Oracle® Communications Indexing and Search Service

Security Guide

Release 1.0.5

E67906-02

August 2017

ORACLE®

Oracle Communications Indexing and Search Service Security Guide, Release 1.0.5

E67906-02

Contents

Preface

This guide provides guidelines and recommendations for setting up Oracle Communications Indexing and Search Service in a secure configuration.

Audience

This document is intended for system administrators or software technicians who work with Indexing and Search Service.

Related Documents

For more information, see the following documents in the Indexing and Search Service documentation set:

- *Indexing and Search Service Installation and Configuration Guide*: Provides instructions for installing and configuring Indexing and Search Service.
- *Indexing and Search Service Release Notes*: Describes the new features, fixes, known issues, troubleshooting tips, and required third-party products and licensing.
- *Indexing and Search Service System Administrator's Guide*: Describes the tasks and concepts for administering Indexing and Search Service.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Indexing and Search Service Security Overview

This chapter provides an overview of Oracle Communications Indexing and Search Service security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

1. **Keep software up to date.** This includes the latest product release and any patches that apply to it.
2. **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
3. **Monitor system activity.** Establish who should access which system components, how often they should be accessed, and who should monitor those components.
4. **Install software securely.** For example, use firewalls, secure protocols (such as SSL), and secure passwords. See "Performing a Secure Indexing and Search Service Installation" for more information.
5. **Learn about and use Indexing and Search Service security features.** See "Implementing Indexing and Search Service Security" for more information.
6. **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.
7. **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See "Critical Patch Updates and Security Alerts" on the Oracle website at:

   `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Understanding the Indexing and Search Service Environment

When planning your Indexing and Search Service implementation, consider the following:

- Which resources must be protected?

  For example:

  – Indexing and Search Service web host (runs Indexing and Search Service search services)

  - Indexing and Search Service index host (runs Indexing and Search Service indexing services)
  - Dependent resources, such as Oracle GlassFish Server, Oracle Directory Server Enterprise Edition, Oracle Communications Messaging Server, and Oracle Communications Convergence

- From whom am I protecting the resources?

  In general, resources must be protected from everyone on the Internet. But should the Indexing and Search Service deployment be protected from employees on the intranet in your enterprise? Should your employees have access to all resources within the GlassFish Server environment? Should the system administrators have access to all resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. On the other hand, perhaps it would be best to allow no system administrators access to the data or resources.

- What happens if protections on strategic resources fail?

  In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use Indexing and Search Service. Understanding the security ramifications of each resource help you protect it properly.

Overview of Indexing and Search Service Security

The files in the Indexing and Search Service attachment store and index are owned by the Indexing and Search Service user whom you specified during configuration. This is analogous to the Messaging Server user owning the files in the message store. Regular users can read only their own files in the store. They cannot access other users' files.

To search mail in the Indexing and Search Service store, users need to authenticate to LDAP to be able to use the RESTful web service. A second means of authentication is for the Messaging Server host itself to authenticate to Indexing and Search Service through the **mail.server.ip** property that you specified during configuration and defined in the **jiss.conf** file. This verification grants access to the Messaging Server host or hosts, through the host IP address, to access the RESTful web service.

When securing your Indexing and Search Service deployment, be sure to change the passwords for the Java Message Queue (JMQ) guest and administrative users. For more information, see the steps for configuring the GlassFish Message Queue broker in the topic on preparing Messaging Server for Indexing and Search Service integration in *Indexing and Search Service Installation and Configuration Guide*.

If necessary, you can also configure JMQ to use SSL, though this configuration has not officially been tested yet.

Recommended Deployment Topologies

You can deploy Indexing and Search Service on a single host or on multiple hosts, splitting up the components into multiple front-end hosts and multiple back-end hosts. For more information, see the topic about planning your installation in *Indexing and Search Service Installation and Configuration Guide*.

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture.

Operating System Security

This section lists Indexing and Search Service-specific operating system security configurations. This section applies to all supported operating systems.

Firewall Port Configuration

Indexing and Search Service communicates with various components on specific ports. Depending on your deployment and use of a firewall, you might need to ensure that the firewalls are configured to manage traffic for the following components:

- Indexing and Search Service back-end port (default 8080)
- Message Queue port (default 7676)
- GlassFish Server administration server port (default 4848)
- Indexing and Search Service access port (default 443)
- Notification mail server port (default 25)

Close all unused ports, especially non-SSL ports. Opt for SSL-enabled ports, instead of non-SSL ports, for all communications (for example: HTTPS, IIOPS, t3s).

For more information about securing your OS, see your OS documentation.

Secure Communications

Secure connections between applications connected over the World Wide Web can be obtained by using protocols such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). SSL is often used to refer to either of these protocols or a combination of the two (SSL/TLS). Due to a security problem with SSLv3, Indexing and Search Service recommends the use of only TLS. However, throughout this guide, secure communications may be referred to by the generic term SSL.

In a Indexing and Search Service deployment, you can enable the use of TLS between the following components:

- Indexing and Search Service and Directory Server
- Indexing and Search Service and Messaging Server
- Indexing and Search Service and Convergence

See "Implementing Indexing and Search Service Security" for more information.

LDAP Security

To enhance client security in communicating with Directory Server, use a strong password policy for user authentication. For more information on securing Directory Server, see the discussion about Directory Server Security in *Oracle Directory Server Enterprise Edition Administration Guide*.

2

Performing a Secure Indexing and Search Service Installation

This chapter presents planning information for your Oracle Communications Indexing and Search Service system and describes recommended deployment topologies that enhance security.

For more information about installing Indexing and Search Service, see *Indexing and Search Service Installation and Configuration Guide*.

Installing Infrastructure Components Securely

Indexing and Search Service is deployed within Oracle GlassFish Server. When installing and configuring GlassFish Server, it is recommended to:

- Use a non-root user account to install and run GlassFish Server

  The non-root user must be the same user specified for the **iss.user** parameter in the **jiss.conf** file. Also, you set the **appserv.issuser.enabled** parameter to **`true`**.
- Configure HTTPS and disable HTTP
- Configure the JMX port for GlassFish Server to use SSL
- Configure GlassFish Server to prevent Denial of Service (DoS) attacks

To configure and administer GlassFish Server security, see *Oracle GlassFish Server Security Guide*.

Credentials Needed to Install Indexing and Search Service Components

The installation prompts for authentication credentials for the following:

- Messaging Server read-only message store administrator (**store.indexeradmin**)
- Message Queue broker handling Messaging Server notifications (user account)
- Indexing and Search Service Message Queue broker (user and administrator accounts)
- Directory Server manager (bind DN and password)

Post-Installation Configuration

After installation, configuring Indexing and Search Service for a secure deployment involves several steps:

1. Enable LDAP over SSL, if not previously done

2. Enable SSL between the Indexing and Search Service indexing node and the Messaging Server IMAP server
3. Disabling SSLv3 on front-end GlassFish Server hosts
4. Creating a secure connection between Convergence and Indexing and Search Service

See "Implementing Indexing and Search Service Security" for more information.

3

Implementing Indexing and Search Service Security

This chapter explains the security features of Oracle Communications Indexing and Search Service and the security-related tasks.

Enabling SSL for User/Group Directory Server

The following procedure describes how to enable Secure Sockets Layer (SSL) from Indexing and Search Service components to the User/Group Directory Server.

> **Note:** Import the certificate for the User/Group Directory Server to the operating system before running the Indexing and Search Service **setup** command. Otherwise, the setup command fails when trying to verify Messaging Server parameters.

To enable SSL for the User/Group Directory Server:

1. On the User/Group Directory Server, use the **dsadm** command to display the certificate.

   ```
   dsadm show-cert -F ascii -o user-group1.cert Directory_Server_instance_path
   ```

2. Copy the **user-group1.cert** file to the Indexing and Search Service host.
3. Use the **certutil** command to import the certificate.

   ```
   certutil -A -n "UserGroup1" -i user-group1.cert -t "CT" -d /var/ldap
   ```

   On Red Hat Linux, you need to manually create the **/var/ldap** directory.
4. When running the **setup** command to configure Indexing and Search Service, set the following option and adjust the port.

   ```
   mail.ldap.enablessl = true
   mail.ldap.port = 636
   mail.ldap = ldap.example.com:636
   ```

5. (Optional) If you are using a list of User/Group Directory Servers for **mail.ldap**, repeat for each server in the list.

Enabling SSL/TLS for IMAP Communications to the Messaging Server

To enable Secure Sockets Layer/Transport Layer Security (SSL/TLS) between the Indexing and Search Service indexing node and the Messaging Server IMAP server, set

the following options when running the **setup** command to configure Indexing and Search Service:

```
mail.imap.port = 993
# Messaging Server IMAP protocol: ssl or tls
mail.imap.protocol = ssl
```

If necessary, you can change these values later by editing the *IndexSearch_home***/etc/jiss.conf** file. If you do edit the **jiss.conf** file, you must restart Indexing and Search Service indexing services by using the *IndexSearch_home***/bin/svc_control.sh** command.

Enabling SSL for isshttpd

To enable SSL for the **isshttpd** web proxy:

1. Edit the *IndexSearch_home***/etc/jiss.conf** file.
2. Set the following **iss.isshttpd.ssl.*** configuration parameters:

   ```
   iss.isshttpd.ssl.port = port
   iss.isshttpd.outgoing.ssl.enabled = true
   iss.isshttpd.incoming.ssl.enabled = true
   iss.isshttpd.incoming.plain.enabled = true
   iss.ssl.keystore = path_and_file_name
   ```

   where:

   port is the SSL port on which **isshttpd** listens to process requests.

   path_and_file_name is the path and file name of the Java KeyStore file.
3. Use the **jks** utility to set the KeyStore password, which is stored in the **iss.ssl.keystorepassword** configuration parameter.

   See "jks Utility" for more information.
4. Refresh the Indexing and Search Service configuration for the change to take place.

   ```
   issadmin.sh --refresh
   ```

Disabling SSLv3 on Front-End GlassFish Server Hosts

Identify the http-listener for the publicly accessible port that has SSL/TLS enabled (**security-enabled=true**) on which requests for Indexing and Search Service are received. Ensure that SSLv3 is disabled for this listener by setting the option ssl3-enabled to false.

To disable SSLv3 on GlassFish Server 3:

1. Identify the HTTP listeners that have SSL/TLS enabled (**security-enabled=true**) and verify whether SSLv3 is enabled on that listener (**ssl3-enabled=true**).

   ```
   asadmin get configs.config.server-config.network-config.protocols.protocol.* |
   grep http-listener.*security-enabled=true
   configs.config.server-config.network-config.protocols.protocol.http-listener-2
   .security-enabled=true

   asadmin get
   configs.config.server-config.network-config.protocols.protocol.http-listener-2
   .ssl.ssl3-enabled
   configs.config.server-config.network-config.protocols.protocol.http-listener-2
   .ssl.ssl3-enabled=true
   ```

```
Command get executed successfully.
```

2. Disable those HTTP listeners.

```
asadmin set
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.ssl.ssl3-enabled=false
configs.config.server-config.network-config.protocols.protocol.http-listener-2
.ssl.ssl3-enabled=false
Command set executed successfully.
```

3. Restart GlassFish Server.

To disable SSLv3 on GlassFish Server 2:

1. Identify the HTTP listeners that have SSL/TLS enabled (**security-enabled=true**) and verify whether SSLv3 is enabled on that listener (**ssl3-enabled=true**).

```
asadmin get --user admin --passwordfile /password.gf
server-config.http-service.http-listener.*.* | grep
'http-listener-.*security-enabled = true'
server-config.http-service.http-listener.http-listener-2.security-enabled =
true

asadmin get --user admin --passwordfile /password.gf
server-config.http-service.http-listener.http-listener-2.ssl.ssl3-enabled
server-config.http-service.http-listener.http-listener-2.ssl.ssl3-enabled =
true
```

2. Disable those HTTP listeners.

```
asadmin set --user admin --passwordfile /password.gf
server-config.http-service.http-listener.http-listener-2.ssl.ssl3-enabled=fals
e
server-config.http-service.http-listener.http-listener-2.ssl.ssl3-enabled =
false
```

3. Restart GlassFish Server.

Creating a Secure Connection Between Convergence and Indexing and Search Service

To configure Convergence to access Indexing and Search Service, see *Convergence System Administrator's Guide*. If you want a secure connection between Convergence and Indexing and Search Service, set the Convergence **ISS.enablessl** parameter to **true**, for example:

```
iwcadmin -u adminuserid -w adminpassword -o ISS.enablessl -v true
```

Correspondingly, you must also set the port number (**ISS.port**) to the SSL port number.

To configure the security protocol used by the IMAP connection to the Messaging Server, configure either the **--protocol ssl** or **--protocol tls** option. See the **issadmin.sh** utility documentation in *Indexing and Search Service System Administrator's Guide* for more information about setting the **--protocol** option.

Accessing Mail in the Message Store

Indexing and Search Service enables users to read their own files in the Messaging Server message store, but not other users' files. To search mail in the Indexing and Search Service store, users need to authenticate to LDAP to be able to use the RESTful web service. For more information, see "Overview of Indexing and Search Service Security."

Storing Passwords in the Java KeyStore

Indexing and Search Service stores passwords in the Java KeyStore. Use the **jks** utility to set, maintain, and retrieve password values. To refresh the keystore after adding or changing a password value, use the **issadmin.sh --refresh** command.

The Java KeyStore utility replaces the **jiss_passwd.conf** text file from previous versions of Indexing and Search Service, providing a more secure way to store and maintain passwords. Security enhancements include password protection along with ownership and permission restrictions at the operating system level.

Java KeyStore Configuration

The Java KeyStore replaces the **jiss_password.conf** with two files:

- **stowg**
- **keystore.jks**

stowg

The *IndexSearch_home***/etc/stowg** (symlink **/etc/jiss/stowg**) file contains the password for the Java KeyStore. Any command run on the keystore must have access to this file. The **iss.user** and **iss.group** should own this file with 0600 permissions. The password in this file is randomly generated during install (setup) or patch time, and is not displayed to the user.

keystore.jks

The *IndexSearch_home***/etc/keystore.jks** (symlink **/etc/jiss/keystore.jks**) file contains the Java KeyStore. The passwords are stored in **KeyStore.SecretKeyEntry** format where the alias is the property name used in the code base, for example, **ldap.password**. (For more information about this format, see the **java.security.KeyStore** Javadoc.) The **iss.user** and **iss.group** should own this file with 0600 permissions.

stowg and keystore.jks Portability

The **stowg** and **keystore.jks** files are platform independent and can be copied to an Indexing and Search Service instance. Complete this operation before running the **setup** script on a fresh installation. If you are copying the files to an Indexing and Search Service instance after setup, ensure that the permissions and ownership are correct.

jks Utility

The *IndexSearch_home***/bin/jks** utility sets and retrieves passwords to and from the Java KeyStore. The utility reads the *IndexSearch_home***/etc/stowg** and *IndexSearch_home***/etc/keystore.jks** files for information.

Syntax

```
jks [-h|--help]
[--set --key key_name --password|--passwordfile file]
[--get --key key_name]
[--delete --key key_name]
[--list ]
```

Options

Table 3–1 shows the **jks** utility options. Arguments can be listed in any order.

Table 3–1 jks Options

Option	Description
--key *key_name*	Identifies the key name on which to perform an operation. Required for **--set**, **--get**,, and **--delete** options.
--set	Sets the following key to the value that you supply. Used with the **--key** option.
--get	Displays the value for the following key. Used with the **--key** option.
--delete	Deletes the value for the following key. Used with the **--key** option.
--list	Lists all key names in the keystore.
--password	Prompts for a password. Used with the **--set** option.
--passwordfile *file*	Reads the password from a file. Used with the **--set** option.
--help	Optional. Prints the help text.

Exit code 0 indicates a success, and exit code 1 indicates a failure.

Example

To set the **ldap.password** password and then refresh the keystore to update the password information immediately:

```
jks --set --key ldap.password --password
Enter Password:
/opt/sun/comms/jiss/bin/issadmin.sh --refresh
```

A

Secure Deployment Checklist

The following security checklist provides guidelines to help you secure Oracle Communications Indexing and Search Service and its components.

Secure Deployment Checklist

- Install only the components you require.
- Lock and expire default user accounts.
- Use a strong LDAP password policy for user authentication.
- Restrict, control, and revisit user privileges:
  - Grant only the necessary privileges to each user.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Enforce the use of access controls by using the Authorization Policies.
- Require clients to authenticate.
- Restrict network access by doing the following:
  - Use firewalls.
  - Never leave an unnecessary hole in a firewall.
  - Password-protect the Oracle listener against remote access.
  - Monitor listener activity.
  - Monitor who accesses your systems.
  - Restrict system access by IP addresses.
  - Encrypt network traffic.
- Apply all security patches and workarounds.
- Encrypt sensitive information.
- Contact Oracle if you discover a vulnerability in any Oracle product.