Login' button with the text: 'If the login is not successful, select different potential LDAP properties and test your ability to log in to the LDAP server again.' The background window also shows a 'Test User Entries' button and various configuration options like 'Use LTPA token', 'Configure LTPA token time', 'Cookie domain', 'LTPA interval', and 'LTPA key file name'.

## Exploring the Security Dashboard

The screenshot displays the Security Dashboard interface with a modal window titled "Discover User and Group Attributes" open. The modal is divided into two sections: "Discover User and Group Attributes" and "Discover Group Attributes".

**Discover User and Group Attributes Section:**

- Buttons: "Discover Entries", "Test User Entries", "Validate the LDAP configuration for user entries."
- Fields: "Base DN:" (o=omnifind), "User ID attribute:" (uid), "Object class for user entries:" (person).
- Results: "User entry test results: Successful" (indicated by a green checkmark).

**Discover Group Attributes Section:**

- Text: "Enter a fully qualified Distinguished Name for an example group (such as cn=administrators,o=analytics), and then click to discover possible group entries.:"
- Field: "Base DN:" (cn=wpsadmins,o=omnifind)
- Button: "Discover Group Entries" (circled in red)
- Results: "1 entries found. Possible group entries. After you select an entry, you can select possible DN attributes." (Listed: cn=wpsadmins,o=omnifind)
- Fields: "Base DN for group entries:" (o=omnifind), "Group ID attribute:" (cn), "Member attribute in group entries:" (member), "Object class for group entries:" (groupOfNames)
- Button: "Retrieve Group Information" (circled in red)
- Text: "Validate the LDAP configuration for group entries." and "Group entry test results:"
- Buttons: "OK", "Cancel"

**Callouts:**

- A yellow callout box states: "Repeat equivalent steps to test your ability to retrieve information about groups that a user belongs to."

**Background Dashboard Elements:**

- Left sidebar: "User entries", "Group entries", "Use LTPA tool", "Configure LTPA", "Token time", "Cookie domain", "LTPA inter...", "LTPA key", "LTPA key file name:"
- Right sidebar: "des", "E"

## Exploring the Security Dashboard

Group entries

Base DN for group entries:

Group ID attribute:

Member attribute in group entries:

Object class for group entries:

Validate the LDAP configuration for group entries.

Group entry test results:

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

LTPA key password:

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

Additional domain:

Additional user name suffix:

To specify information that enables users to search secure sources that support single sign-on (SSO) authentication, scroll down and select the **Use LTPA tokens for application single sign-on** check box.

## Exploring the Security Dashboard

**Group Entries**

Base DN for group entries:

Group ID attribute:

Member attribute in group entries:

Object class for group entries:

Validate the LDAP configuration for group entries.

Group entry test results:

---

Use LTPA tokens for application single sign-on

**Configure LTPA token parameters**

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

**LTPA key**


LTPA key file name:

LTPA key password:

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

Additional domain:

Additional user name suffix:

 The LTPA token enables a user to skip the application log-in screen if the user is already authenticated by another system that is configured to use the same LTPA token.

## Exploring the Security Dashboard

o=omnifind

Group ID attribute:  
cn

Member attribute in group entries:  
member

Object class for group entries:  
groupOfNames

validate the LDAP configuration for group entries.  
**Test Group Entries**  
Group entry test results:

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
150 minutes

Cookie domain name:  
ltpa.ibm.com

LTPA interoperability mode

LTPA key

LTPA key file name:  
/home/esadmin/ltpa.key **Generate Key**

LTPA key password:  
●●●●●●●● **Validate Password**

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

**Import Key** **Export Key**

Additional domain:  
\_\_\_\_\_

Additional user name suffix:  
\_\_\_\_\_

**OK** **Cancel**

You must specify a time limit for SSO sessions. For example, specify that the LTPA token expires after 150 minutes.

You must also specify a domain where the LTPA cookie can be accessed by all servers that share the SSO session, such as ltpa.example.com.

## Exploring the Security Dashboard

<input type="text" value="o=omnifind"/> Group ID attribute: <input type="text" value="cn"/> Member attribute in group entries: <input type="text" value="member"/> Object class for group entries: <input type="text" value="groupOfNames"/>	validate the LDAP configuration for group entries. <input type="button" value="Test Group Entries"/> Group entry test results:
--	--

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

If you share the LTPA key file with an application that does not support attribute propagation, such as older versions of WebSphere Application Server, select the check box to enable interoperability.

LTPA key

LTPA key file name:

LTPA key password:

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

Additional domain:

Additional user name suffix:

## Exploring the Security Dashboard

<input type="text" value="o=omnifind"/> Group ID attribute: <input type="text" value="cn"/> Member attribute in group entries: <input type="text" value="member"/> Object class for group entries: <input type="text" value="groupOfNames"/>	validate the LDAP configuration for group entries. <input type="button" value="Test Group Entries"/> Group entry test results:
--	--

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
 minutes

Cookie domain name:

LTPA interoperability mode

LTPA key

LTPA key file name:

LTPA key password:

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

Additional domain:

Additional user name suffix:

There are several ways to configure the system to use an LTPA key file. For example, you can specify the key file path and password, and click a button to validate that they are correct.

## Exploring the Security Dashboard

<p>o=omnifind</p> <p>Group ID attribute: cn</p> <p>Member attribute in group entries: member</p> <p>Object class for group entries: groupOfNames</p>	<p>validate the LDAP configuration for group entries.</p> <p><input type="button" value="Test Group Entries"/></p> <p>Group entry test results:</p>
--	---

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
150 minutes

Cookie domain name:  
ltpa.ibm.com

LTPA interoperability mode

LTPA key

LTPA key file name:  
/home/esadmin/ltpa.key

LTPA key password:  
●●●●●●●●

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

Additional domain:  
\_\_\_\_\_

Additional user name suffix:  
\_\_\_\_\_

If a key file does not exist, you can generate one.



## Exploring the Security Dashboard

<p>o=omnifind</p> <p>Group ID attribute: cn</p> <p>Member attribute in group entries: member</p> <p>Object class for group entries: groupOfNames</p>	<p>validate the LDAP configuration for group entries.</p> <p><b>Test Group Entries</b></p> <p>Group entry test results:</p>
--	---

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
150 minutes

Cookie domain name:  
ltpa.ibm.com

LTPA interoperability mode

LTPA key

LTPA key file name:  
/home/esadmin/ltpa.key **Generate Key**

LTPA key  
●●●●● **Password**

The same key is used for all applications. You can generate a new key, import an existing key file, and export the key to another server.

**Import Key** **Export Key**

Additional domain:

Additional user name suffix:

**OK** **Cancel**

You can also import a key file. For example, you can import the key file from WebSphere Application Server.

## Exploring the Security Dashboard

o=omnifind

Group ID attribute:  
cn

Member attribute in group entries:  
member

Object class for group entries:  
groupOfNames

validate the LDAP configuration for group entries.  
**Test Group Entries**

Group entry test results:

**Hint:** The same key file must exist on all servers that share the SSO session.

If your collections include sources that require WebSphere Application Server, such as sources are hosted on WebSphere Portal servers, you can share the LTPA key file in the proper format.

For example, you can import the key file from WebSphere Application Server to use for secure enterprise search, or export the key file and then import it into WebSphere Application Server.

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
150 minutes

Cookie domain name:  
ltpa.ibm.com

LTPA interoperability mode

LTPA key

LTPA key file name:  
/home/esadmin/ltpa.key **Generate Key**

LTPA key password:  
●●●●●●●● **Validate Password**

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

**Import Key** **Export Key**

Additional domain:  
\_\_\_\_\_

Additional user name suffix:  
\_\_\_\_\_

**OK** **Cancel**

## Exploring the Security Dashboard

<p>o=omnifind</p> <p>Group ID attribute: cn</p> <p>Member attribute in group entries: member</p> <p>Object class for group entries: groupOfNames</p>	<p>validate the LDAP configuration for group entries.</p> <p><input type="button" value="Test Group Entries"/></p> <p>Group entry test results:</p>
--	---

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
150 minutes

Cookie domain name:  
ltpa.ibm.com

LTPA interoperability mode

LTPA key

LTPA key file name:  
/home/esadmin/ltpa.key

LTPA key password:  
●●●●●●●●

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

Additional domain:  
\_\_\_\_\_

Additional user name suffix:  
\_\_\_\_\_

If you share the LTPA key file with a WebSphere Application Server server that uses a federated repository, copy the additional domain name and user name suffix values from the federated repository base entry in WebSphere Application Server.

## Exploring the Security Dashboard

o=omnifind

Group ID attribute:  
cn

Member attribute in group entries:  
member

Object class for group entries:  
groupOfNames

validate the LDAP configuration for group entries.  
**Test Group Entries**

Group entry test results:

After you click **OK** to save your LDAP server and LTPA token file configuration settings, you must restart the IBM Content Analytics with Enterprise Search system to apply the changes.

Use LTPA tokens for application single sign-on

Configure LTPA token parameters

Token timeout value:  
150 minutes

Cookie domain name:  
ltpa.ibm.com

LTPA interoperability mode

LTPA key

LTPA key file name:  
/home/esadmin/ltpa.key **Generate Key**

LTPA key password:  
●●●●●●●● **Validate Password**

The same key file must exist on all servers that share the SSO session. You can generate a new key, import an existing key file, and export the key file to use with WebSphere Application Server, Domino, or another server.

**Import Key** **Export Key**

Additional domain:  
\_\_\_\_\_

Additional user name suffix:  
\_\_\_\_\_

**OK** **Cancel**

## Exploring the Security Dashboard

IBM Content Analytics with Enterprise Search Search Customizer | Analytics Customizer | Log Out | Help | About

Collections System Security

Application Login Security	Actions ▾
Collection-Level Security	Actions ▾
System-Level Security	Actions ▾

This concludes the tour of the Security dashboard in the IBM Content Analytics with Enterprise Search administration console.