

Oracle® Communications Convergence
System Administrator's Guide
Release 2

July 2015

ORACLE®

Oracle Communications Convergence System Administrator's Guide, Release 2

Copyright © 2007, 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1. Overview of Convergence	4
2. Overview of the Convergence Command-Line Utility	7
3. Convergence Administrative Tasks	13
4. Configuring Convergence to Use Proxy Authentication	51
5. Configuring Convergence With Sun OpenSSO Enterprise 8.0 for Authentication and SSO ...	53
6. Administering SMIME in Convergence	56
What Is SMIME?	57
Software and Hardware Requirements for Convergence with SMIME	58
Certificate Requirements for Using SMIME in Convergence	60
Configuring and Sending Encrypted Mail - Instructions for Convergence End Users	63
Securing Internet Links With SSL	67
Key Access Libraries for the Client Machines	69
Verifying Private and Public Keys	71
Granting Permission to Use SMIME Features	77
Managing Certificates for SMIME	78
Configuring Messaging Server to Use SMIME in Convergence	83
Messaging Server configutil Options for SMIME	89
Messaging Server smime.conf Parameters	91
7. Configuring Horizontal Scalability for Personal Address Book	100
8. Convergence Address Book JMQ Notification	104
9. Convergence Reference	113
10. Convergence Troubleshooting	160
11. Enabling Services for Convergence	161
12. Enhancing Corporate Directory Search for Convergence by Using VLV Indexing in Directory Server	167
13. Writing a Custom Authentication Module for Convergence	176
14. Convergence Configuration Example - Creating an Authentication Realm in Access Manager .. 190	
15. Writing a Pluggable SSO Module for Convergence	194
16. Administering Convergence Display Name to Map to LDAP displayName	202
17. Setting Up Multiple Corporate Directories in Convergence	204
18. Convergence Performance Tuning	207
ExpiresFilter.java	217
19. Convergence Cluster Deployment Example	221
20. Setting Up and Managing Convergence Security	226

Chapter 1. Overview of Convergence

Overview of Convergence

This information provides an overview of Convergence.

Topics:

- [System Requirements](#)
- [Product Features](#)
- [High Level Architecture](#)
- [Default Paths and File Names](#)

System Requirements

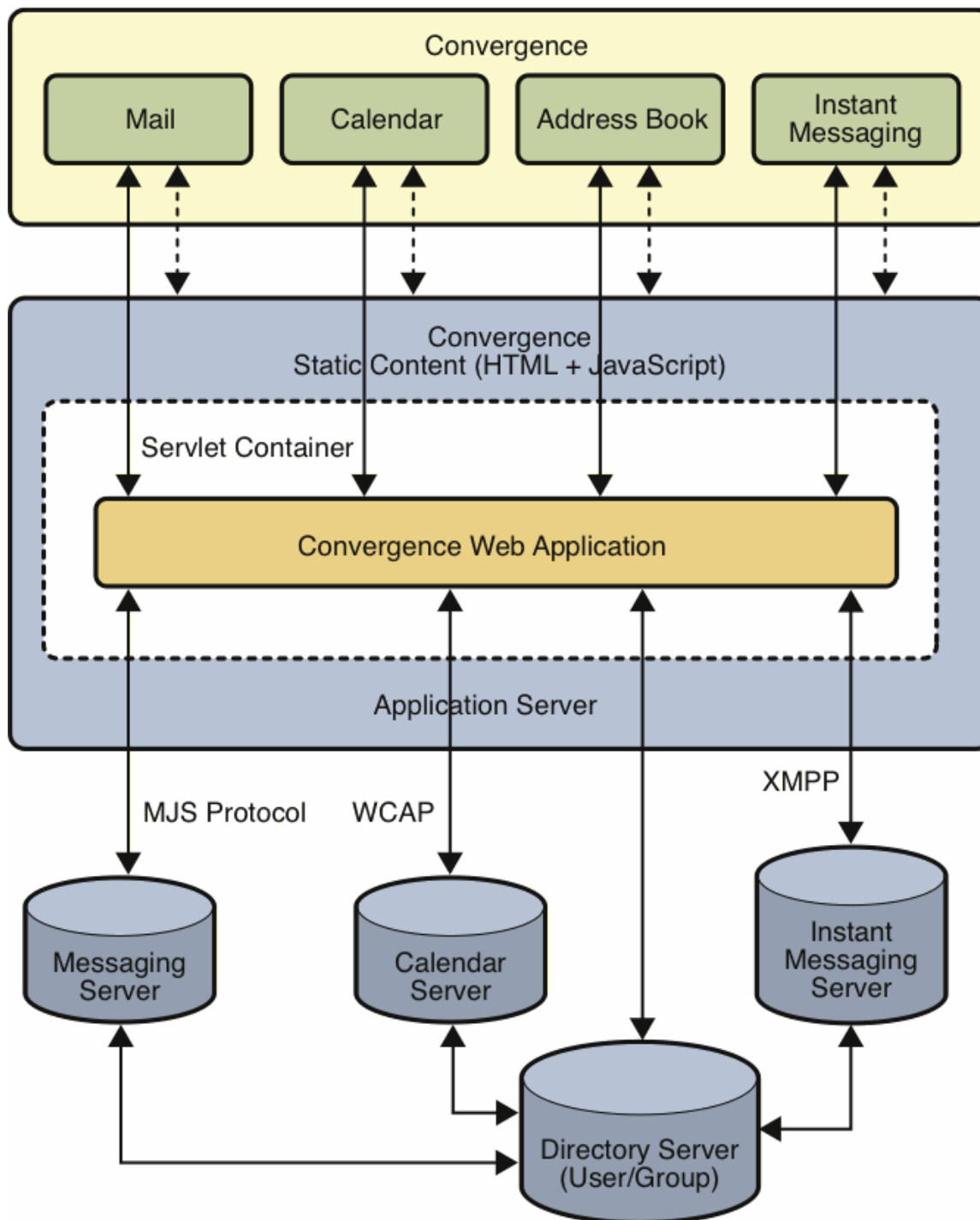
See [Requirements for Communications Suite](#).

Product Features

Convergence is an AJAX based communications web client. Convergence provides a user access to Mail, Calendar, Address Book, and Instant Messaging services. For more information about features of Convergence, see [Introduction to Convergence](#).

High Level Architecture

Convergence is a web-based Java application deployed on a web container. The following figure describes the Convergence architecture.



Convergence has the following major components:

Web Client Component

In the figure, the client component, Convergence, is a browser that uses Dojo to provide the basic infrastructure for the client components. The web client user interface provides features such as virtual list box, drag-and-drop, context menus, type ahead for address look up, and flexible layout and resizing. The client component retrieves data from the server by using protocol commands based on the AJAX technology. The client module also provides API modules for extension and customization the client.

Web Server Static Client Component

Convergence uses static content files such as HTML, CSS, and JavaScript. These static files are deployed on a web container in the static `docroot` directory.

Server Components

The server components of Convergence are deployed as a web application on Application Server. The server components reside in the application and interact with the back-end services such as Directory Server for authentication and user preferences, Messaging Server for mail-related services, Calendar for loading the user's calendar, and Instant Messaging for instant messaging. The Convergence server is a servlets-based implementation. The server provides the services that are used by the client to render data on the browser. The client API communicates with the services to fetch this data.

Convergence provides the following core services:

- Authentication and authorization
- Session management and Single Sign-On (SSO)
- Protocol service
- Configuration management (XML configuration files and Command Line Interface)
- Proxy services for mail, calendar data from back-end communications servers
- Centralized and secure request management
- Logging and basic monitoring of activities
- HTTP binding to XMPP service for instant messaging

Default Paths and File Names

The following table provides platform-specific information about the directories that are created when you install Convergence.

Description	Oracle Solaris	Red Hat Linux
Installation Directory	<code>/opt/sun/comms/iwc</code>	<code>/opt/sun/comms/iwc</code>
Data Directory	<code>/var/opt/sun/comms/iwc/</code>	<code>/var/opt/sun/comms/iwc/</code>
Binary Directory	<code>/opt/sun/comms/iwc/sbin</code>	<code>/opt/sun/comms/iwc/sbin</code>

Chapter 2. Overview of the Convergence Command-Line Utility

Using the Convergence Administration Utility

This chapter provides an overview of how to use the `iwadmin` administration utility to administer a Convergence deployment. This chapter contains the following sections:

- [Convergence Command-Line Utility](#)
- [iwadmin Command-Line Utility Options](#)
- [Finding Information About Configuration Parameters](#)
- [Setting and Unsetting Configuration Parameters](#)
- [Running the iwadmin Utility in Batch Mode](#)

Convergence Command-Line Utility

You can use the `iwadmin` command-line utility to administer Convergence. The following are some of the reasons you would want to run the configuration utility for Convergence:

- During the initial runtime configuration, you created the runtime environment for your deployment using the initial configuration utility. While some of the many possible properties were set from your choices, many of the configuration properties were merely given default values that might not be right for your site. You can use the administration utility to change those values to ones appropriate to your site.
- In time you will need to make various changes to the configuration to accommodate changing business needs, including day-to day-operations. The configuration utility enables you to change the properties to suite your needs.
- The utility validates the values you specify. It confirms that your new values are of the proper data types, and fall within the range of valid values, if appropriate.

iwadmin Command-Line Utility Options

The `iwadmin` command-line utility reads or writes single or multiple configuration file properties. When the utility writes to the configuration file, it performs a validity check on the value that you provide for the property. The validity check validates data types, value limits, and ranges. The `iwadmin` utility exists in the `iwc-home/sbin` directory.



Note

You can use the `iwadmin` command only on the local machine on which Convergence is installed.

The following sections describe the `iwadmin` syntax and options:

- [iwadmin Syntax](#)
- [Command-line Options](#)

iwadmin Syntax

To invoke the `iwcadmin` utility, type the `iwcadmin` command:

- To display usage, type:
`iwcadmin`
or:
`iwcadmin -help`

Example:

iwcadmin command	
USAGE: <code>./iwcadmin [-W <pwdfile>] [-p <port>] [-s] [-o <param-name> [-v <param-value>]] [-l [<group-name>]] [-f <config-params-file>] [-V]</code>	
<code>-W --pwdfile</code>	The file from which to read the administrator password. Recommended for batch processes.
<code>-u --admin</code>	userID of user authorized to make <code>iwcadmin</code> updates. Optional parameter. If <code>-u</code> is not specified, userID (default: <code>admin</code>)
<code>-p --port</code>	is pulled from the <code>iwcadmin.properties</code> file. Administration port of the server.
<code>-s --secure</code>	Use a secure connection (HTTPS).
<code>-o --option</code>	The configuration parameter name to read or write.
<code>-v --value</code>	The value to be set. Must be used with the <code>-o</code> option and must be specified immediately after the <code>-o</code> option.
<code>-l --list</code>	List all the configuration parameters and their values.
<code>-f --file</code>	The file from which to read configuration property/value pairs.
<code>-V --version</code>	Display the version information of the product.
<code>-h --help</code>	Display this message.



Note

Beginning with Convergence 3.0.0.0.0, the `-w <password>` option has been removed. After completing the `iwcadmin` command, you are prompted for the password.

- To read the value of a property, type:

```
iwcadmin [-p|--port <port_number>]
         [-s|--secure] -o|--option <option_name>
```

- To write the value of a property, type:

```
iwcadmin [-p|--port port_number]
         [-s|--secure] -o|--option <option_name> -v <option_value>
```

- To update multiple properties, type:

```
iwcadmin [-p|--port <port_number>] [-s|--secure] -f|--file
         <filename>
```


- To read the value of all configuration properties, type:

```
iwcadmin [-p|--port <port_number>] [-s|--secure] -l|--list
```

- To get information about configuration properties:

```
iwcadmin [-p|--port <port_number>] [-s|--secure] -o|--option  
<config_parameter_name> -h|--help
```

- To get information about configuration properties for a specific module, type the following command. This option is useful when you want to see the values of the configuration parameters for a specific group.

```
iwcadmin [-p|--port <port_number>] [-s|--secure] -l <group_name>
```

Here is an example:

```
./iwcadmin -l mail  
mail.cookieName = webmailsid  
mail.enable = true  
mail.enableSSL = false  
mail.host = siroe.com  
mail.port = 8990  
mail.proxyAdminID = admin  
mail.proxyAdminPwd = r6iwhIcDUL6r69vu2Jt24A==  
mail.requestTimeout =  
mail.spam.enableAction =  
mail.spam.folder =  
mail.uwcsieveCompatible = true
```

In the above command, the <group_name> is the name of the group for which you want to list the parameters. To get a list of the groups available in the Convergence deployment, use the -h option.

Here is an example:

```
# iwcadmin -l -h  
List all the configuration parameters and their values. Optionally takes  
group name as an argument and lists the parameters that belong to the  
given group.  
Available groups: base, ugldap, auth, mail, log, cal, ISS, ab, client,  
admin, sso, im, smime, user, notify
```

- To get the current version of the software:

```
iwcadmin -V
```

**Note**

You must restart GlassFish Server if you make any configuration changes using the `iwcadmin` command.

**Note**

If you use `tcsh` and enter an `iwcadmin` parameter enclosed in curly braces `{}`, you must escape or "quote" the braces by preceding each brace with a backslash (`\`).

For example:

```
\{ ... \}.
```

Command-line Options

This section gives a summary of all the command-line syntax options.

Options for Configuration Utility for Convergence

Option	Long Name	Description
<code>-W</code> (uppercase)	<code>--pwdfile</code>	File from which the utility reads the administrator password. Recommended for batch processes.
<code>-p</code>	<code>--port</code>	Administration port the server listens to.
<code>-s</code>	<code>--secure</code>	Optional. Ensures a secure HTTPS connection.
<code>-o</code>	<code>--option</code>	Configuration property name to read or write. If you do not specify the <code>-v</code> option, the utility performs a read operation. If this option is specified in the same command with the <code>-f</code> option, the <code>-f</code> option is ignored. The <code>-o</code> option takes precedence.
<code>-v</code>	<code>--value</code>	Value to be set. Use with the <code>-o</code> option and must be specified immediately after the <code>-o</code> option.
<code>-f</code>	<code>--file</code>	The file that contains the property name value pairs. This file contains multiple pairs of properties and their values. It enables an administrator to update multiple properties in a batch mode using a single command. The format of the file is a list of option and value pairs (separated by <code>=</code>), and a line return between options.
<code>-V</code>	<code>--version</code>	Version information of the product.
<code>-l</code>	<code>--list</code>	This option has no values. It retrieves all existing configuration parameters and displays them. Optionally, this parameter also takes a group name as an argument and lists the parameters that belong to the given group.
<code>-h</code>	<code>--help</code>	Help to use this utility.

Finding Information About Configuration Parameters

The `iwcadmin` command enables you to obtain details about the configuration parameters that you can use with the `-o` option by using this option along with the `-h` option. Before setting a configuration

parameter value, you can learn about the parameter usage, the functionality, and the supported data type.

The following syntax shows the usage of the `-o` option with the `-h` option:

```
iwcadmin [-p port_number] [-s] -o|--option <config_parameter_name>
-h|--help
```

The `--help` option displays the following configuration parameter details:

- Option Name: Name of the configuration parameter.
- Description: Short description.
- Syntax: Input data type.
- Allowed Pattern: Accepted parameter pattern or range of values.
- Current Value: Current value of this parameter in the Convergence deployment.

The following example displays help for the `user.mail.blockimages` configuration parameter:

```
iwcadmin -o user.mail.blockimages -h
Option Name: user.mail.blockimages
Description: Specifies if images in the incoming mail should be shown or
blocked
Syntax: boolean
Current Value: false
```

Setting and Unsetting Configuration Parameters

You can set or unset configuration parameters in Convergence. If a parameter does not require mandatory values, you can unset the parameter by setting its value to a blank string. You cannot unset parameters that require mandatory values.

For example, to unset the `ab.pstore.[psidentifier1].ldaphost` parameter, type the following command:

```
iwcadmin -o ab.pstore.[psidentifier1].ldaphost -v ""
```

This parameter is unset in the configuration.

To set a parameter, type the following command:

```
iwcadmin -o ab.pstore.[psidentifier1].ldaphost -v "<ldap_host_name>"
```

The `iwcadmin` command checks whether the parameter that you set is valid and has acceptable values.

Running the `iwcadmin` Utility in Batch Mode

To update multiple attributes or configuration parameters in your deployment, invoke the `iwcadmin` utility in batch mode. The `-f` option in the `iwcadmin` command enables you to set multiple parameters in a file by invoking the command only once.

To run the `iwcadmin` command in the batch mode:

1. Create a file with the name-value pairs for the options that you want to set. For example, the following entries in a file set the log level for all the log related modules in Convergence to the DEBUG level and the log rotation policy to 2048 bytes.

logLevelSetting
<pre>log.ADDRESS_BOOK.level = DEBUG log.ADMIN.level = DEBUG log.AUTH.level = DEBUG log.CONFIG.level = DEBUG log.DEFAULT.level = DEBUG log.PROTOCOL.level = DEBUG log.PROXY_CAL.level = DEBUG log.PROXY_MAIL.level = DEBUG log.SIEVE.level = DEBUG log.sizetriggerval = 2048</pre>

In this example, the left hand side option is the name of the parameter that you want to set and the right hand side string is the value that you want to set it to.

2. Save the file at an appropriate location. For example, /tmp/logLevelSetting.
3. Type the iwadmin command with the -f option and provide the path to the file:

running iwadmin command in batch mode
<pre>iwadmin -f /tmp/logLevelSetting</pre>

Chapter 3. Convergence Administrative Tasks

Convergence Administrative Tasks

- Authentication
- Access Manager
- OpenSSO
- Basic Monitoring
- Logging
- User Options
- SSL
- Address Book
- Single Sign-on
- LDAP Service
- Configuration Management
- Deployment Specific Customizable Client Options for Convergence
- Instant Messaging
- Enabling Anti-Spam
- Enabling Indexing and Search Service
- Enabling CalDAV Service
- Miscellaneous



Note

Unless otherwise specified, the instructions for these common Convergence administrative tasks are applicable to all Convergence versions.

Authentication

- How do I set up Convergence user interface login for end users?
- How do I configure LDAP authentication in Convergence?
- How do I configure Convergence to use separate Directory Server for user authentication and another to store User/Group information?
- How to use LDAP in SSL mode?
- How do I write a custom authentication module?

How do I set up Convergence user interface login for end users?

To set up Convergence UI login for end users, evaluate if you want to use:

- UID (default), or
- Email Address Login (LDAP mail attribute)

The procedures for setting up email address login which uses the LDAP `mail` attribute are the following:

- Constructing a Filter for Email Address Login
- Enabling Email Address Login on Convergence Server
- Activating `mailAlternateAddress` (optional)

Constructing a Filter for Email Address Login

In order to create a filter for email address login, you need the `uid` and `mail` attributes.

`mail` identifies the primary email address for a user, Calendar group, or Calendar resource. This is the email address retrieved and displayed by lookup applications.

The following variables are used in constructing the filter:

Variable	Description
%U	Name part of the login name (that is, everything before the login separator stored in the servers configuration)
%V	Domain part of the login string
%o	Original login ID entered by the user

For more information on LDAP attributes, specifically, `inetDomainSearchFilter`, see [Messaging Server, Calendar Server, and Contacts Server LDAP Object Classes and Attributes](#).

Enabling Email Address Login on Convergence Server

To set up email address login, enable it on the Convergence Server:

```
iwcadmin -o ugldap.ugfilter -v "(|(uid=%U)(mail=%o))"
```

See: [Convergence Reference](#) for information on `ugldap.ugfilter`.

Activating `mailAlternateAddress` (optional)

`mailAlternateAddress` is the alternate RFC 822 email address of this recipient. A filter similar to `mail` can be performed on `mailalternateaddress`:

```
iwcadmin -o ugldap.ugfilter -v  
"(|(uid=%U)(mail=%o)(mailalternateaddress=%o))"
```

How do I configure LDAP authentication in Convergence?

LDAP authentication is enabled by default when you configure Convergence. You can use separate LDAP servers to store authentication information and user preferences. By default, Convergence uses UG LDAP as the authentication LDAP server. You can enable LDAP authentication by using the following command line option:

```
iwcadmin -o auth.ldap.enable -v true
```

How do I configure Convergence to use separate Directory Server for user authentication and another to store User/Group information?

When LDAP authentication module is configured for authentication, the LDAP authentication module, by default, uses the UG LDAP for authentication. If you use separate LDAP servers for storing the authentication information and user preferences, the schema type and user trees should match in both the LDAP stores.

To enable your site to use a separate LDAP server for authentication, you must set the following

configuration parameters.

- `auth.ldap.enable` - Set this parameter to `true`.
- `auth.ldap.schemaversion` - Set this parameter to the schema version that you are using for the UG LDAP. The schema versions for the UG LDAP and authentication LDAP must be the same.
- `auth.ldap.dcreot` - DC (Domain Component) or user tree root node in the LDAP. This should be the same value as in the UG LDAP.
- `auth.ldap.host` - Host name of the authentication LDAP server.
- `auth.ldap.enablessl` - Set this parameter to `true` or `false` to enable or disable SSL.
- `auth.ldap.port` - Port number that the LDAP server listens to. If the LDAP server is configured in SSL mode, you must provide the SSL port.
- `auth.ldap.minpool` - Minimum number of connections that you want to have when the LDAP pool is initialized.
- `auth.ldap.maxpool` - Maximum number of connections that you want to have when the LDAP pool is initialized.
- `auth.ldap.timeout` - Set this to the maximum number seconds that the LDAP server should wait for returning search results before aborting the search.
- `auth.ldap.binddn` - The Bind DN of the user. The LDAP server privilege user ID. For example, `cn=DirectoryManager`.
- `auth.ldap.bindpwd` - The bind DN user password.

You can set the parameters in batch mode. See [Running the `iwcadmin` command in Batch Mode](#).

The following configuration parameter can be set when the administrator needs to customize default values.

```
iwcadmin -o auth.ldap.ugfilter -v <ugfilter>
```

This should result in unique user entry under given domain/organization. For example, `(|(uid=%U)(mail=%o))` otherwise it will cause unexpected results. If not set `(uid=%U)` will be used as default value.

How to use LDAP in SSL mode?

If you use the same LDAP server, both for authentication and storing user preferences, you must set the `ugldap.enablessl` and `ugldap.port` configuration parameters by using the `iwcadmin` command-line utility.

```
iwcadmin -o ugldap.enablessl -v true
iwcadmin -o ugldap.port -v <user_group_ldap_port>
```

if your deployment uses an LDAP server other than the User/Group LDAP for authentication, you must set the following parameters by using the `iwcadmin` command-line utility:

```
iwcadmin -o auth.ldap.enablessl -v true
iwcadmin -o auth.ldap.port -v <ldapport>
```

How do I write a custom authentication module?

See [Writing a Custom Authentication Module for Convergence](#).

Access Manager



Note

Access Manager can only be used with Convergence 2.x and earlier. See: [Deprecated Support of Access Manager and Sun OpenSSO](#).

- How do I set up Access Manager authentication?
- How do I set up Access Manager SSO?



Note

A pre-requisite for the use of Access Manager for authentication and/or SSO is that either the Access Manager Server be deployed in the same web-container as Convergence or the Access Manager Client SDK has been correctly configured to access the remote Access Manager Server. For more information, see [Communications Suite 6 Installation Scenario - Install Convergence](#).

How do I set up Access Manager authentication?

The Convergence configurator by default uses LDAP authentication for authentication mechanism. For authentication through Access Manager in Legacy mode, type the following command:

```
iwcadmin -o auth.am.enable -v true
```

To enable Access Manager in realm mode for authentication, set the `auth.am.realmmode` and `auth.am.enable` parameters to `true`. Type the following command:

```
iwcadmin -o auth.am.realmmode -v true
```



Note

To set up an authentication realm in Access Manager, you should also read the following example: [Convergence Configuration Example - Creating an Authentication Realm in Access Manager](#) in addition to reading this section.

How do I set up Access Manager SSO?

Access Manager Single Sign-On can be enabled by setting the following parameters:

- `sso.am.enable` - Set this parameter to `true`.
- `sso.adminuid` - Set this parameter to Access Manager's administrator user ID.
- `sso.adminpwd` - Set this parameter to Access Manager's administrator password.
- `sso.enablerefreshsso` - Set this parameter to `true` to enable Access Manager SSO refresh.
- `sso.refreshinterval` - Set this to the Access Manager maximum session idle time (in percentage) after which the SSO token should be refreshed.
- `sso.enablesignoff` - Set this parameter to `true` to enable single sign-off.
- `sso.loginpage` - Set this parameter to redirect the user to login page.

**Note**

User is redirected to the page that is set using the `sso.loginpage` parameter when the user tries to access Convergence without authenticating with Access Manager or after session timeout. The valid entry for `sso.loginpage` parameter is Access Manager Login URL with goto URL to Convergence and it is used only when SSO is enabled.

For example: `sso.loginpage =`

`"http://AccessManagerHost:Port/amserver/UI/Login?goto=
http://ConvergenceHost:Port/iwc"`

For example:

```
iwcadmin -o sso.am.enable -v true
iwcadmin -o sso.adminuid -v <adminuserid>
iwcadmin -o sso.adminpwd -v <adminpassword>
iwcadmin -o sso.enablerefreshsso -v true
iwcadmin -o sso.refreshinterval -v 10
iwcadmin -o sso.enablesignoff -v true
iwcadmin -o sso.loginpage -v <login_page>
```

OpenSSO

**Note**

Open SSO is only supported on Convergence 2.x and earlier. See: [Deprecated Support of Access Manager and Sun OpenSSO](#).

- [How do I set up OpenSSO SSO and Authentication in Convergence ?](#)

How do I set up OpenSSO SSO and Authentication in Convergence ?

See [Configuring Convergence With OpenSSO Enterprise 8.0 for Authentication and SSO](#).

Basic Monitoring

Monitoring is the process of gathering run time data, exposing the data, and computing quality of service so that an administrator can assess the performance of the deployment. This section describes how to monitor Convergence. Convergence can be monitored using any JMX (Java Management Extension) compliant monitoring client.

- [What are the parameters that can be monitored in Convergence?](#)
- [How do I monitor Convergence using Jconsole?](#)

What are the parameters that can be monitored in Convergence?

You can monitor the following components and modules:

- Authentication LDAP
 - Hostname of the directory server from which the connections are being served
 - Number of free connections in the pool
 - Number of used connections in the pool

- Calendar Service Connection
 - Total number of active sessions
 - Details of each active session. Including user ID, IP address, domain name, and the duration of this connection
 - Number of sessions since the start of the server
- Mail Service Connection
 - Total number of active sessions
 - Details of each active session. Including user ID, IP address, domain name, and the duration of this connection
 - Number of sessions since the start of the server
- Session
 - Total number of active sessions
 - Details of each active session
 - Number of sessions since the start of the server
- User and Group LDAP
 - Host name of the directory server from which the connections are being served
 - Number of free connections in the pool
 - Number of used connections in the pool

You can also see the duration for which the server is active.

How do I monitor Convergence using Jconsole?

Jconsole is a JMX-compliant GUI tool that connects to a running JVM. The JMX management agent to monitor the server is not started on server startup by default. You can start the management agent by setting the `admin.enablemonitoring` attribute by using the `iwadmin` command-line utility. To enable monitoring, type the following command:

```
iwadmin -o admin.enablemonitoring -v true
```



Note

You must restart the Application Server for Convergence 1.x (or GlassFish Server starting with Convergence 2) if you make any configuration changes by using the `iwadmin` command.

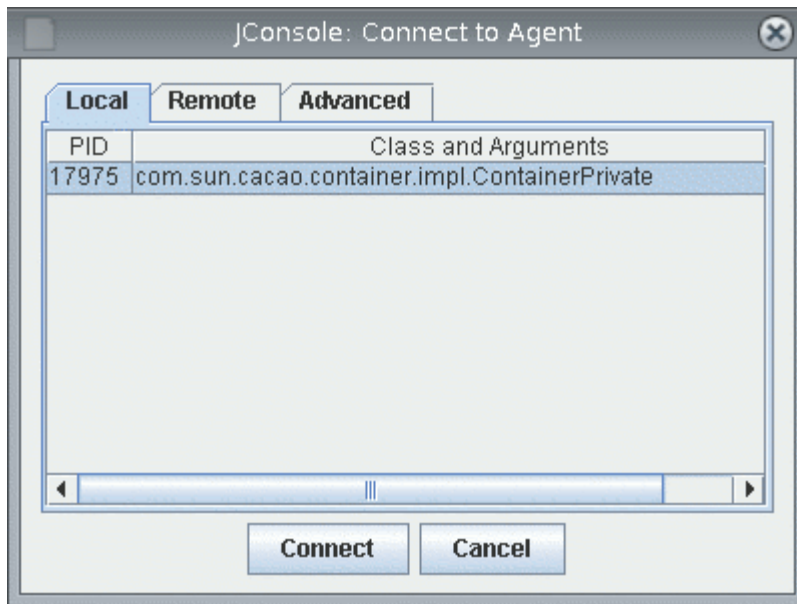
To monitor the various parameters in Convergence:

1. Start Jconsole.

To start Jconsole, run the following command:

```
#<JAVA_HOME>/bin/jconsole
```

The Jconsole Connection Agent dialog box appears.



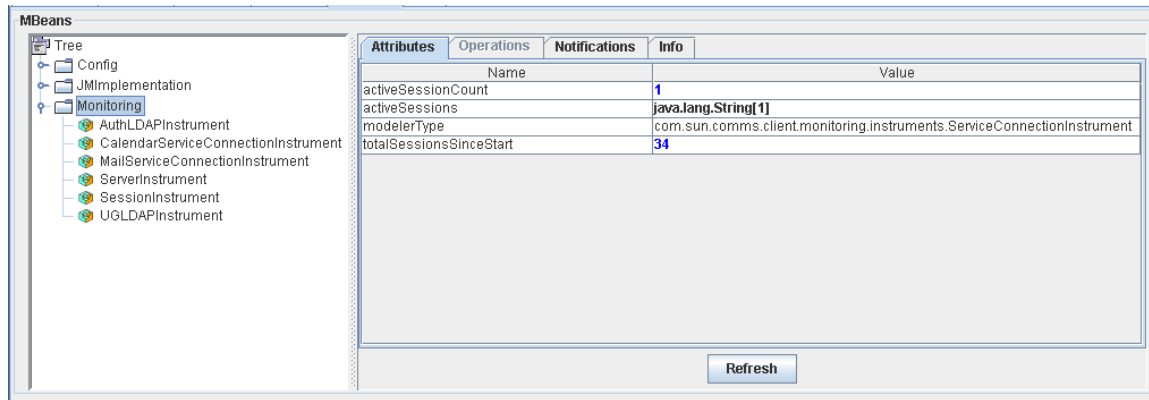
2. Click the Advanced tab.
3. In the JMX URL field type
`service:jmx:rmi://<hostname>:port/jndi/rmi://<hostname>:port/jmxrmi.`

i Tip

You can obtain this URL from the `iwc.log` file. The JMX console URL is written to the log file when Convergence server starts the admin server. Here is an example:

```
CONFIG: INFO from com.sun.comms.client.admin.web.JMXAgent
Thread pool-1-thread-7
at 2009-02-23 21:55:31,981 - RMI connector server in non-SSL
mode started successfully.
CONFIG: INFO from com.sun.comms.client.admin.web.JMXAgent
Thread pool-1-thread-7
at 2009-02-23 21:55:31,983 - Service URL is:
[ service:jmx:rmi://siroe.com:50005/jndi/rmi://siroe
.com:50005/jmxrmi ]
```

4. Enter the administrator userid and password.
5. Click Connect.
6. Expand the Monitoring node.



On the right hand side of the screen you will see the various components of JVM available in tabs. The leaves under the Monitoring node on the left hand side shows the various Instruments that can be used to monitor the JVM.

Logging

Convergence creates log files that records events, status of various software components, system errors, and other aspects of the server such as session, IP addresses and so on. By examining the log files, you can monitor the server's operation. This section provides information about logging:

- [How do I enable logging?](#)
- [What are the existing Log Levels?](#)
- [What are the components for which I can enable logging?](#)
- [How do I specify a log file location?](#)
- [Can the administration log file be separate from the application log file?](#)
- [What is log rotation and how do I enable rotation policy for logs?](#)
- [How do I log the IP address and the session tracking information for a user?](#)
- [What does a typical Convergence logging session look like?](#)

How do I enable logging?

Communication Center uses a set of loggers for various components of the server. You can enable and set log levels for each of the components by using the `iwadmin` command.

For example, the following command sets the Address Book logging to the level `INFO`.

```
iwadmin -o log.ADDRESS_BOOK.level -v INFO
```

What are the existing Log Levels?

Convergence uses Apache Log4j as its underlying logging framework. All the log levels that Log4j offers are available in Convergence. The following log levels are available:

- OFF
- ERROR
- WARN
- INFO
- DEBUG

What are the components for which I can enable logging?

The following are the components of Convergence that you can set logging information.

- Address Book
- Administration
- Authentication
- Configuration
- Default
- Protocol
- Proxy
- Mail Proxy
- SIEVE filters

For each of the above components, you can set a log level. The existing log levels are described in [What are the Different Log Levels Available?](#). To see the list of components for which logging can be enabled, use the following command:

```
iwcadmin -l | grep log.*.level

log.ADDRESS_BOOK.level = INFO
log.ADMIN.level = INFO
log.AUTH.level = DEBUG
log.CONFIG.level = INFO
log.DEFAULT.level = INFO
log.PROTOCOL.level = INFO
log.PROXY_CAL.level = INFO
log.PROXY_MAIL.level = INFO
log.SIEVE.level = INFO
```

How do I specify a log file location?

You can specify the following log locations:

- Application log location: All log information generated by the server are sent to the application log. This log file contains information about the behavior of the application.
- Administration log location: All log information that is generated by the administration command-line utility, `iwcadmin` are sent to the administration log location.

To set log information for the application logger, type the following command:

```
iwcadmin -W /location/mypasswordfile -o log.location -v /data/logs/
```

To set the logging information for the administration logger, use the following command:

```
iwcadmin -W /location/mypasswordfile -o log.adminloglocation -v
/data/logs/newadminlogfile.log
```

Can the administration log file be separate from the application log file?

Yes, the administration log file is separate from the application log.

Type the following command to determine the administration log file location:

```
iwcadmin -W /location/mypasswordfile -o log.adminloglocation
```

What is log rotation and how do I enable rotation policy for logs?

Log rotation is an approach to manage log files by renaming the existing log file and creating a new log file. All the log messages generated after creating the new file is written in this new log file.

Convergence supports log rotation based on size or time. Size-based log rotation is triggered when the log file reaches a specified size in kb (kilobytes). Time based log rotation is triggered based on the date pattern specified by the administrator.

This example shows how to set size based log rotation:

```
iwcadmin -W /location/mypasswordfile -o log.sizetriggerval -v 102400
```

This example shows how to set time based log rotation policy:

```
iwcadmin -W /location/mypasswordfile -o log.timetriggerval -v  
"'. 'YYYY-MM"
```

For more information about frequency patterns for time based log rotation, see <http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/DailyRollingFileAppender.html>.

How do I log the IP address and the session tracking information for a user?

To log IP address and session tracking information, you must modify the log pattern to include the IP address and session ID of a user so that these get added into the log file. Type the following command:

```
iwcadmin -W /location/mypasswordfile -o log.pattern -v '%c: %p from %C  
Thread %t ipaddress=%X{ipaddress} sessionid=%X{sessionid} at %d - %m %n'  
iwcadmin -W /location/mypasswordfile -o log.enableusertrace -v true
```

Modify the log-pattern to include the user IP address (%X{ipaddress}) and session id (%X{sessionid}) in the log messages.



Note

If the GlassFish Server hosting Convergence resides behind a front-end reverse proxy or load balancer (WebServer), this front-end's IP address is captured, not the browser's IP address. To overcome this situation, use the following command to set the `authPassthroughEnabled` or `auth-pass-through-enabled` parameter to `true` on the GlassFish Server.

For GlassFish Server 2.x:

```
./asadmin set <CLUSTER_NAME>-config.http-service.property
.authPassthroughEnabled=true
```

For GlassFish Server 3.x:

```
./asadmin set server-config.network-config.protocols.protocol
.http-listener-1.http.auth-pass-through-enabled=true
```

In case you are using a reverse proxy in front of Convergence, you have to configure that reverse proxy to put the original client IP address into an HTTP Header that **must** be called `proxy-ip`.

For GlassFish Server 3.x, if you have set `auth-pass-through-enabled` to `true`, then your load balancer or reverse proxy must be passing the IP address to the client. If you do not configure the load balancer or reverse proxy in this manner, or if you bypass the load balancer, you will not be able to log into Convergence.

GlassFish Load Balancer plugin automatically adds client original IP address to HTTP Header `proxy-ip`.

What does a typical Convergence logging session look like?

The following example shows a typical logging session:

```
PROTOCOL: DEBUG from com.sun.comms.client.web.IwcCookieManager Thread
httpSSLWorkerThread-80-23 ipaddress=198.51.100.0 sessionId= at
23:08:31,920- cleaning client cookies: webmailcookieName is webmailsid
PROTOCOL: DEBUG from com.sun.comms.client.web.IwcCookieManager Thread
httpSSLWorkerThread-80-23 ipaddress=198.51.100.0 sessionId= at
23:08:31,920- cleaning client cookies: webmailcookiePath is /
PROTOCOL: DEBUG from com.sun.comms.client.web.IwcCookieManager Thread
httpSSLWorkerThread-80-23 ipaddress=198.51.100.0 sessionId= at
23:08:31,920- Cookie sent by client : JSESSIONID
value=687380a1199c738c5165692c4587 path=null comment=null domain=null
version=0 isSecure? false maxAge=-1
PROTOCOL: DEBUG from com.sun.comms.client.web.IwcCookieManager Thread
httpSSLWorkerThread-80-23 ipaddress=198.51.100.0 sessionId= at
23:08:31,921- Removing iwc client cookie JSESSIONID
```

These messages indicate that the user session has been invalidated by the server. There are a few reasons why a user session is invalidated:

- a logout is issued from the browser.
- a new login is initiated, but there is already active session in progress.
- the Application Server is shutdown. All sessions are then invalidated.

User Options

- [How do I set end user option defaults for Convergence?](#)
- [How do I change the set of services available to users of Convergence?](#)

How do I set end user option defaults for Convergence?

Convergence provides default values for user attributes. However, you can change these default values to suite your needs.

For Convergence 1.x: the default values can be changed by using the `imadmin` command-line utility. To see a list of all the user options, see [User Preferences Configuration Properties for Convergence 1.x](#).

For Convergence 2 and later: the default values can be changed by using the `iwcadmin` command-line utility. To see a list of all the user options, see [User Preferences Configuration Properties for Convergence 2 and later](#)

How do I change the set of services available to users of Convergence?

See [Enabling Services for Convergence](#).

SSL

- [How do I configure SSL in Convergence?](#)
- [What is authentication only SSL and how do I configure it?](#)
- [How do I enable SSL for back-end servers?](#)

How do I configure SSL in Convergence?

SSL provides a secure means of communication between the web-browser client and the server. You can enable SSL in Convergence in two ways:

- At the time of configuring Convergence, or
- By setting the SSL configuration parameters after configuration.

To enable Convergence to use SSL, you must enable SSL at the Application Server level for Convergence 1.x (or GlassFish Server for Convergence 2 and later) and also set the `base.sslport` configuration parameters using the `iwcadmin` command-line utility.

For `base.sslport` properties, refer to [Global Configuration Properties](#).

```
iwcadmin -o base.sslport -v <base_ssl_port>
```

What is authentication only SSL and how do I configure it?

Authentication-Only SSL is a mechanism in which users are authenticated by using the HTTPS protocol which prevents user authentication details from being sent unencrypted. All other requests from the client are performed using the HTTP protocol. To configure Convergence to use Authentication only SSL, you must set both the `base.sslport` to the Application Server (or GlassFish Server for Convergence 2 and

later) SSL port value, and the `base.enableauthonlyssl` value using the `iwcadmin` command-line utility. For example:

```
iwcadmin -o base.sslport -v <base_ssl_port>
iwcadmin -o base.enableauthonlyssl -v true
```

How do I enable SSL for back-end servers?

To enable SSL for back-end servers, you must set the SSL parameters for Mail and Calendar servers by using the `iwcadmin` command-line utility:

Enabling SSL for Mail Server

To enable SSL for mail server, set the `mail.enable` and `mail.port` configuration parameters.

```
iwcadmin -o mail.enablessl -v true
iwcadmin -o mail.port -v <mail_port>
```



Note

Mail server must be running in SSL mode on this port.

Enabling SSL for Calendar Server

To enable SSL for Calendar server, set the `cal.enablessl` and `cal.port` configuration properties.

```
iwcadmin -o cal.enablessl -v true
iwcadmin -o cal.port -v <calendar_port>
```



Note

Calendar server must be running in SSL mode on this port.

Enabling SSL for Address Book

Address book is a part of Convergence server. If you need to configure Address Book for SSL, Convergence should be configured for SSL. You can also configure Convergence to communicate with Directory in SSL mode.

Enabling SSL for Instant Messaging

In the case of Instant Messaging server, end to end (that is, Instant Messaging web client to Instant Messaging Back-end server) TLS/SSL is not supported. The reason being, whenever chat messages are sent to the instant messaging server, they pass through HTTP bind. HTTP bind in turn interprets these messages and sends them to the instant messaging server. Therefore, an SSL connection is not possible.

You can however configure HTTP bind and instant messaging server to communicate in TLS (Transport Layer Security) mode. Enable the following parameters in the `iim.conf` file. The `iim.conf` file is present in the `/opt/sun/comms/im/config/` directory.

```
iim_server.component.requiresssl=true
```

When this parameter is enabled, the server mandates that the communication from HTTP bind happens only by TLS. That is, the server will send and receive only encrypted data and messages.

Set the `iim_server` parameter to true to enable SSL.

```
iim_server.usessl=true
```

Set the `iim_server.sslkeystore` parameter to point to the location of the SSL keystore file.

```
iim_server.sslkeystore=/opt/SUNWiim/config/<keystore_file_name>.jks
```

Set the `iim_server.keystorepasswordfile` parameter to the SSL password.

```
iim_server.keystorepasswordfile=/opt/SUNWiim/config/sslpassword.conf
```

Address Book

- Which data store is used by address book in an out of the box setup?
- How do I configure horizontal scalability for personal address book?
- How to configure address book to use directory server other than user group directory server?
- How do I configure the corporate directory?
- How do I enable autocompletion of address for Corporate Directory?
- How to set up a domain based configuration for address book?
- How do I disable the Corporate Directory in specific domains?
- How do I change the default Corporate Directory search filter in Address Book?
- How do I configure Convergence to make use of Virtual List View (VLV) for Corporate Directory?
- What vCard standards does supported by Convergence?
- What character formats does the Convergence Address Book support for importing and exporting vCard?
- How do I change the character set for a locale to import or export vCard entries?
- How to enable export and import of contacts with photo in vCard 3.0?
- How do I hide the admin accounts from the Corporate Directory in the default domain?
- How do I remove personal address books of deleted users?
- What does Convergence do with personal address book contacts that have been deleted by the end user?

Which data store is used by address book in an out of the box setup?

Address book uses user group directory server configuration for personal address book and corporate directory.

How do I configure horizontal scalability for personal address book?

See [Configuring Horizontal Scalability of Address Book](#).

How to configure address book to use directory server other than user group directory server?

To configure Personal Address Book to use directory server other than user group directory server, set the following configuration parameters:

- `ab.pstore.[<identifier>].ldaphost` - Set this parameter to the hostname of the LDAP server.
- `ab.pstore.[<identifier>].ldapport` - Set this parameter to the port number on which the LDAP server listens.
- `ab.pstore.[<identifier>].ldapbinddn` - Set this parameter to the LDAP binddn value of the LDAP server.
- `ab.pstore.[<identifier>].ldapbindcred` - Set this parameter to the Bind credentials of the LDAP server.

The following example shows the configuration parameter settings:

```
iwcaadmin -W /location/mypasswordfile -o
ab.pstore.[psidentifier1].ldaphost -v host.siroe.com
iwcaadmin -W /location/mypasswordfile -o
ab.pstore.[psidentifier1].ldapport -v 400
iwcaadmin -W /location/mypasswordfile -o
ab.pstore.[psidentifier1].ldapbinddn -v "cn=Directory Manager"
iwcaadmin -W /location/mypasswordfile -o
ab.pstore.[psidentifier1].ldapbindcred -v dmcredentials
```

Personal store can be configured with multiple directory servers. In above example `psidentifier1` is used to identify personal store configuration for `siroe.com`.

If the above configured directory server needs to act as the personal store's default server, then set the `{ab.pstore.defaultserver}` configuration parameter. Here is an example:

```
iwcaadmin -W /location/mypasswordfile -o ab.pstore.defaultserver -v
psidentifier1
```

How do I configure the corporate directory?

To configure corporate directory to use directory server other than user group directory server, set the following configuration parameters:

- `ab.corpdir.[<identifier>].ldaphost`
- `ab.corpdir.[<identifier>].ldapport`
- `ab.corpdir.[<identifier>].ldapbinddn`
- `ab.corpdir.[<identifier>].ldapbindcred`

The following example has the configuration parameters settings:

```
iwcaadmin -W /location/mypasswordfile -o ab.corpdir.[default].ldaphost
-v host.siroe.com
iwcaadmin -W /location/mypasswordfile -o ab.corpdir.[default].ldapport
-v 400
iwcaadmin -W /location/mypasswordfile -o ab.corpdir.[default].ldapbinddn
-v "cn=Directory Manager"
iwcaadmin -W /location/mypasswordfile -o
ab.corpdir.[default].ldapbindcred -v xyzxyz
```

In the above example `default` is used to identify corporate directory configuration for `host.siroe.com`.



Note

For a single corporate directory configuration, you must use `default` as the identifier.

To configure and enable multiple corporate directories, see: [Setting Up Multiple Corporate Directories in Convergence](#).

How do I enable auto completion of address for Corporate Directory?

To enable auto completion of email address for Corporate Directory, you must set the `client.enablecorpabautocomplete` configuration parameter to `true`.

```
iwcadmin -o client.enablecorpabautocomplete -v true
```



Note

The search results will appear in the Convergence client, after the first three characters of the name or email address are typed.

How to set up a domain based configuration for address book?

You can set up a domain based configuration for Personal Address Book and Corporate Directory.

To set up domain-based configuration for Personal Address Book, set the following parameters by using the `iwcadmin` command-line utility:

- `ab.{<identifier>}.psrootpattern`
- `ab.{<identifier>}.pstore.defaultserver`
- `ab.{<identifier>}.pstore.[<identifier>].ldaphost`
- `ab.{<identifier>}.pstore.[<identifier>].ldapport`
- `ab.{<identifier>}.pstore.[<identifier>].ldapbinddn`
- `ab.{<identifier>}.pstore.[<identifier>].ldapbindcred`

The following example shows the configuration parameter settings:

```
iwcadmin -W /location/mypasswordfile -o ab.{somedomain.com}.psrootpattern -v ldap:///piPStoreOwner=%U,o=%D,o=PiServerDb
iwcadmin -W /location/mypasswordfile -o ab.{somedomain.com}.pstore.defaultserver -v domainid1
iwcadmin -W /location/mypasswordfile -o ab.{somedomain.com}.pstore.[domainid1].ldaphost -v host.xyz.com
iwcadmin -W /location/mypasswordfile -o ab.{somedomain.com}.pstore.[domainid1].ldapport -v 400
iwcadmin -W /location/mypasswordfile -o ab.{somedomain.com}.pstore.[domainid1].ldapbinddn -v "cn=Directory Manager"
iwcadmin -W /location/mypasswordfile -o ab.{somedomain.com}.pstore.[domainid1].ldapbindcred -v xyzcred
```

In the above example, `somedomain.com` is the domain (within curly braces).

All the above configuration data for the domain `somedomain.com` is grouped in to one logical set identified by using the identifier `domainid1`.

The example shows the minimum set of configuration parameters that you need to set for the domain based configuration for Personal Address Book. However, you can set other configuration parameters.

To set the `lookthruLimit` to 2000 for Personal Address Book in domain `somedomain.com`, type the following command:

```
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.pstore.lookthruLimit -v 2000.
```

To set up domain-based configuration for Corporate Directory:

1. Set the following configuration parameters:

- `ab.{<identifier>}.corpdir.[<identifier>].urlmatch`
- `ab.{<identifier>}.corpdir.[<identifier>].searchattr`
- `ab.{<identifier>}.corpdir.[<identifier>].lookthruLimit`
- `ab.{<identifier>}.corpdir.[<identifier>].ldaphost`
- `ab.{<identifier>}.corpdir.[<identifier>].ldapport`
- `ab.{<identifier>}.corpdir.[<identifier>].ldapbinddn`
- `ab.{<identifier>}.corpdir.[<identifier>].ldapbindcred`

The following example shows the configuration parameter settings:

```
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].urlmatch
-v ldap://corp-directory1
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].searchattr
-v entry/displayname,@uid
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].lookthruLimit
-v 3000
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].ldaphost
-v host.abc.com
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].ldapport
-v 389
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].ldapbinddn
-v "cn=Directory Manager"
iwcadmin -W /location/mypasswordfile -o
ab.{somedomain.com}.corpdir.[corpdomainid1].ldapbindcred
-v abcabc
```



Note

The value for the `urlmatch` configuration parameter must be unique. Format for `urlmatch` is `ldap://<unique_value>` or `ldap://host:port/DN` e.g. `ldap://corp-directory1`, `ldap://corporatedirectory2`, `ldap://somehost:390/ou=people,o=ab.org` etc.

First time when user does address book operation (apart from login.wabp), corporate directory entry (under `piPStoreOwner=<user>`, `o=<domain>`, `o=PiServerDb`) with `piRemotePiURL` attribute value as `urlmatch` gets created. After this if `urlmatch` is changed, either delete such entries so that this entry gets created when first AB command is issued or update corporate directory entry for all users with new `urlmatch` value.

In the above example, `somedomain.com` specifies the domain. All the above configuration data for the domain `somedomain.com` is grouped in to one logical set identified by using identifier `corpdomainid1`.

2. Copy `dictionary-<locale>.xml` (for example: `dictionary-en.xml`) from `convergence_srv_base/config/templates/ab/domain/defaulttps` to `convergence_srv_base/config/templates/ab/domain/<domain-directory>`. The `dictionary-<locale>.xml` file can be updated in order to change or to customize display name and description.

How do I disable the Corporate Directory in specific domains?

In some cases, you might want to disable your corporate directory in certain domains. To do so, follow these steps:

1. Set both personal address book and Corporate Directory settings as described in [How to set up a domain based configuration for address book?](#)
2. Disable the Corporate Directory for the specific domain:

```
./iwcadmin -o ab.{somedomain.com}.corpdir.[default].enable" -v  
false
```

3. Restart GlassFish Server.

Note

You can ignore errors or exceptions in the log files.

How do I change the default Corporate Directory search filter in Address Book?

Note

In Convergence 1.x patch 137631-01 (Solaris Sparc), 137632-01 (Solaris x86), 137633-01 (Linux) or greater is required for this functionality to work as documented.

To change the default corporate directory search filter, you must set the `ab.corpdir.<identifier>.searchfilter` configuration parameter with the search criteria you want to base your corporate directory searches on.

The following is an example of the usage of search customization:

```
iwcadmin -o ab.corpdir.[default].searchattr  
-v entry/displayname,@uid,person/surname  
iwcadmin -o ab.corpdir.[default].searchfilter  
-v '(&(&([filter]))(|(objectClass=GROUPOFUNIQUE NAMES)(objectClass=GROUPOFURLS)  
\\  
(objectClass=ICSCALENDARRESOURCE)(objectClass=INETORGP PERSON)))(objectClass=*))
```

In the above command, `[filter]` is replaced with the search generated by the `ab.corpdir.<identifier>.searchattr` configuration option.

The above example produced the following LDAP output in the corporate LDAP directory access logs when an end-user searched for `"bob"`:

```
[13/Oct/2008:11:51:54 +1100] conn=686404 op=30 msgId=576 - SRCH
base="o=sun.com,o=isp" scope=2
filter="(&(&(|(|(cn=bob*)(uid=bob*)))(sn=bob*))(|(objectClass=GROUPOFUNIQUENAME
createTimestamp cn uid description mail multiLineDescription modifyTimestamp"
```

How do I configure Convergence to make use of Virtual List View (VLV) for Corporate Directory?

Follow these steps to configure Convergence to make use of VLV:

1. Configure Directory Server with VLV. For more information on creating and managing browsing indexes in Directory Server:
 - [How do I configure VLV \(Virtual List View\) browsing indexes for Directory Server?.](#)
 - [Managing Browsing Indexes.](#)
2. Set the VLV filter and scope in the corporate directory.

```
iwcadmin -o ab.corpdir.[default].vlvfilter -v "(&(mail=*)(cn=*))"
iwcadmin -o ab.corpdir.[default].vlvscope -v 2
```

3. Enable the `ab.corpdir.[default].vlvpaging` configuration parameter to `true`.

```
iwcadmin -o ab.corpdir.[default].vlvpaging -v true
```

What vCard standards does supported by Convergence?

Convergence supports the following vCard standards:

- vCard 2.1
- vCard 3.0

What character formats does the Convergence Address Book support for importing and exporting vCard?

Convergence supports the following encoding formats:

- UTF-8
- ISO-8859-1
- BIG5
- EUC-CN
- EUC-JP
- EUC-KR
- SHIFT_JIS

How do I change the character set for a locale to import or export vCard entries?

Convergence supports the following locales:

- English
- Japanese
- French
- German
- Spanish
- Korean
- Traditional Chinese

- Simplified Chinese

For each locale, configuration parameters for import and export exist in the Convergence server. By default, these configuration parameters are assigned a character encoding when you install Convergence.

The following table shows the default encoding formats for locales when Convergence is installed. The table also lists the configuration parameters that are assigned for storing the import and export preference for the locale.

Locale	Encoding	Configuration Parameter for Import	Configuration Parameter for Export
English	UTF-8	ab.import.vcard.misc.en	ab.export.vcard.misc.en
Japanese	UTF_8	ab.import.vcard.misc.ja	ab.export.vcard.misc.ja
French	UTF-8	ab.import.vcard.misc.fr	ab.export.vcard.misc.fr
German	UTF-8	ab.import.vcard.misc.de	ab.export.vcard.misc.de
Korean	UTF-8	ab.import.vcard.misc.ko	ab.export.vcard.misc.ko
Traditional Chinese	UTF-8	ab.import.vcard.misc.zh-tw	ab.export.vcard.misc.zh-tw
Simplified Chinese	UTF-8	ab.import.vcard.misc.zh-cn	ab.export.vcard.misc.zh-cn

In the previous table, the character encoding for English is set to UTF-8. This setting means that when you import or export vCard contacts to or from the Convergence client, the vCard entries are imported or exported in the UTF-8 format character set. In this case, UTF-8 is the default setting for English users.

To enable the Convergence client to import or export vCard entries to other character sets, set the address book vCard configuration parameter in the Convergence server. To learn more about the character sets supported by Convergence, see [What character sets does Convergence Address Book support for importing and exporting vCard?](#)

Type the `iwcadmin` command to set the import and export character set preferences for the configuration parameters of the locale. This command enables you to change the character set encoding for importing or exporting vCard entries.

To change the character encoding for the Japanese user vCard from UTF-8 to Shift_JIS for example, set the corresponding configuration parameters for import and export.

To set the character encoding to import vCard entries for the Japanese locale, type the following command:

```
iwcadmin -o ab.import.vcard.misc.ja -v Shift_JIS
```

To set the character encoding to export vCard entries for the Japanese locale, type the following command:

```
iwcadmin -o ab.export.vcard.misc.ja -v Shift_JIS
```

The vCard entries are imported or exported in the Shift_JIS encoding character set.

**Note**

You must set the same character set encoding for both import and export for a locale.

How to enable export and import of contacts with photo in vCard 3.0?

Convergence supports Vcard 3.0. Vcard 3.0 enables users to include photos in their contacts. By default, Convergence does not import or export photos of your contacts. If you want photos to be imported or exported, you must enable the `ab.exportphoto` and `ab.importphoto` configuration parameters.

To enable exporting of contacts with photo in Vcard 3.0 format, type the following command:

```
iwcadadmin -W /location/mypasswordfile -o ab.exportphoto -v true
```

To import contacts with photo in Vcard 3.0 format, type the following command:

```
iwcadadmin -W /location/mypasswordfile -o ab.importphoto -v true
```

How do I hide the admin accounts from the Corporate Directory in the default domain?

**Note**

Convergence 1.x patch 137631-01 (Solaris Sparc), 137632-01 (Solaris x86), 137633-01 (Linux) or greater is required for this functionality to work as documented.

When looking in the Corporate Directory of the default domain all the administrative accounts are being displayed. These can be hidden by using `psIncludeInGAB` attribute in the ldap server. The default value of this attribute is true.

If you want to hide users in the Corporate Directory, set in a first step the `psIncludeInGAB` attribute to false for these users.

Next, the corporate directory search filter needs to exclude these users with their `psIncludeInGAB` attribute set to false. Changing the search filter is documented [here](#) but an example of this can be the following :

```
iwcadadmin -W /location/mypasswordfile -o
ab.corpdir.[default].searchfilter -v
"(&(&(&([filter])|(objectClass=GROUPOFUNIQUENAMES)(objectClass=GROUPOFURLS
\\
(objectClass=ICSCALENDARRESOURCE)
(objectClass=INETORGPERSO))) (objectClass=*))(!(psIncludeInGAB=false)))"
```

How do I remove personal address books of deleted users?

See: [How Do You Remove the Personal Address Books of Deleted Users?](#)

What does Convergence do with personal address book contacts that have been deleted by the end user?

If a contact has been deleted by the end user, Convergence determines what to do with that information based on how you set the `ab.pstore.deleteperm` configuration parameter. If you set the parameter to `true`, the contact is deleted from the user's personal address book entries on Directory Server. If, however, you set `ab.ps.deleteperm` to `false`, the following attribute/value pair is added to the deleted contact in Directory Server:

```
delete: true
```

The contact no longer displays in the Convergence UI as if it were permanently deleted from the Directory Server.

This task can be particularly useful when you are synchronizing deleted contact entries in Microsoft Outlook and Convergence when using Connector for Microsoft Outlook.

Single Sign-on

- [How do I configure Convergence for trusted circle SSO?](#)
- [How do I configure Convergence for Single Sign-Off?](#)
- [How do I write custom SSO module for convergence?](#)

How do I configure Convergence for trusted circle SSO?

To configure Convergence to use Trusted Circle SSO, you must enable the `sso.ms.enable` configuration parameter.

```
iwcadmin -o sso.ms.enable -v true
```

How do I configure Convergence for Single Sign-Off?

Enabling SSO, by default enables Single Sign-Off. If you have configured Convergence for Access Manager SSO, execute these commands to enable Single Sign-Off:

```
iwcadmin -o sso.enablesignoff -v true
iwcadmin -o sso.notifyserviceimpl -v
com.sun.comms.client.security.sso.impl.AMSSOTokenListener
```

If you have configured Convergence for Messaging SSO, type the following command to enable Single Sign-Off:

```
iwcadmin -o sso.enablesignoff -v true
```



Note

As of Communications Suite 7 Update 1, support for Access Manager has been deprecated. See: [Deprecated Support of Access Manager and Sun OpenSSO](#).

How do I write custom SSO module for convergence?

See [Writing a Pluggable SSO Module for Convergence](#) .

LDAP Service

- [How do I configure LDAP failover for Convergence?](#)
- [How do I change the Convergence display name to map to the LDAP `displayName`?](#)

How do I configure LDAP failover for Convergence?

To configure Convergence for LDAP failover, type the following command:

```
iwcadmin -o ugldap.host -v ldap1:port1,ldap2:port2
```

`ldap1:port1` and `ldap2:port2` are the LDAP servers that are a part of the failover.

If your LDAP hosts are configured for SSL, all the failover LDAP servers in the failover mechanism are also in SSL mode. Each host does not have a separate SSL flag. All the LDAP servers should have the same privileged `userid` and `password`. All the LDAP servers should run in Master-Master replication mode.

How do I change the Convergence display name to map to the LDAP `displayName`?

See: [Administering Convergence Display Name to Map to LDAP `displayName`](#).

Configuration Management

- [How do I configure Convergence to use SSL for configuration management?](#)
- [How do I change Convergence administrator user password?](#)

How do I configure Convergence to use SSL for configuration management?

To configure Convergence for SSL, you must first configure the Convergence server to accept SSL requests. Additionally, you must also configure the client utility: the `iwcadmin` command to communicate to the Convergence server in SSL mode.

To configure Convergence server administration for SSL:

1. Enable SSL by using the `iwcadmin` command.

```
iwcadmin -o admin.enablessl -v true
```

2. Generate keystore and truststore using `keytool`.
3. Set the keystore password.

```
iwcadmin -o admin.keystorepwd -v password
```

4. Copy keystore to the configuration and data files directory. The default location of this directory is `/var/opt/sun/comms/iwc/`
5. Restart Application Server for Convergence 1.x (or GlassFish Server starting with Convergence 2 and later).

The following log message appears indicates that the SSL configuration is a successful:

```
RMI connector server in SSL mode started successfully.
```

Set up the client to securely connect to Convergence. To do this, modify the following parameters in the `iwadmin.properties` file. This file is available in the configuration and data files directory. The default path is: `/var/opt/sun/comms/iwc`.

1. Set the parameter `secure` to `true`. Optionally, you can use the `-s` option in the `iwadmin` command.
2. Set the `truststorepath` parameter to the directory where you stored the truststore generated in the Step 2 in the above procedure.
3. Set the password to `truststorepasswd= <truststorepassword>`

How do I change Convergence administrator user password?

To change the Convergence administrator password, type the following command.

```
iwadmin -o admin.adminpwd -v <newpassword>
```

Deployment Specific Customizable Client Options for Convergence

- [How do I customize the Login page based on the domain name in the URL to access the Convergence client?](#)
- [How do I set the auto logout time?](#)
- [How do I remove the option to compose messages using Rich Text Formatting?](#)

How do I customize the Login page based on the domain name in the URL to access the Convergence client?

Convergence enables you to configure multiple domains in a deployment. Users can login to a domain by typing the URL and suffix the domain name to the user name. For example, `user1@siroe.com`. On successful authentication, the domain information is extracted from the login name and the user is logged into the specific domain.

Convergence provides an alternative way for users to log in to a specific domain. For example, you can configure Convergence to display a customized login page based on the domain information. The Convergence server displays the login page by extracting the domain name from the URL and determining if it contains a known domain and presents the domain specific login screen for the domain. The user can then type the user name and password and login to the domain. Note that in this case the user will not have to suffix the domain name to the user name.

Consider an example where `siroe.com` is a configured domain for a Convergence deployment. When users access Convergence by typing the URL `http://webmail.siroe.com/`, the server presents a customized login page for the domain `siroe.com`. Convergence server determines this based on the value of the `client.{domain-name}.loginpage` property. To set a customized login page for a domain, set the `client.{domain-name}.loginpage` configuration property by typing the following command.

```
# iwadmin -o client.{siroe.com}.loginpage -v  
"/iwc_static/layout/loginpage_siroe.html"
```

How do I set the auto logout time?

Convergence enables you to set a time in minutes to automatically log out of the application in case of user inactivity in client and also when the user closes the application without logging out. By default, the time is set to zero and is disabled. To set a time and enable the automatic logout option, set the `client.autologouttime` configuration property by typing the following command.

```
# iwadmin -o client.autologouttime -v <logouttime>
```



Note

Convergence 1.x patch 13 or greater is required for the automatic logout feature to work.

How do I remove the option to compose messages using Rich Text Formatting?

Convergence enables you to remove the Rich Text Formatting option for composing messages. To do so, set the `client.enablertfcompose` configuration property to `false`. By default, this parameter is set to `true`. For example:

```
# iwadmin -o client.enablertfcompose -v false
```

See: [Deployment Specific Customizable Client Options for the Convergence Interface Reference](#).

Instant Messaging

- [How Do I Configure Multiple Domains for Instant Messaging?](#)
- [How Do I Configure Convergence so that Presence Information is Shown in my Email?](#)

How Do I Configure Multiple Domains for Instant Messaging?

After creating a new non default domain (by using the Delegated Administrator GUI for example), you need to perform the following steps to enable Instant Messaging for users in a new domain:

In this example the user or group base is `dc=example,dc=com`. The new domain is called `Hosted Domain` and it has a DNS domain name of `other.hosteddomain.com`.

1. Run the Instant Messaging `imadmin assign_services` utility.

```
cd /opt/sun/comms/im/sbin/  
bash-3.00# ./imadmin assign_services  
Please enter base DN: o=Hosted Domain,dc=aus,dc=example,dc=com
```

2. Edit the Convergence `httpbind.conf` file to include both default domain and hosted domains to the `default.domains` attribute, for example:

```
default.domains=example.com, other.hosteddomain.com
```

You should then be able to log in to Convergence as `user@hosteddomain`. The default domain user can log in with just the UID.

For more information on hosted domain support in Instant Messaging, see [Configuring Hosted Domain Support](#).

How Do I Configure Convergence so that Presence Information is Shown in my Email?

- [Configuring Convergence with Instant Messaging 8](#)
- [Configuring Convergence with Instant Messaging 9](#)

Configuring Convergence with Instant Messaging 8

To enable Convergence to show presence information in email, you must edit the `iim.conf` file. The `iim.conf` file is available at `im-svr-base/config/iim.conf`

1. Add the following lines in the `iim.conf` file.

```
iim_server.roster.extra = "true"
iim_server.roster.extra.attributes.mail = "mailalternateaddress,
mail"
iim_ldap.user.attributes = "mailalternateaddress, mail"
```

2. Restart the Instant Messaging server.

```
# im_svr_base/sbin/imadmin stop
# im_svr_base/sbin/imadmin start
```

Configuring Convergence with Instant Messaging 9

To enable Convergence to show presence information in email, use the `imconfutil` command to modify the `iim.conf.xml` file. The `iim.conf.xml` file is available at `im-svr-base/config/iim.conf.xml`

1. Run `imconfutil` to set the following properties in the `iim.conf.xml` file.

```
imconfutil set-prop -u -c /opt/sun/comms/im/config/iim.conf.xml
iim_server.roster.extra=true iim_ldap.user.attributes=mail
```



Note

Beginning with Instant Messaging 9 Patch 1, `mailalternateaddress`, `mailequivalentaddress`, and `mail` are default Instant Messaging presence statuses for `iim_server.roster.extra.attributes.mail`.

2. Restart the Instant Messaging server.

```
# im_svr_base/sbin/imadmin stop
# im_svr_base/sbin/imadmin start
```

Enabling Anti-Spam

**Note**

If you are using Sun Convergence 1 Update 2, perform the steps documented in the section [I'm using Convergence 1 Update 2. How do I Enable the Anti-Spam feature?](#)

How do I Enable the Anti-Spam feature?

You can configure Convergence to take action against spam messages in the following ways:

- By setting the anti-spam related parameters in Convergence
- By integrating a spam filter in Messaging Server in addition to setting the anti-spam related parameters in Convergence

Configuring Convergence for Anti-Spam Action

Set the following parameters in Convergence:

- `mail.spam.enableaction`: Set this parameter to `true` to enable the anti-spam functionality. Setting this parameter will enable users to take action against spam messages.

```
# iwadmin -o mail.spam.enableaction -v true
```

- `mail.spam.folder`: Set this parameter to the folder name into which spam messages should be moved.

```
# iwadmin -o mail.spam.folder -v SpamFolder
```

**Note**

You must restart Application Server for Convergence 1.x (or GlassFish Server starting with Convergence 2 and later) after making the configuration changes.

When you set the above parameters, the following spam related functionality will be available in the Convergence client:

- A system folder is made available as the designated spam folder. This is based on the value set for the `mail.spam.folder` parameter assigned by the administrator.
- Users will be able to mark messages as spam or not spam. Messages marked as spam are moved into the designated spam folder and messages that are marked as not spam are moved into the Inbox.

Configuring Messaging Server in Addition to Configuring Convergence for Anti-Spam Action

A more effective way to counter spam messages is to deploy a spam filter at the back-end Messaging Server in addition to enabling the anti-spam functionality in Convergence. For information on how to integrate a spam filter with the Messaging Server, see [Integrating Spam and Virus Filtering Programs Into Messaging Server](#).

After integrating the spam filter, set the value of the `service.feedback.spam` parameter in Messaging Server to the email address at which spam reports are accepted.

```
configutil -o service.feedback.spam -v <email_address>
```

When you set this parameter, the following spam related functionality will be available to the Convergence client.

- Users will be able to mark messages as spam. When users mark a message as spam, the message is flagged in the message store, and forwarded to the email address set for the `service.feedback.spam` configuration utility option. The spam messages are marked in the message list and displayed with a warning in the message viewer.
- Users will be able to mark messages incorrectly identified as spam, as not spam. When the user marks incorrectly identified spam messages as not spam, the flag is removed from the message in the message store.

If Messaging Server is configured with a spam filter that accepts reports of messages that are incorrectly identified as spam, set the value of the parameter `service.feedback.notspam` to the email address at which Convergence will forward the messages marked as not a spam.

```
configutil -o service.feedback.notspam -v <email_address>
```

**Note**

You must restart Messaging Server after making these configuration changes.

Set the the anti-spam related parameters in Convergence. See [Configuring Convergence for Anti-Spam Action](#).

I'm using Convergence 1 Update 2. How do I Enable the Anti-Spam feature?

**Note**

The feature documented in this section is applicable for Convergence 1 Update 2 release.

To use the spam feature in the Convergence client, you must deploy a spam filter in the backend Messaging Server. For information on how to integrate a spam filter with the Messaging Server, see [Integrating Spam and Virus Filtering Programs Into Messaging Server](#).

To enable marking of spam messages in the Convergence client, set the value of the `service.feedback.spam` parameter in Messaging Server to the email address at which the spam filter accepts spam reports.

```
configutil -o service.feedback.spam -v <email_address>
```

When you set this parameter, the following spam related functionality will be available to the Convergence client.

- Users will be able to mark messages as spam. When users mark a message as spam, the message is flagged in the message store, and forwarded to the spam filter. The spam messages are marked in the message list and displayed with a warning in the message viewer.
- Users will be able to mark messages incorrectly identified as spam as not spam. When the user marks incorrectly identified spam messages as not spam, the flag is removed from the message in the message store.

If Messaging Server is configured with a spam filter that accepts reports of messages that are incorrectly identified as spam, set the value of the parameter `service.feedback.notspam` to the email address at which the spam filter accepts such reports.


```
configutil -o service.feedback.notspam -v <email_address>
```

When you set the `service.feedback.notspam` parameter, in addition to the functionality described above, the Convergence client also forwards the messages that should not be flagged as spam to the spam filter.



Note

You must restart Messaging Server after making these configuration changes.

Enabling Indexing and Search Service

[Indexing and Search Service](#) (ISS) is a general-purpose indexing and searching server. Convergence can be configured to use the indexing and search capabilities of ISS.

To configure Indexing and Search Service with Convergence, you must have the ISS server installed and configured. To know more about how to do this, see [Indexing and Search Service Documentation](#).

To enable Convergence to work with ISS, perform the following steps:

1. Enable the following ISS related parameters in Convergence:
 - `ISS.enable` - Set this parameter to `true` to enable the search service.

```
# iwadmin -o ISS.enable -v true
```

- `ISS.host` - Set this parameter to the hostname on which the ISS server installed.

```
# iwadmin -o ISS.host -v siroe.com
```

- `ISS.port` - Set this parameter to the web component port number on which ISS is deployed. This should be the same as the port number for `appserver.web.port` in the ISS configuration file: `jiss.conf`.

```
# iwadmin -o ISS.port -v <port_number>
```



Note

If you want a secure connection between Convergence and ISS, set the `ISS.enablenessl` parameter to `true`. Correspondingly, you must also set the port number (`ISS.port`) to the SSL port number.

```
# iwadmin -o ISS.enablenessl -v true
```



Note

Beginning with Convergence 2, set the following parameters:

- `ISS.proxyadminid` - Set this parameter to the proxy admin ID for ISS. This should be the same as the Store Admin Username specified during ISS configuration (the value of `mail.imap.admin.username` in the `jiss.conf` file).

```
# iwcaadmin -o ISS.proxyadminid -v <proxy_adminid>
```

- `ISS.proxyadminpwd` - Set this parameter to the proxy admin password for ISS. This should be same as the password specified for the Store Admin during ISS configuration.

```
# iwcaadmin -o ISS.proxyadminpwd -v <proxy_adminpwd>
```



Note

To enable attachment search, `mail.proxyseparator` in `jiss.conf` should be set to `;` (semicolon), which is the default setting.

2. Restart GlassFish Server.

Deploying Convergence and Index and Search Service on the Same Instance of Application Server

If Convergence and ISS are deployed on the same instance of application server, the application server becomes unresponsive when users switch between the Attachments folder and Inbox.

To fix this, perform the following steps:

1. Set number of request processing threads to double the number of CPUs in the system. This can be done by setting the `server.http-service.request-processing.thread-count` parameter in application server using the `asadmin` command. Here is an example:

```
# asadmin set  
server.http-service.request-processing.thread-count=8
```

2. Restart GlassFish Server.

Enabling CalDAV Service

To configure CalDAV Service with Convergence, you must have the CalDAV server installed and configured.

To enable Convergence to work with CalDAV, perform the following steps:

1. Enable the following CalDAV related parameters in Convergence:
 - `caldav.enable` - Set this parameter to `true` to enable the search service.

```
# iwcaadmin -o caldav.enable -v true
```

- `caldav.host` - Set this parameter to the hostname on which the CalDAV server installed.

```
# iwcaadmin -o caldav.host -v siroe.com
```

- `caldav.port` - Set this parameter to the web component port number on which CalDAV is deployed. This should be same as the port number specified for `Server Instance HTTP Port` in the Application Server Configuration Details panel during the Calendar Server 7

Initial Configuration.

```
# iwcaadmin -o caldav.port -v <port_number>
```

- `caldav.proxyadminid` - Set this parameter to the proxy admin id on which CalDAV is deployed. This should be same as the Administrator User Id specified during Calendar Server 7 Initial Configuration.

```
# iwcaadmin -o caldav.proxyadminid -v <proxy_adminid>
```

- `caldav.proxyadminpwd` - Set this parameter to the proxy admin password on which CalDAV is deployed. This should be same as the Administrator password specified during Calendar Server 7 Initial Configuration.

```
# iwcaadmin -o caldav.proxyadminpwd -v <proxy_adminpwd>
```

- `caldav.serviceuri` - Set this parameter to the serviceuri on which CalDAV is deployed. This should be same as the URI Path where the Calendar Server 7 is deployed and should be suffixed with `/wcap`. For example, if the URI path where Calendar Server 7 is deployed is `/caldav`, then this parameter should be set to `/caldav/wcap`.

```
# iwcaadmin -o caldav.serviceuri -v <service_uri>
```



Note

Convergence can be configured to enable calendar service using both CS 6.x and CalDAV backend servers and it is called co-existence mode. In this mode of configuration some users may be using CS 6.x server and others might have been migrated to CalDAV server.

You need to set the `caldav.davuserattr` parameter to an LDAP attribute used in the user entry to indicate that the user has been migrated to CalDAV. The default value of this attribute is `davStore` (defined as part of `davEntity` ObjectClass). If this attribute is not present in user LDAP entry then it indicates that you are a CS 6.x user and not a CalDAV user.

```
# iwcaadmin -o caldav.davuserattr -v <userattr>
```

2. Restart Application Server for Convergence 1.x (or GlassFish Server starting with Convergence 2).

Enabling SMS Calendar Notifications in Convergence

See [How Do I Turn on SMS Notifications for Calendar Event Reminders in Convergence?](#)

Miscellaneous

- [How to enable Communications Express Compatibility for Mail Filters?](#)
- [How do I verify passwords in Convergence?](#)
- [I do not want to manage Convergence using the `cn=Directory Manager` user. How do I create a Directory Server user in LDAP with the required privileges to manage a Convergence Installation?](#)
- [How do I configure VLV \(Virtual List View\) browsing indexes for Directory Server?](#)

- [How Do I Handle Invalid Session Redirects in Convergence?](#)
- [How Do I Add Comments to JSON Configuration Files?](#)

How to enable Communications Express Compatibility for Mail Filters?

If you want your deployment to coexist with Convergence and Communications Express, you must enable the compatibility for sieve. Communications Express sends raw sieve filters to the server. The server then parses the sieve filters and stores them in LDAP. In cases where Convergence and Communications Express coexist, you must enable the `mail.uwcsievecompatible` configuration parameter so that sieve filters are managed appropriately.

```
iwcadmin -o mail.uwcsievecompatible -v true
```



Note

The storage mechanism and data format to store sieve rules for Convergence and Communications Express is the same. The sieve rules are stored in the `mailSieveRuleSource` LDAP attribute in the user's LDAP. This format is in compliance with [RFC 3028](#) (base Sieve specification) format and not with XML. Communications Express requires metadata for sieve rules, such as `rule name`, `priority`, `enable/disable` to manage sieve filters. This meta data is not a part of RFC 3028. The data is stored in the form of sieve comments. The `mail.uwcsievecompatible` configuration parameter determines whether Convergence should use the metadata to create or manage the sieve rules that are compatible with Communications Express.

The following example shows how the sieve filter appears when stored in the LDAP:

```
#RULE: $Name="Modified name" $Order=2 $Type="DEFAULT_TYPE"
require "fileinto";
#BEGINFILTER
if anyof (
header :contains
[ "From", "Sender", "Resent-from", "Resent-sender", "Return-path" ] "JohnDoe"
){
fileinto "Inbox";
stop;
}
#ENDFILTER
```

How do I verify passwords in Convergence?

Convergence allows you to verify the administration passwords. Convergence stores all passwords in encrypted format during configuration. You can verify if the password you have set while configuring Convergence is correct by using the `EncryptPwd` utility. The utility takes the password that you want to verify, as the input, and provides an encrypted string. To verify the password, you must compare this encrypted string with the encrypted password string stored in the Convergence configuration file.

To verify a password:

1. Type the following command from the command-line prompt.

```
java -cp /var/opt/sun/comms/iwc/WEB-INF/lib/iwc-shared-util.jar
com.sun.comms.shared.util.EncryptPwd
```

You will be prompted to provide the encryption key.

Note

In the above command, `/var/opt/sun/comms/iwc/WEB-INF` refers to the default deploy directory to which Convergence is deployed.

2. Type the encryption key. By default the encryption key is available in the file:
`/var/opt/sun/comms/iwc/config/.ngc_enc`.

```
Enter the encryption key ( To generate a new key press Enter ):
```

You will be prompted to enter a string to encrypt.

3. Type the password that you guess is the right password.
Here is an example.

```
Enter string to encrypt: admin123
```

The password you guess is encrypted and displayed at the prompt.

```
admin123 ---> rE9Zlq6H0r49RgsQrKHxsw==
```

4. Compare the encrypted password (`rE9Zlq6H0r49RgsQrKHxsw==`) with the encrypted password available in the configuration file to verify if the password you provided is correct. If the encrypted password strings match, the password you guessed is correct.
5. If the encrypted password strings do not match you can provide another string, or type `quit` to exit.

```
Enter string to encrypt: quit
Bye...
```

I do not want to manage Convergence using the `cn=Directory Manager` user. How do I create a Directory Server user in LDAP with the required privileges to manage a Convergence Installation?

A user must have a minimum set of LDAP privileges to manage the LDAP tasks for a Convergence deployment. Instead of using `cn=Directory Manager`, create an administrator user with a set of privileges that can enable him to manage a Convergence installation. The following privileges must be available for the user:

- Read
- Write
- Search
- Add
- Delete
- Update

The following LDIF file contains the ACIs assignments for Schema 1 for a user named convergenceAdminUser.

```
# Sample for Schema 1
# Adding ACIs to DC Tree
dn: o=internet
changetype: modify
add: aci
aci: (targetattr="*") (version 3.0; acl "foo"; allow (read,search)
userdn="ldap:///uid=convergenceAdminUser, ou=people,
o=siroe.sun.com,dc=siroe,dc=sun,dc=com";)

# Adding ACIs to Organization Tree
dn: dc=siroe,dc=sun,dc=com
changetype: modify
add: aci
aci: (targetattr="*") (version 3.0; acl "foo"; allow (all)
userdn="ldap:///uid=convergenceAdminUser, ou=people,
o=siroe.sun.com,dc=siroe,dc=sun,dc=com";)

# Adding ACIs to Address Book BaseDN
dn: o=PiServerDb
changetype: modify
add: aci
aci: (targetattr="*") (version 3.0; acl "foo"; allow (all)
userdn="ldap:///uid=convergenceAdminUser, ou=people,
o=siroe.sun.com,dc=siroe,dc=sun,dc=com";)
```

The following LDIF file contains the ACIs assignments for Schema 2 for a user named convergenceAdminUser:

```
# Sample for Schema 2
# Adding ACIs to Organization Tree
dn: dc=siroe,dc=sun,dc=com
changetype: modify
add: aci
aci: (targetattr="*") (version 3.0; acl "foo"; allow (all)
userdn="ldap:///uid=convergenceAdminUser, ou=people,
o=siroe.sun.com,dc=siroe,dc=sun,dc=com";)

# Adding ACIs to Address Book BaseDN
dn: o=PiServerDb
changetype: modify
add: aci
aci: (targetattr="*") (version 3.0; acl "foo"; allow (all)
userdn="ldap:///uid=convergenceAdminUser, ou=people,
o=siroe.sun.com,dc=siroe,dc=sun,dc=com";)
```

Using the LDAP modify command, create the user:

```
# ldapmodify -h <hostname> -p <portname> -D "cn=Directory Manager" -w
password -f add_acis.ldif

modifying entry o=internet

modifying entry o=usergroup

modifying entry o=PiServerDb
```

Additionally, you must also set the `ugldap.binddn` and `ugldap.bindpwd` parameters in Convergence to reflect the user credentials:

```
# iwcadmin -o ugldap.binddn -v uid=convergenceAdminUser, ou=people,
o=siroe.com,o=usergroup

# iwcadmin -o ugldap.bindpwd -v <ugldap_bindpassword>
```

How do I configure VLV (Virtual List View) browsing indexes for Directory Server?

Directory Server provides a mechanism to create indexes. These indexes improve the turnaround time at the time of searching for entries in the directory server instance. You must set the following parameters to enable VLV indexes in Directory Server.

- `search_base`
- `vlv_search_filter`
- `vlv_sort_attribute`
- `vlv_scope`



Note

If you have multiple Directory Server backends that store user group information, you must create the indexes on all the instances.

Before setting the VLV Browsing indexes, you must have information about the directory server settings. The directory server settings are available in the `dse.ldif` file under the `<directory_server_root>/config` directory. Specifically, you would need the value of the `cn` attribute. The following is an example of the `dse.ldif` file:

```

dn: cn=isp,cn=ldbm database,cn=plugins,cn=config

objectClass: top
objectClass: extensibleObject
objectClass: nsBackendInstance
cn: isp
creatorsName: cn=directory manager
modifiersName: cn=directory manager
entrydn: cn=isp,cn=ldbm database,cn=plugins,cn=config
numSubordinates: 4
nsslapd-suffix: o=isp
nsslapd-cachesize: -1
nsslapd-cachememsize: 10485760
nsslapd-readonly: off
nsslapd-require-index: off
nsslapd-directory: /var/opt/SUNWdsee/dsins1/db/isp

```

Applying the VLV Browsing Index Settings

Use the `ldapmodify` command to specify the Directory Server browsing search indexes. The following is an example:

```

# ldapmodify -h directory.aus.sun.com -p 389 -D "cn=Directory Manager"
dn: cn=Browsing isp,cn=isp,cn=ldbm database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvSearch
cn: Browsing isp
vlvbase: o=aus.sun.com,o=isp
vlvscope: 2
vlvfilter: (&(mail=*)(cn=*))
aci: (targetattr="*)(version 3.0; acl "VLV for Anonymous";
allow (read,search,compare) userdn="ldap:///anyone";)

dn: cn=Sort by cn,cn=Browsing isp,cn=isp,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Sort by cn
vlvSort: cn

```

Generate the Indexes

In the previous section, we provided the information about the search indexes that we want to create for your search base. For the settings to take effect, the indexes must be generated. It is recommended that these steps should be performed during during a scheduled change window. This is because the Directory Server needs to be restarted.

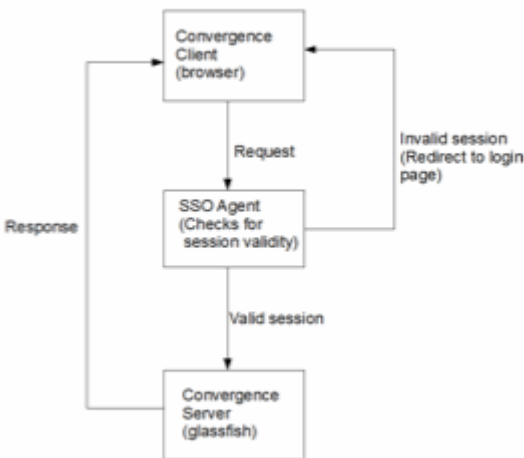
The following commands describes the steps to create the indexes:

1. Change directory to the directory server installation.
`cd /opt/SUNWdsee/ds6/bin`

2. Stop the directory server instance.
`./dsadm stop /var/opt/SUNWdsee/dsins1/`
3. Populate the index entries by using the `dsadm reindex` command. The `reindex` option requires you to provide the `vlv_sort_attribute`, the path to the directory server instance, and the value of the user group base.
`./dsadm reindex -l -t "Sort by cn" /var/opt/SUNWdsee/dsins1/ "o=isp"`
4. Start the directory server instance.
`./dsadm start /var/opt/SUNWdsee/dsins1/`

How Do I Handle Invalid Session Redirects in Convergence?

The Convergence client sends AJAX requests to communicate with the server. If these requests are redirected for any reason, you must take special care with the redirects. With AJAX requests, redirects are automatically handled by the browser. The contents of the redirected page are handed over as the AJAX response. But, when you look at the response headers, you cannot determine if the request was successful or if the request was redirected. If the request is redirected, then the application may not understand the response. As a result, you must configure Convergence to understand the contents of a redirected page.



When there is a security agent in between the Convergence client and server, problems occur when the agent intercepts every request while looking for a valid session. If the session is invalid, the request is redirected to a login page configured in security agent. Because Convergence does not understand the contents of the login page, it displays a response parsing error, such as a syntax error. To get around this problem, the security agent should redirect to a page that Convergence is able to understand, instead of redirecting to a custom login page.

Convergence expects session time out error messages to be in specific format. When the agent encounters session time out, it needs to redirect the request to a page that generates this error message instead of its login page. Sample error messages are provided in [Table: Requests that are Redirected, URL Patterns, and Error Responses](#) and can be copied to the policy agents deployment location.

Convergence uses different protocols for each service. For Mail: the `wmap` protocol, for Calendar: the `wcap` protocol, for Address book: `wabp` protocol, and for Options: the `iwcp` protocol.

The agent should be configured to differentiate between the kinds of requests it receives and correspondingly send the error response specific to that service.

For example, if the agent receives `/iwc/svc/wmap/*` request, the error response should be as mentioned in `$Convergence_Deployment_Directory/jsp/samplefiles/MailServiceErrorJSON.jsp`.

The following table lists the requests that are redirected, the URL patterns, and appropriate error responses:

Note
The error responses come from sample files in the `$Convergence_Deployment_Directory/jsp/samplefiles` directory that, at this time, can only be found in the Convergence 1.x product. If you have access to the Convergence 1.x product, you can use those sample files with Convergence 2 and later. If you don't have access to the Convergence 1.x error response sample files, contact Oracle Support.

Once you have the sample JSP files, move them to your docroot directory. Decode the redirect by determining if it is a mail, calendar, address book, or Convergence server request. Redirect the URL to the corresponding JSP page. Within each JSP page, set the URL location.

Note
In each sample file, replace any occurrence of `http://host.domain.com/loginpage` with the URL of the application login page to which the user has to be redirected to login to the application.

Table: Requests that are Redirected, URL Patterns, and Error Responses

Service Request	URL Pattern	Redirect to File
Mail	<code>/iwc/svc/wmap/*</code>	<code>MailServiceErrorJSON.jsp</code>
Calendar	<code>/iwc/svc/wcap/*</code>	<code>CalServiceErrorJSON.jsp</code>
Address Book	<code>/iwc/svc/wabp/*</code>	If the expected response type is JSON: <code>AddressBookErrorJSON.jsp</code> ; If the expected response type is XML: <code>AddressBookErrorXML.jsp</code>
Options	<code>/iwc/svc/iwcp/</code>	<code>IwcProtocolErrorJSON.jsp</code>

How Do I Add Comments to JSON Configuration Files?

While comments are not supported in JSON files, there are a couple of exceptions to these standards to make the files more user-friendly:

1. Only single line comments are supported (with `//`).
2. Comments either should start from beginning of the line or should prefix with WHITESPACE or TAB or COMMA characters.

Chapter 4. Configuring Convergence to Use Proxy Authentication

This information describes how to enable Proxy Authentication in Convergence. The proxy authentication mechanism uses various components that Convergence depends on. You must have thorough knowledge of the following products and technologies:

- Convergence administration
- Directory Server administration
- Knowledge of Communications Suite Schemas

Proxy authentication is performed by using the credentials of a more privileged user on behalf of a normal user. The `username` and `password` of the privileged user requesting the authentication is sent with the username of the user requesting the authentication.

The parameters include:

- `username` - The username of the privileged user.
- `password` - The password of the privileged user.
- `proxyauth` - The username of the user for whom authentication is requested

The protocol request must pass the above parameters for performing authentication.

Configuring Convergence for Proxy Authentication

For proxy authentication to work, the privileged user (Proxy Admin user) must be provisioned for the domain. A user is considered a proxy admin user if the LDAP entry has `isMemberOf` operational attribute, whose value is set to the DN of `Service Administrators`. The admin user must be a member of the `Service Administrators` group in the DC tree.

For example:

```
cn=Service Administrators, ou=Groups, <DC-ROOT>
```

The `Service Administrators` group and the admin user are provisioned when the administrators for Messaging Server (`admin`) and Calendar Server (`calmaster`) are configured. This admin user can also be used for Convergence proxy authentication.

To configure proxy authentication in Convergence, enable proxy authentication by setting the `auth.ldap.enableproxyauth` configuration parameter.

For example:

```
# iwadmin -u admin -o auth.ldap.enableproxyauth -v true
```



Note

Convergence does not provision an administrator user.

Proxy Authentication Request

Convergence requires the following parameters for performing proxy authentication based on a specific format that is applicable to the `login.iwc` or `login.wabp` commands.

For example:

```
http://<hostname>:<port>/iwc/login.iwc?username=<username_privileged_user>&pas
```

Where the values for:

- `username` is the username of the privileged user: `<username_privileged_user>`.
- `password` is the password of the privileged user: `<password_privileged_user>`.
- `proxyauth` is the username of the user for whom authentication is requested: `<username>`.
- `fmt-out=text/json` specifies the JSON output. XML output is no longer valid.

Chapter 5. Configuring Convergence With Sun OpenSSO Enterprise 8.0 for Authentication and SSO

Configuring Convergence With OpenSSO Enterprise 8.0 for Authentication and SSO

Support for this Feature has been Deprecated

OpenSSO can only be used with Convergence 2.x and earlier. For details, refer to [Deprecated Features in Communications Suite](#).

This article describes the steps to configure OpenSSO Enterprise 8.0 with Convergence. Convergence supports OpenSSO Enterprise 8.0 starting Sun Convergence 1 Update 2 release.

Prerequisites:

- You must have Sun OpenSSO Enterprise 8.0 installed and configured. For more information, see [Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide](#).
- Convergence must be installed and configured (minimum version Sun Convergence 1 Update 2).

Configuring OpenSSO Enterprise 8 with Convergence

Configuring OpenSSO with Convergence involves configuration for both OpenSSO and Convergence.

Configuring OpenSSO

To configure OpenSSO with Convergence, enable cookie encoding and set up a Realm.

Enabling Cookie Encoding

To enable cookie encoding, perform the following steps:

1. Log in to OpenSSO console as user `amAdmin`.
2. Click Configuration -> Server and Sites.
3. Click the link corresponding to the server on which OpenSSO is deployed.
4. Click Security -> Cookie. By default the cookie encoding is set to No.
5. Click the Inheritance Settings button.
6. Deselect Encode Cookie Value.
7. Click Save.
You can now change the cookie encoding option.
8. Set the value of Cookie Encoding Value to Yes. See step 4.
9. Click Save to save your changes.
10. Restart the application server on which OpenSSO is deployed.

Setting Up the Realm

**Note**

To set up an authentication realm in OpenSSO, you should also read the following example: [Convergence Configuration Example - Creating an Authentication Realm in Access Manager](#) in addition to reading this section.

You must set up a Realm in OpenSSO to enable authentication. To do this, you must perform the following steps:

1. Create a Realm.
To learn more about how to create Realms in OpenSSO, see [Chapter 2 Managing Realms](#) in the [Sun OpenSSO Enterprise 8.0 Administration Guide](#).
2. Create a Data Store. The type of the Data Store must be "Sun DS with OpenSSO Schema".
To learn more about how to create Data Stores in OpenSSO, see [Chapter 3 Data Stores](#) in the [Sun OpenSSO Enterprise 8.0 Administration Guide](#).
3. Configure the realm for OpenSSO Enterprise authentication service. The LDAP service must be configured and the criteria must be set to `REQUIRED`.
To learn more about configuring the authentication service, see [Chapter 4 Managing Authentication](#) in the [Sun OpenSSO Enterprise 8.0 Administration Guide](#).

Configuring Convergence

To configure Convergence, perform the following steps:

1. Copy the `AMConfig.properties.template` as `AMConfig.properties`. By default, this exists in the `/opt/sun/comms/iwc/config` directory.

```
cp AMConfig.properties.template AMConfig.properties
```

2. Edit the `AMConfig.properties` file and set the following properties:

```
com.iplanet.am.naming.url=http://<your_host_name>:<portnumber>/opensso
```

Enabling OpenSSO Authentication

To use OpenSSO as the authentication provider for Convergence, perform the following steps:

1. Set the value of the `auth.opensso.enable` parameter to `true`.

```
iwcadmin -u <adminuserid> -o auth.opensso.enable -v true
```

2. Set the value of the `auth.opensso.cookieDomain` parameter to the domain on which Convergence is deployed.

```
iwcadmin -u <adminuserid> -o auth.opensso.cookieDomain -v  
<domain_name>
```

**Note**

You must restart the application server after making configuration changes.

Enabling OpenSSO Single SignOn in Convergence

To enable OpenSSO Single SignOn, you must set the `sso.opensso.enable` parameter to `true`.

```
iwadmin -u <adminuserid> -o sso.opensso.enable -v true
```



Note

You must restart the application server after making configuration changes.

Chapter 6. Administering SMIME in Convergence

Administering S/MIME in Convergence

Support for Secure/Multipurpose Internet Mail Extension (S/MIME) 3.1 is available in Convergence. Convergence users who are set up to use S/MIME can exchange signed or encrypted messages with other users of Convergence, Communications Express Mail, Microsoft Outlook Express, and Mozilla mail systems.

The Convergence online help instructs end users in how to configure and send encrypted mail.

The following pages describe how to administer S/MIME in Convergence:

- [What Is S/MIME?](#)
- [Software and Hardware Requirements for Convergence with S/MIME](#)
- [Certificate Requirements for Using S/MIME in Convergence](#)
- [Configuring Messaging Server to Use S/MIME in Convergence](#)
- [Securing Internet Links Between Messaging Server and Convergence With SSL](#)
- [Key Access Libraries for the Client Machines](#)
- [Verifying Private and Public Keys](#)
- [Granting Permission to Use S/MIME Features](#)
- [Managing Certificates for S/MIME](#)
- [Configuring and Sending Encrypted Mail: Instructions for Convergence End Users](#)



[Printable PDF Version for End Users](#)

The following pages provide S/MIME reference information:

- [smime.conf Parameters in Messaging Server](#)
- [S/MIME configutil Options in Messaging Server](#)



S/MIME in Communications Express Mail

S/MIME is also supported in another Communications Suite client: Sun Java System Communications Express. For more information, see [Administering S/MIME in Communications Express](#).

What Is SMIME?

What Is S/MIME?

Secure/Multipurpose Internet Mail Extensions (S/MIME) provides a consistent way for email users to send and receive secure MIME data, using digital signatures for authentication, message integrity and non-repudiation and encryption for privacy and data security. S/MIME version 3.1 (RFC 3851) is supported.

Several email clients support the S/MIME specification, including Microsoft Outlook Express and Mozilla mail.

You can deploy a secure mail solution by using Messaging Server and S/MIME. Convergence users who are set up to use S/MIME can exchange signed or encrypted messages with other users of Convergence, Microsoft Outlook Express, and Mozilla mail systems. A messaging proxy can provide an additional layer of security at the firewall to further protect information assets within Messaging Server.

The Convergence client supports S/MIME with these features:

- Create a digital signature for an outgoing mail message to assure the message's recipient that the message was not tampered with and is from the person who sent it
- Encrypt an outgoing mail message to prevent anyone from viewing, changing or otherwise using the message's content before the message arrives in the recipient's mailbox
- Verify the digital signature of an incoming signed message with a process involving a certificate revocation list (CRL)
- Automatically decrypt an incoming encrypted message so the recipient can read the message's contents
- Exchange signed or encrypted messages with other users of an S/MIME compliant client such as Convergence, Communications Express Mail, and Mozilla mail systems

The other pages in [Administering S/MIME in Convergence](#) describe how to configure Messaging Server and Convergence for S/MIME. Note that you do not have to exclusively use Convergence to be able to use S/MIME with Messaging Server.

Concepts You Need to Know

To properly administer S/MIME, you need to be familiar with the following concepts:

- Basic administrative procedures for your platform
- Structure and use of a lightweight directory access protocol (LDAP) directory
- Addition or modification of entries in an LDAP directory
- Configuration process for the Directory Server
- Concepts and purpose of the following:
 - Secure Socket Layer (SSL) for a secured communications line
 - Digitally signed email messages
 - Encrypted email messages
 - Local key store of a browser
 - Smart cards and the software and hardware to use them
 - Private-public key pairs and their certificates
 - Certificate authorities (CA)
 - Verifying keys and their certificates
 - Certificate revocation list (CRL). (See [When is a Certificate Checked Against a CRL?](#))

Software and Hardware Requirements for Convergence with SMIME

Software and Hardware Requirements for Convergence with S/MIME

This information describes the required hardware and software for using Convergence with S/MIME. Ensure that you install all the correct versions of the software on the server and client machines before attempting to configure for S/MIME.

Topics:

- [Standard Requirements to Support Convergence](#)
- [Required Hardware and Software to Support S/MIME on a Client Machine](#)

Standard Requirements to Support Convergence

Convergence Requirements

The product software required to support Convergence is described in [Requirements for Communications Suite](#).

Server Requirements

The following server software products are required for Convergence and S/MIME:

- Messaging Server
- Directory Server Enterprise Edition



To support S/MIME, you must configure and store certificate information in Messaging Server and Directory Server.

In a typical deployment, these products run on server machines separate from the clients on which Convergence is running.

For information about the requirements to support Messaging Server and Directory Server, see [Requirements for Communications Suite](#).

Required Hardware and Software to Support S/MIME on a Client Machine

In addition to the standard requirements to support Convergence on a client machine, the following hardware and software are required to support the S/MIME features in Convergence.

Component	Description
Operating system	Microsoft Windows XP, Windows Vista, or Windows 7
Browser	<p>Microsoft Internet Explorer (32-bit browser version): Version 7, Version 8, and Version 9 Firefox 7 on Windows XP (beginning with Convergence 2 Patch 3) Firefox 8 on Windows 7 (beginning with Convergence 2 Patch 3)</p> <div data-bbox="425 390 1390 567" style="background-color: #e6f2ff; padding: 10px;"> <p> Note Although S/MIME works with Firefox browsers, it uses certificates from the Windows Certificate Store (certificates stored in Internet Options). S/MIME does not read the certificates from the Firefox Certificate Store.</p> </div>
Oracle software	<p>Java Runtime Environment (JRE) 6 with latest critical patch update</p> <div data-bbox="425 642 1390 848" style="background-color: #e6f2ff; padding: 10px;"> <p> Note If you are enabling S/MIME, be sure to install the most recent Java plug-in patch, beginning with 1.6.0_29. For more details, see: http://www.oracle.com/technetwork/java/javase/6u29-relnotes-507960.html</p> </div>
Private-public keys with certificates	<p>One or more private-public key pair with certificates. Certificates are required and they must be in standard X.509 v3 format. Obtain keys and certificates from a CA for each Convergence user who will use the S/MIME features. The keys and their certificates are stored on the client machine or on a smart card. The public keys and certificates are also stored in an LDAP directory that can be accessed by Directory Server.</p> <p>A certificate revocation list (CRL), maintained by the CA, must be part of your system if you want key certificates checked against it to further ensure that the keys are valid. See When is a Certificate Checked Against a CRL?</p>
Smart card software (only required when keys and certificates are stored on smart cards)	ActivIdentity ActiveClient, Version 6.2, or Litronic NetSign 215 Reader CAC Compliant
Smart card reader	Any model of smart card reading device complying with ISO 7816 supported by the client machine and smart card software.

Certificate Requirements for Using SMIME in Convergence

Certificate Requirements for Using S/MIME in Convergence

The signature and encryption features are not immediately available to Convergence users after you install Messaging Server. Before a user can take advantage of S/MIME, the requirements described in this information must be met.

Topics:

- [Private and Public Keys](#)
- [Keys Stored on Smart Cards](#)
- [Keys Stored on the Client Machine](#)
- [Publish Public Keys in LDAP Directory](#)
- [Give Mail Users Permission to Use S/MIME](#)
- [Multi-language Support](#)
- [Wildcard SSL Certificates: Not Supported](#)

Private and Public Keys

At least one private and public key pair, including a certificate in standard X.509 v3 format, must be issued to each Convergence user who will use S/MIME. The certificate, used in a verification process, assures other mail users that the keys really belong to the person who uses them. A user can have more than one key pair and associated certificate.

Keys and their certificates are issued from within your organization or purchased from a third-party vendor. Regardless of how the keys and certificates are issued, the issuing organization is referred to as a certificate authority (CA).

Key pairs and their certificates are stored in two ways:

- On a smart card

These cards are similar to commercial credit cards and should be used and safeguarded by the mail user as they do their own credit cards. Smart cards require special card readers attached to the mail user's computer (client machine) to read the private key information. See [Keys Stored on Smart Cards](#) for more information.

- In a local key store on the mail user's computer (client machine)

A mail user's browser provides the key store. The browser also provides commands to download a key pair and certificate to the key store. See [Keys Stored on the Client Machine](#) for more information.

Keys Stored on Smart Cards

If the private-public key pair, with its certificate, is stored on a smart card, a card reader must be properly attached to the mail user's computer. The card reading device also requires software; the device and its software are supplied by the vendor from whom you purchase this equipment.

There are actually two parts to a system with card reading capabilities. One part is the hardware card reader and its driver. The second part is the actual card, which is usually provided by a different vendor and requires drivers for reading the cards. Not all cards are supported. Refer to [Required Hardware and Software to Support S/MIME on a Client Machine](#) to see a list of the supported SmartCards (ActiveCard, now renamed ActivIdentity, and NetSign).

When properly installed, a mail user inserts their smart card into the reading device when they want to create a digital signature for an outgoing message. After verification of their smart card password, the private key is accessible by Convergence to sign the message. See [Required Hardware and Software to Support S/MIME on a Client Machine](#) for information on supported smart cards and reading devices.

Libraries from the vendor of the smart card are required on the user's computer. See [Key Access Libraries for the Client Machines](#) for more information.

Keys Stored on the Client Machine

If key pairs and certificates are not stored on smart cards, they must be kept in a local key store on the mail user's computer (client machine). Their browser provides the key store and also has commands to download a key pair and certificate to the key store. The key store may be password-protected; this depends on the browser.

Libraries from the vendor of the browser are required on the user's computer to support a local key store. See [Key Access Libraries for the Client Machines](#) for more information.

Publish Public Keys in LDAP Directory

All public keys and certificates must also be stored to an LDAP directory, accessible by the Sun Java System Directory Server. This is referred to as publishing the public keys so they are available to other mail users who are creating S/MIME messages.

Public keys of the sender and receiver are used in the encrypting-decrypting process of an encrypted message. Public key certificates are used to validate private keys that were used for digital signatures.

See [Managing Certificates](#) for more information on using `ldapmodify` to publish the public keys and certificates.

Give Mail Users Permission to Use S/MIME

To create a signed or encrypted message, a valid Convergence user must have permission to do so. This involves using the `mailAllowedServiceAccess` or `mailDomainAllowedServiceAccess` LDAP attributes for a user's LDAP entry. These attributes can be used to include or exclude mail users from S/MIME on an individual or domain basis.

See [Granting Permission to Use SMIME Features](#) for more information.

Multi-language Support

A Convergence user who only uses English for their mail messages might not be able to read an S/MIME message which contains non-Latin language characters, such as Chinese. One reason for this situation is that the Java 6 Runtime Environment (JRE) installed on the user's machine does not have the `charsets.jar` file in the `/lib` directory.

The `charsets.jar` file is not installed if the English version of JRE was downloaded using the default JRE installation process. However, `charsets.jar` is installed for all other language choices of a default installation.

To ensure that the `charsets.jar` file is installed in the `/lib` directory, alert your users to use the custom installation to install the English version of JRE. During the installation process, the user must select the "Support for Additional Languages" option.

Wildcard SSL Certificates: Not Supported

While Wildcard SSL certificates enable SSL encryption on multiple subdomains with a single certificate, there are a number of security, certificate management, compatibility, and protection issues. Therefore, Wildcard SSL certificates are **NOT** supported in Convergence.

Configuring and Sending Encrypted Mail - Instructions for Convergence End Users

Configuring and Sending Encrypted Mail: Instructions for Convergence End Users

This page consists of information intended for the end user. It contains the following topics:

- [Logging In for the First Time](#)
- [Signature and Encryption Settings](#)
- [Enabling the Java Console](#)

Logging In for the First Time

When mail users log in to Convergence for the first time, they encounter special prompts relating to the S/MIME applet.

[Top](#)

Prompts for Windows

When logging in to Convergence for the first time on Windows 98, 2000 or XP, the following prompts display:

1. If the Java 6 Runtime Environment (JRE) is not installed on your computer (client machine), you receive a prompt looking something like this:

```
Do you want to install and run "Java Plug-in 1.6.2_03 signed on 10/01/08
and distributed by Sun Microsystems, Inc."?Publisher authenticity
verified by: VeriSign Class 3 Code Signing 2001 CA
```

Click Yes and follow the subsequent prompts to install JRE.



Note

If you desire English language support and also want to read incoming S/MIME messages that contain non-Latin characters, such as Chinese, the `charsets.jar` file must be in the `/lib` directory on your computer.

To ensure that the `charsets.jar` file is installed in the `/lib` directory, use the custom installation to install the English version of JRE. During the installation process, select the "Support for Additional Languages" option.

See [Multi-language Support](#) for more information.

Click Finish at the last installation prompt. Restart your computer and log in to Convergence again.

2. A prompt asking you:

```
Do you want to trust the signed applet distributed by "Sun Microsystems,
Inc."?Publisher authenticity verified by: Thawte Consulting cc
```

Click one of the following responses:

- Yes, to accept the S/MIME applet for this Convergence session. The prompt displays each time you log in.
 - No, to reject the S/MIME applet. You cannot use the S/MIME features.
 - Always, to accept the S/MIME applet for this and all subsequent Convergence sessions. You will not see the prompt again.
3. A prompt asking you:

Do you want to trust the signed applet distributed by "sun microsystems, inc."?Publisher authenticity verified by: VeriSign, Inc.

Click one of the following responses:

- Yes, to accept the S/MIME applet for this Convergence session. The prompt displays each time you log in.
- No, to reject the S/MIME applet. You cannot use the S/MIME features.
- Always, to accept the S/MIME applet for this and all subsequent Convergence sessions. You will not see the prompt again.

[Top](#)

Signature and Encryption Settings

There are initial signature and encryption settings that you can set to control whether all users' outgoing messages are:

- Automatically signed, or
- Automatically encrypted, or
- Automatically signed and encrypted

The initial settings also control whether the signature and encryption check boxes located at the top of a Convergence window and in the Options - Security window are displayed as checked (feature turned on) or unchecked (feature turned off). Use the `alwaysencrypt` and `alwaysign` parameters in the `smime.conf` file to specify the initial settings.

Let your mail users know that they can change the initial settings for their mail messages. After they log in to Convergence, a user can temporarily override a setting for one message, or for all their messages on an on-going basis.

The following table summarizes the use of the check boxes.

Signature and Encryption Check Boxes in Convergence

Text for Check Box	Location	What Convergence User Does
Sign Message	At the top of the Convergence Compose tab (used for composing, forwarding, or replying to a message).	<ul style="list-style-type: none"> • Check the box to sign the current message. • Uncheck the box not to sign the current message.
Encrypt Message	At the top of the Convergence Compose tab (used for composing, forwarding, or replying to a message).	<ul style="list-style-type: none"> • Check the box to encrypt the current message. • Uncheck the box not to encrypt the current message.
Sign all outgoing Messages	In Convergence Options - Security dialog, under the Default Sending Settings heading:	<ul style="list-style-type: none"> • Check the box to sign all your messages automatically. • Uncheck the box not to sign all your messages automatically. <p>Note: You can override the setting of "Sign all messages during send" on a message-by-message basis with the "Sign Message" check box.</p>
Encrypt all outgoing Messages	In the Convergence Options - Security dialog, under the Default Sending Settings heading:	<ul style="list-style-type: none"> • Check the box to encrypt all your messages automatically • Uncheck the box not to encrypt all your messages automatically. <p>Note: You can override the setting of "Encrypt all messages during send" on a message-by-message basis with the "Encrypt Message" check box.</p>

Enabling the Java Console

A variety of operating messages can be written to the Java Console by the S/MIME applet as a Convergence user processes signed and encrypted messages. The Java Console messages can be helpful when troubleshooting a problem reported by a mail user. However, operating messages are only generated when the Java Console is enabled for the user by adding a `nswmExtendedUserPrefs` attribute to the `inetMailUser` object class of their LDAP entry. For example:

```
nswmExtendedUserPrefs: mesmimedebug=on
```

Do not enable the Java Console for all mail users all the time because this significantly decreases the performance of Convergence.

Securing Internet Links With SSL

Securing Internet Links Between Oracle Communications Messaging Server and Convergence With SSL

The Messaging Server supports the use of the Secure Socket Layer (SSL) for Internet links affecting Convergence, as summarized in the following table.

Link Between:	Description
Messaging Server and Convergence	Securing this link with SSL requires administrative work for the Messaging Server. The Convergence user must use the HTTPS protocol, rather than HTTP, when entering the URL information for the Messaging Server in their browser. See Securing the Link Between Messaging Server and Convergence
Messaging Server and S/MIME applet	When checking public keys certificates against a CRL, the S/MIME applet must communicate directly with the Messaging Server. Securing this link with SSL requires administrative work for the Messaging Server in addition to setting <code>sslrootcacertsurl</code> and <code>checkoverssl</code> in the <code>smime.conf</code> file. See Securing the Link Between the Messaging Server and S/MIME Applet

Securing the Link Between Messaging Server and Convergence

The Messaging Server supports the use of Secure Socket Layer (SSL) for the Internet link between it and Convergence. Once you have set up Messaging Server for SSL, configure Convergence for SSL. See [Sun Convergence Administrative Tasks: SSL](#). A Convergence user specifies the Convergence URL in their browser with the HTTPS protocol:

```
HTTPS://hostname.domain:  
secured_port
```

instead of the HTTP protocol (`HTTP://hostname.domain:_unsecure_port_`). When the Convergence login window displays, the user sees a lock icon in a locked position at the bottom of their window to indicate they have a secure link.

See [Configuring Encryption and Certificate-Based Authentication](#) for SSL configuration information for Messaging Server.

[Top](#)

Securing the Link Between the Messaging Server and S/MIME Applet

When checking the certificate of a public key against a CRL, the S/MIME applet must communicate directly with the Messaging Server.

To Secure the Communications Link with SSL

1. Do the administrative tasks to configure the Messaging Server for SSL. See [Configuring Encryption and Certificate-Based Authentication](#).
2. Set the `sslrootcacertsurl` parameter in the `smime.conf` file to specify the information to locate the root SSL CA certificates. These CA certificates are used to verify the Messaging

Server's SSL certificates when the SSL link is established between the Messaging Server and the S/MIME applet.

3. Set the `checkoverssl` parameter in the `smime.conf` file to 1. This Messaging Server option determines whether SSL is used for the link between the Messaging Server and the S/MIME applet. Regardless of how a Convergence user specifies the URL for the Messenger Server (`HTTP` or `HTTPS`), the link between the Messaging Server and the S/MIME applet is secured with SSL when `checkoverssl` is set to 1.



Note

A proxy server can be used between the Messaging Server and client applications such as Convergence. See [Proxy Server and CRL Checking](#) using a proxy server with and without a secured communications link.

Key Access Libraries for the Client Machines

Key Access Libraries for the Client Machines

Whether your mail users keep their private-public key pairs and certificates on a smart card or in a local key store of their browsers, key access libraries must be present on the client machines to support the storage methods.

The libraries are supplied by vendors of the smart cards and browsers. You must ensure that the correct libraries are on the client machines and specify the library name or names with the appropriate platform parameter in the `smime.conf` file. The parameters choices are:

- `platformwin` for Microsoft Windows running on a PC.

You can specify only the libraries you know are installed on the client machines or you can specify all the library names for a given platform and vendor if you are not sure what is installed. If the S/MIME applet does not find the library it needs among the names you specify, the S/MIME features do not work.

The syntax to specify one or more library filenames is:

```
platform_parameter==vendor:library=  
library_name;...
```

where:

platform_parameter is the parameter name for the platform of the client machine where Convergence is accessed. Choose one of these names: `platformwin`

vendor specifies the vendor of the smart card or browser. Choose one of these literals:

CAC (for an ActivCard or NetSign smart card)

CAPI (for Internet Explorer with CAPI)

MOZILLA (for Mozilla with Network Security Services)

library_name specifies the library filename. See [Special Libraries for the Client Machines](#) for the library name for your vendor and operating system.

Special Libraries for the Client Machines

Smart Card or Browser Vendor	Operating System	Library Filename
	Windows	acpkcs211.dll
Internet Explorer with Cryptographic Application Programming Interface (CAPI)	Windows	capibridge.dll
	Windows	softokn3.dll
	Windows	core32.dll

Example

The following example specifies one smart card library and one Internet Explorer library, and one Mozilla library for a Windows platform:

```
platformwin==CAC:library=acpkcs211.dll;CAPI:library=capibridge.dll;  
MOZILLA:library=softokn3.dll;
```

Verifying Private and Public Keys

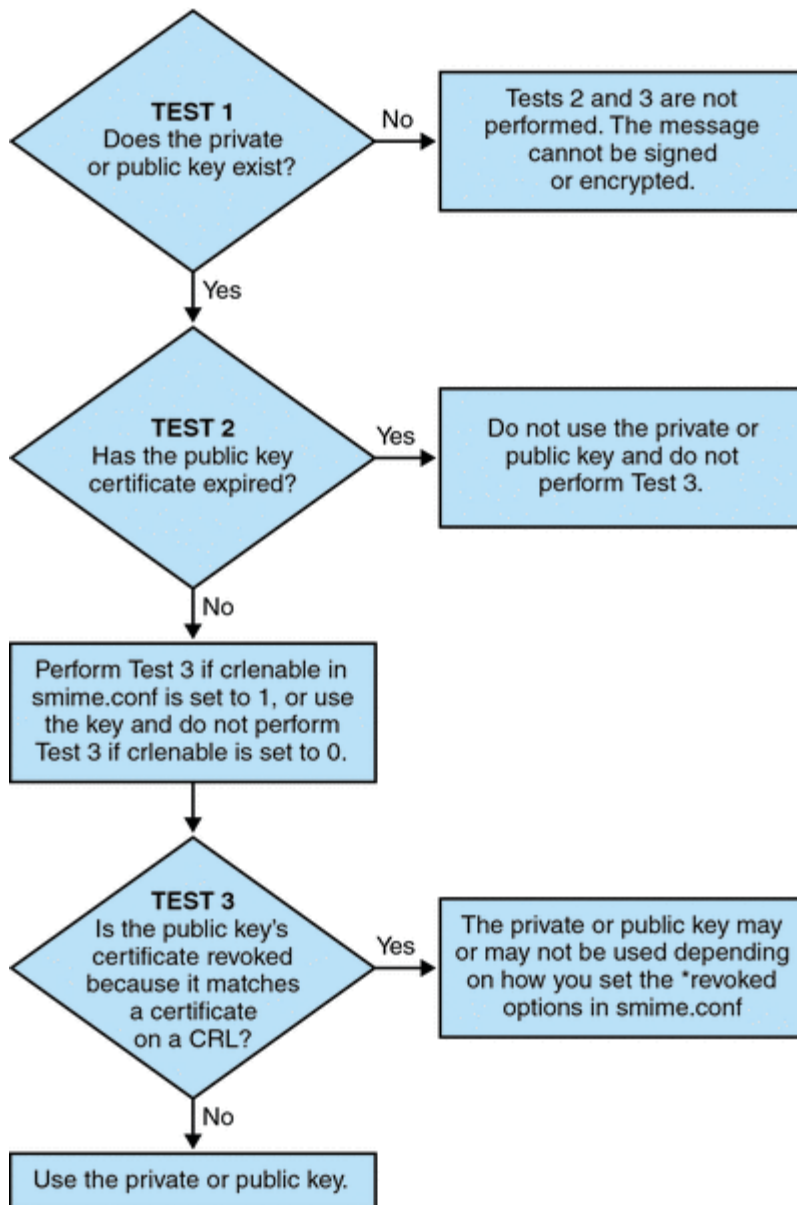
Verifying Private and Public Keys

Before Convergence Mail uses a private or public key, it must pass the verification tests shown in [Figure 1](#). The remainder of this section describes the details of checking a public key's certificate against a CRL.

This chapter contains the following sections:

- [Verifying Private and Public Keys.](#)
- [Finding a User's Private or Public Key](#)
- [When is a Certificate Checked Against a CRL?](#)
- [Accessing a CRL](#)
- [Proxy Server and CRL Checking](#)
- [Using a Stale CRL](#)
- [Determining Which Message Time to Use](#)
- [Trouble Accessing a CRL](#)
- [When a Certificate is Revoked](#)

Verifying Private and Public Keys.



Finding a User's Private or Public Key

When a Convergence Mail user has multiple private-public key pairs and multiple email addresses (primary, alternate, or alias addresses), it is possible that their keys are associated among their addresses. In this case, it is important that the S/MIME applet finds all the keys for verification purposes. Use the `usercertfilter` parameter in the `smime.conf` file to define a filter that creates a list of mail addresses for a key's owner at the time the public key's certificate is checked against a CRL. See [usercertfilter in smime.conf Parameters in Messaging Server](#) for more information.

When is a Certificate Checked Against a CRL?

A certificate revocation list, or CRL, is a list of revoked certificates maintained by the CA who issues the key pairs and certificates. When CRL checking is enabled, it causes the system to check the CRL whenever a certificate request has been made to see whether or not that certificate has been revoked.

When `crlenable` is set to 1 in the `smime.conf` file, a CRL test is performed after an unexpired key is found. The public key's certificate is checked against a CRL. There can only be one CRL for each CA, however the same CRL can be located in different places.

Checking a certificate against a CRL is done by the Messaging Server after the S/MIME applet sends it a request to do so. A public key certificate is used to validate a public key. Because a private key is kept secret, only used by the person who owns it, a private key cannot be checked directly against a CRL. To determine if a private key is good, the public key certificate of the key pair is used. When the public key's certificate passes the CRL test, the associated private key passes the test too.

Revocation of a certificate can happen for a variety of reasons, such as its owner has left your organization or lost the smart card.

There are three situations for checking a certificate against a CRL:

- When an outgoing message is signed

The S/MIME applet always does this check unless you set `sendsigncert` to 0 or `crlenable` to 0.

- When an incoming signed message is read

The S/MIME applet always does this check unless you set `readsigncert` to 0 or `crlenable` to 0.

- When an outgoing message is encrypted

The S/MIME applet always does this check unless you set `sendencryptcert` to 0 or `crlenable` to 0.

Accessing a CRL

A certificate contains zero or more URLs, known as distribution points, that are used by Messaging Server to locate a CRL. If the certificate does not have a CRL URL, it cannot be checked against a CRL and the private or public key is used to sign or encrypt a message without knowing its true status.

If Messaging Server fails to locate or gain access to a CRL after trying all the URLs available to it, the status of the certificate is treated as unknown. Whether a private or public key with an unknown status is used is determined by the setting of `revocationunknown`.

While only one CRL for each CA is supported, there can be multiple copies of the same CRL in different locations, reflected in different URLs among a user's public key certificates. Messaging Server tries all the URL locations for a certificate until it gains access to the CRL.

You can manage multiple copies of a CRL for optimum access by periodically downloading the current CRL from the CA to a place where you want it. While you cannot change the URLs embedded in the certificates, you can redirect Messaging Server to use new CRL locations by mapping the URLs in a certificate to a new URL containing the CRL information. Create a list of one or more mapping definitions in the LDAP directory (see `crmappingurl` in [S/MIME Configuration Parameters in smime.conf File](#)) with this syntax:

```
msgCRLMappingRecord=url_in_certificate==
new_url[|url_login_DN|url_login_password]
```

`url_in_certificate` is the URL in the certificate containing the old information to locate the CRL. `new_url` is the new URL containing the new CRL information. `url_login_DN` and `url_login_password` are the DN and password of the entry allowed access to `new_url`. Both are optional, and if specified, will be used for the new URL access only.

If the DN and password fails, LDAP access is denied and no retry with other credentials is attempted. These login credentials are only valid for LDAP URLs. If you use `curlurllogindn` and `curlurlloginpw` in `smmime.conf`, then you don't need to specify the login DN and password in the

mapping record. See [Accessing LDAP for Public Keys, CA certificates and CRLs Using Credentials](#)

Only one layer of mapping is allowed. Different URLs in the certificates can be mapped to the same new URL, but you cannot assign a certificate URL to multiple new URLs. For example, the following mapping list is not valid:

```
msgCRLMappingRecord=URL12==URL45
msgCRLMappingRecord=URL12==URL66
msgCRLMappingRecord=URL12==URL88
msgCRLMappingRecord=URL20==URL90
msgCRLMappingRecord=URL20==URL93
```

The next example is a correct mapping list:

```
msgCRLMappingRecord=URL12==URL45
msgCRLMappingRecord=URL14==URL66
msgCRLMappingRecord=URL88==URL66
msgCRLMappingRecord=URL201==URL90
msgCRLMappingRecord=URL202==URL93
```

Once you have created the mapping definitions in your LDAP directory, use `crlmappingurl` in the `smime.conf` file to specify the directory information to locate them. See [smime.conf Parameters in Messaging Server](#).

Proxy Server and CRL Checking

If your system uses a proxy server between client applications and the Messaging Server, CRL checking can be blocked despite the fact that you correctly configured the S/MIME applet to perform CRL checking. When this problem occurs, users of Convergence Mail receive error messages alerting them to revoked or unknown status for valid key certificates.

The following conditions cause the problem:

- CRL checking is requested with these configuration values:
 - `crlenable` parameter in the `smime.conf` file is set to 1
 - `local.webmail.cert.enable` option of Messaging Server is set to 1
- The communications link between the S/MIME applet and the proxy server is not secured with SSL, but the S/MIME applet is expecting a secured link because the `checkoverssl` parameter in the `smime.conf` file is set to 1

To solve this problem, you can:

1. Set up the communications link between the client machines and proxy server as a secured link with SSL and leave all the configuration values as they are. Or,
2. Leave the communications link unsecured and set `checkoverssl` to 0.

For more information see [Securing Internet Links With SSL](#).

Using a Stale CRL

Checking a certificate against a CRL is done by the Messaging Server after the S/MIME applet sends it a request to do so. Rather than download a CRL to memory each time a certificate is checked, Messaging Server downloads a copy of the CRL to disk and uses that copy for certificate checking. Every CRL has a next-update field which specifies the date after which a newer CRL version should be used. The next-update date can be viewed as an expiration date or time limit for using the CRL. A CRL that is past

it's next-update date is considered old or stale and triggers Messaging Server to download the latest version of the CRL the next time a certificate is checked.

Every time the S/MIME applet requests that a certificate be checked against a CRL, the Messaging Server does the following:

1. Compares the current date to the next-update date of the CRL.
2. If the CRL is stale, the Messaging Server downloads the latest version of the CRL to replace the stale CRL on disk and checking proceeds. However, if a newer CRL cannot be found or cannot be downloaded, the value of `crlusepastnextupdate` in the `smime.conf` file is used to determine what to do.
3. If `crlusepastnextupdate` is set to 0, the stale CRL is not used and the certificate in question has an ambiguous status. The S/MIME applet uses the value of `revocationunknown` in `smime.conf` to determine what to do next:
 - a. If `revocationunknown` is set to `ok`, the certificate is treated as valid and the private or public key is used to sign or encrypt a message.
 - b. If `revocationunknown` is set to `revoked`, the certificate is treated as invalid, the private or public key is not used to sign or encrypt a message, and a pop-up error message alerts the mail user that the key cannot be used.

If `crlusepastnextupdate` is set to 1, the S/MIME applet continues to use the stale CRL which causes no interruption of processing within Convergence Mail, however a message is written to the Messaging Server log file to alert you to the situation.

This sequence of events continues to occur as certificates are checked against the CRL. As long as the Messaging Server can download a newer version of the CRL in a timely manner, and depending on the settings in the `smime.conf` file, mail processing proceeds without interruption. Check the Messaging Server log periodically for repeated messages that indicate a stale CRL is in use. If a newer CRL cannot be downloaded, you need to investigate why it is inaccessible.

Determining Which Message Time to Use

The `timestampdelta` parameter is used primarily for these purposes:

1. To handle the situation of a message that takes a long time to arrive at its destination. For this case, the sender's key might be treated as an invalid key despite the fact that the key was valid when the message was sent.
2. To limit the trust in a message's sent time because sent times can be faked.

There are two times associated with every message:

- The time when the message was sent, as found in the Date line of the message header detail
- The time when the message arrives at its destination, as found in the last Received line of the message header detail



Note

View the message header detail by clicking the triangle icon at the right hand side of a message's From field.

A certificate that was valid when a message was sent can be revoked or expired by the time the message reaches its destination. When this happens, which time should be used when checking the validity of the certificate, the sent time or the received time? Using the sent time would verify that the certificate was valid when the message was sent. But always using the sent time does not take into account the fact that it might take a long time for a message to arrive at its destination, in which case it would be better to use the received time.

You can influence which time to use for CRL checking by using the `timestampdelta` parameter in the

`smime.conf` file. Set this parameter to a positive integer, representing seconds. If the received time minus the value of `timestampdelta` is a time before the sent time, the sent time is used. Otherwise, the received time is used. The smaller the value of `timestampdelta`, the more often the received time is used. When `timestampdelta` is not set, the received time is always used. See `timestampdelta` in [S/MIME Configuration Parameters in smime.conf File](#).

Trouble Accessing a CRL

For a variety of reasons, such as network or server problems, a CRL might be unavailable when Messaging Server attempts to check a certificate against it. Rather than let the Messaging Server spend its time constantly trying to gain access to the CRL, you can use the `crlaccessfail` parameter in the `smime.conf` file to manage how often it attempts to access the CRL, freeing up the Messaging Server for other tasks.

Define the following with `crlaccessfail`:

- How many failed attempts are counted (an error message is written to the Messaging Server log after each failed attempt)
- Over what period of time the failed attempts are counted
- How long to wait before attempting a new cycle of accessing the CRL

See `crlaccessfail` in [S/MIME Configuration Parameters in smime.conf File](#) for the parameter's syntax and an example.

When a Certificate is Revoked

When a public key's certificate does not match any entry on the CRL, the private or public key is used to sign or encrypt an outgoing message. When a certificate matches an entry on the CRL or the certificate's status is unknown, a private or public key is considered revoked. By default Convergence Mail does not use a key with a revoked certificate to sign or encrypt an outgoing message. If the private key of a signed message is revoked by the time the recipient reads the message, the recipient receives a warning message indicating that the signature should not be trusted.

If desired, you can change the various default policies for all revoked certificates with the following parameters in the `smime.conf` file:

- Set `sendsigncertrevoked` to `allow` to sign an outgoing message with a private key that is considered revoked because its public key's certificate is revoked
- Set `sendencryptcertrevoked` to `allow` to encrypt an outgoing message with a public key that has a revoked certificate
- Set `revocationunknown` to `ok` to treat a certificate as valid whose status is unknown; the private or public key is used to sign or encrypt an outgoing message

Granting Permission to Use SMIME Features

Granting Permission to Use S/MIME Features

Permission to use the various mail services available through Convergence can be given or denied with LDAP filters. A filter is defined with the `mailAllowedServiceAccess` or `mailDomainAllowedServiceAccess` LDAP attributes. Generally speaking, a filter works in one of three ways:

- Permission is given to all users for all services when no filter is used
- Permission is explicitly given to a list of users for specified service names (a plus sign (+) precedes the service name list)
- Permission is explicitly denied to a list of users for specified service names (a minus sign (-) precedes the service name list)

The required mail service names for S/MIME are `http`, `smime`, and `smtp`. If you need to restrict the use of S/MIME among Convergence users, use the appropriate LDAP attribute syntax and service names to create a filter. The attributes are created or modified with LDAP commands.

S/MIME Permission Examples

1. The following examples block access to the S/MIME features for one Convergence user:

```
mailAllowedServiceAccess  
mailAllowedServiceAccess: -smime:*$+imap,pop,http,smtp:*
```

or

```
mailAllowedServiceAccess: +imap,pop,http,smtp:*
```

2. The following examples block access to the S/MIME features for all Convergence users in a domain:

```
mailDomainAllowedServiceAccess: -smime:*$+imap:*$+pop:*$+smtp:*$+http:*
```

or

```
mailDomainAllowedServiceAccess: +imap:*$+pop:*$+smtp:*$+http:*
```

See [Filter Syntax](#) for more information.

Managing Certificates for SMIME

Managing Certificates for SMIME

Most of the following examples use the `ldapsearch` and `ldapmodify` commands to search an LDAP directory for user keys and certificates. These commands are provided with Directory Server. See the [Sun Java System Directory Server Enterprise Edition Man Page Reference](#) for more information about the commands.

CA Certificates in an LDAP Directory

This example adds a certificate for a certificate authority to an LDAP directory. The directory structure for these certificates already exists. The certificate and the LDAP entries where it belongs are entered into an `.ldif` file named `add-root-CA-cert.ldif`. All text is entered into the file in ASCII text except for the certificate information, which must be entered as Base64 encoded text:

```
dn: cn=SMIME Admin,ou=people,o=demo.siroe.com,o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationAuthority
cn: RootCACerts
sn: CA
authorityRevocationList: novalue
certificateRevocationList: novalue
cacertificate;binary::
MFU01JTUUEjAQBgNVBAsTCU1zZ1NlcnZlcjcmBoGA1UEAxMTydg
QGEwJVUzEOMAwGA1UEMFUJTUUxEjAQBgNVBAsTCU1zZ1NlcnZlcjEMBoGA1UEAxMTQ2Vydg
aFw0wNjAxMwODAwMDBaM267hgbX9FExCzAJByrjgNVBAK9STklBMQwCgYDVQQVHR8EgaQwg
YTA1VMRMQYDVQQIEWpDQUxJRk9STklBMQwwCgYDVQQKEwww3ltgYz11lzAdBgNVBpYSE9Vc
5yZWQaddWlm899XBsYW5ldC5jb20wgZ8wDQYJcGBAK1mUTy8vvnOFg4mlHjkghytQUR1k8l
5mvWRf77ntm5mGXRd3XMU40ciUq6zUfIg3ngvx1LyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FNAJmtOV2A3wMyghqkVPNDP3Aqq2fkc4va3C5nRNAYxNNVE84JJ0H3jyPDXhMB1QU6vQn
weMBAAjggEXMIIBEzARBglghkgBhCAQEeBAPq1Sai4mfuvjh02SQkoPMNDAGTwMB8GA1UdI
QYBAaEd38IK05AHreiU9OYc6vNMOWZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht
bmcucmVklmlbGFuZlZlY29tL1VJdD1DXJ0aWZpY2F0ZSBNYW5hZ2VyLE9VPVBlb3BsZSxPPW
aWxxYT9jZXJ0aZpY2jdu2medXR1lkghytQURyFNrkuoCygKoYoaHR0cDovL3Blal2kgghytQU
Zy5yZWQuaXBsYW5ldC5jb20vcGVranLmNybDAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
4uY29tMA0GCxLm78freCxS3Pp078jyTaDcilAudBL8+RrRUQvxsMjFZeFED+Uuf10Ilt6kw
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
```

The CA's certificate is added to the LDAP directory with an `ldapmodify` command:

```
# ldapmodify -a -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-v
-f add-root-CA-cert.ldif
```

The value of the `trustedurl` parameter in `smime.conf` specifies the location of the CA certificates in the LDAP directory. For Example 1, `trustedurl` is set to:

```
trustedurl==ldap://demo.siroe.com:389/cn=SMIME Admin, ou=people,
o=demo.siroe.com,o=demo?cacertificate;binary?sub?
(objectclass=certificationAuthority)
```

Public Keys and Certificates in an LDAP Directory

This example demonstrates adding a mail user's public key and certificate to the LDAP directory. It assumes the mail user already exists in the LDAP directory. The key and certificate, and the LDAP entries where it belongs, are entered into an `.ldif` file named `add-public-cert.ldif`. All text is entered into the file as ASCII text except for the key and certificate information, which must be entered as Base64 encoded text.

```
dn: uid=JohnDoe,ou=People, o=demo.siroe.com,o=demo
changetype: modify
replace: usercertificate
usercertificate;binary::
MFU01JTUUXeJAQBGNVBAsT1zZ1N1cnZlcjMBoGA1UEAxMTYdG
QGEwJVUzEAWGAlhMFU01JTUUXeJAQBGNVBAsTCU1zZ1N1cnZlcjEcmBoGA1UEAxMTQ2VydG
aFw0wNjAAMTODAwM267hgbcX9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
AlVzMRMwEQYDVQQIDQXJRk9STklBMQwwCgYDVQQKEwww3ltgoOYz11lzAdBgNVBpYSE9Vc
5yZWaddiiWlM899XBsYW5ldB20wgZ8wDQYJoGBAK1mUTy8vv02nOFg4mlHjkghytQUR1k8l
5mvgcWL77ntm5mGXRd3XMU4OcizUfIg3ngvx1LkLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FG9NAqtOV2A3wMyghqkVPNDP3Aqq2BYfkcN4va3RNAYxNNVE84JJ0H3jyPDXhMB1QU6vQn
1NagMBGjggEXMIIBEzARBg1ghkgBhvCAQEEBApq1Sai4mfuvjh02SQMNDAGTwmB8GA1UdI
QYMBaEd38IK05AHreiU9OYc6v+ENMOwZMIGsBgNVHR8EgaQwgaEwb6BuGaWxkYXA6Lyht74
tpbmcmVklmLwbGFuZXRyY29tL1VJRd1DZXJ0aWZpY2F0ZSBNYW5hZ2V9VPVBlb3BsZSxPPW
1haWxT9jZXJ0aWZpY2Jdu2medXR11HjkghytQURyFNrkuoCygKoYoaHDovL3Bla2kgghytQU
luZy5WQuaXBSYw5ldC5jb20vcGVraW5nLmNybdAeBgNVHREEFzAVgRNw0aWEuc2hhb0BzdW
4uY29A0GCxLm78UfreCxS3Pp078jyTaDv2ci1AudBL8+RrRUQvxsMJfZD+Uuf10Ilt6kwhm
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
```

The `ldapmodify` command is used to add the public key and certificate to the LDAP directory:

```
# ldapmodify -a -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-v
-f add-public-cert.ldif
```

The value of the `certurl` parameter in `smime.conf` specifies the location of the public keys and their certificates in the LDAP directory. For Example 2, `certurl` is set to:

```
certurl==ldap://demo.siroe.com:389/ou=people, o=demo.siroe.com,
o=demo?userCertificate;binary?sub?
```

Verifying That Keys and Certificates Exist in the LDAP Directory

The following examples demonstrate searching an LDAP directory for CA certificates and public keys and their certificates.

Searching for One CA Certificate

In the following example, the base DN defined by the `-b` option, `cn=SMIME admin, ou=people, o=demo.siroe.com, o=demo objectclass=*`, describes one CA certificate in the LDAP directory. If found in the directory, `ldapsearch` returns information about the certificate to the `ca-cert.ldif` file.

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b
"cn=SMIME admin, ou=people, o=demo.siroe.com, o=demo" "objectclass=*"
> ca-cert.ldif
```

The example below shows the search results in the `ca-cert.ldif` file. The format of the file's contents is a result of using the `-L` option of `ldapsearch`.

```
# more ca-cert.ldif
dn: cn=SMIME admin,ou=people,o=demo.siroe.com,o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: certificationAuthority
cn: RootCACerts
cn: SMIME admin
sn: CA
authorityRevocationList: novalue
certificateRevocationList: novalue
cacertificate;binary::
MFU01JTUUXEjAQBgNVBAsTCU1zZnlnZlcjcmBoGA1UEAxMTYdG
QGEwJVEOMAwGA1UEChMFU0UUXEjAQBgNVBAsTCU1zZnlnZlcjEcmBoGA1UEAxMTQ2Vydg
aFw0jAxBMTIwODAwMDBaM267X9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
Y1VzMRMwEQYDVQQIEWpDQUx9STklBMQwwCgYDVQQKEw3ltgoOYz11lzAdBgNVBpYSE9Vc
5yQuaddiiWlm899XBsYW51jb20wgZ8wDQYJOGBAK1mUTy8vvO2nOFg4mlHjkghytQUR1k8l
5mcWRfL77ntm5mGXRD3XMciUq6zUfIg3ngvx1LKLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FNAJmqtOV2A3wMyghqkDP3Aqq2BYfkc4va3C5nRNAyxNNVE84JJ0H3jyPDXhMB1QU6vQn
1NABAAGjggEXMIIBEZglghkgBhvhCAQEEBAPq1Sai4mfuvjh02SQkoPMNDAGTwMB8GA1UdI
QYMAFED38IK05AHreOYc6v+ENMOWZMIGsBgNVHR8EgaQwgaEwb6BtoGuGaWxkYXA6Lyht74
tpbucmVklmlwbGFuZyZy29tL1VJRd1DZXJ0aWZpY2F0ZSBNYW5hZ2VyeLE9VPVBlb3BsZSxPPW
1haWYT9jZXJ0aWZpdu2medXR11HjkghytQURyFNrkuoCygKoYoaHR0cDovL3Bl2kgghytQU
luZyZWQuaXBsYW51db20vcGVraW5nLmNybDAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
4uYtMA0GCxLm78Ufre3Pp078jyTaDv2cilAudBL8+RrRUQvxsmJfZeFED+Uuf10Ilt6kwhm
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
```

Searching for a Several Public Keys

In the following example, the base DN defined by the `-b` option, `o=demo.siroe.com, o=demo objectclass=*`, is such that all public keys and certificates found at and below the base DN in the LDAP directory are returned to the file `usergroup.ldif`:

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b "o=demo.siroe.com, o=demo" "objectclass=*" > usergroup.ldif
```

Searching for One Public Key

In the following example, the base DN defined by the `-b` option, `uid=JohnDoe,`

ou=people,o=demo.siroe.com,o=demo objectclass=*, describes one public key and its certificate in the LDAP directory:

```
# ldapsearch -L -h demo.siroe.com -D "cn=Directory Manager" -w mypasswd
-b
"uid=JohnDoe, ou=people,o=demo.siroe.com,o=demo" "objectclass=*" >
public-key.ldif
```

The example below shows the search results in the public-key.ldif file. The format of the file's contents is the result of using the -L option of ldapsearch.

```
# more public-key.ldif
dn: uid=sdemol, ou=people, o=demo.siroe.com, o=demo
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: siroe-am-managed-person
objectClass: inetOrgPerson
objectClass: inetUser
objectClass: ipUser
objectClass: userPresenceProfile
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: icsCalendarUser
objectClass: sunUCPreferences
mail: JohnDoe@demo.siroe.com
mailHost: demo.siroe.com
.
.
uid: JohnDoe
.
.
mailUserStatus: active
inetUserStatus: active
.
.
usercertificate;binary::
MFU01JTUUXEjAQBGNBAsTCU1zZ1N1cnZjcMBoGA1UEAxMTydG
QGEwJEOWGA1UEChMFU01JTUUXEjAQBGNVBAsTCU1zZ1N1cnZlcjEcMBoGA1UEAxMTQ2VyDG
aFw0MTIwODAwMDBaM267hgbX9FExCzAJBgwyrjgNVBAk9STklBMQwwCgYDVQQVHR8EgaQwg
YTA1VEQYDVQQIEWpDQUxJRk9STklBMQwwCgYDVQQKEWww3ltgoOYz111zAdBgNVBpYSE9Vc
5yZWQdWlm899XBsYW5ldC5jb20wgZ8wDQYJOGBAK1mUTy8vv02nOfg4mlHjkghytQUR1k8l
5mvgc7ntm5mGXRd3XMU40ciUq6zUfIg3ngvxlLkLyERTIqjUS8HQU4R5pvj+rrVgsAGjggE
+FG9NmV2A3wMyghqkVPNDP3Aqq2BYfkcN4va3C5nRNAYxNNVE84JJ0H3jyPDXhMB1QU6vQn
1NAGMAGEXMIIBEzARBglghkgBhvhCAQEEBAPq1Sai4mfuvjh02SQkoPMNDAGTwMB8GA1UdI
QYMBaEdK05AHreiU9OYc6v+ENMOWZMIGsBgNVHR8EgaQwgEwb6BtoGuGaWxkYXA6Lyht74
tpbucmVkwBGFuZlZlZjZjZDU2medXRllHjkghytQURYFNrkuoCygKoYoaHR0cDovL3Bla2kghytQU
luZyZWQuaYW5ldC5jb20vcGVraW5nLmNybdAeBgNVHREEFzAVgRNwb3J0aWEuc2hhb0BzdW
4u9tMA0GC78UfreCxS3Pp078jyTaDv2cilAudBL8+RrRUQvxsMJfZeFED+Uuf10Ilt6kwhm
Tc6W5UekbirfEZGAVQIzlt6DQJfgpifGLvtQ60Kw==
.
.
```

Network Security Services Certificates

Various certificates used for Network Security Services (NSS) are stored in their own database, which is not an LDAP database. Two utilities, `certutil` and `crlutil`, are provided with Messaging Server to store the certificates and associated CRLs in the database. You can also use these utilities to search the database.

See the [Sun Java System Directory Server Administration Guide](#) for more information about `certutil`. Use the help text that comes with `crlutil` for more information about that utility (view the online help of both utilities by executing them without arguments).

Configuring Messaging Server to Use SMIME in Convergence

Configuring Messaging Server to Use S/MIME in Convergence

This section explains what the S/MIME applet is and provides a basic configuration procedure to set up S/MIME for Convergence. The configuration process involves setting parameters for the S/MIME applet and options for Messaging Server.

This page includes the following topics:

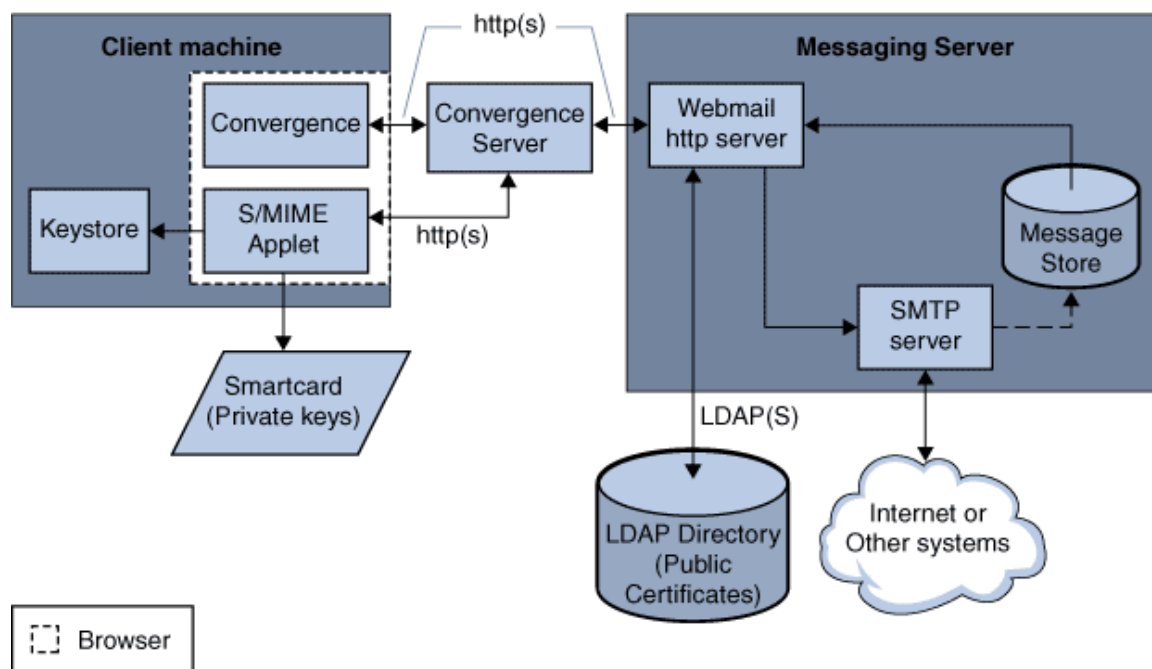
- [Overview of the S/MIME Applet](#)
- [Configuring S/MIME](#)
- [Accessing LDAP for Public Keys, CA certificates and CRLs Using Credentials](#)

Overview of the S/MIME Applet

The process of signing a message, encrypting a message, or decrypting a message, along with the various procedures to verify private and public keys, are handled by a special applet, referred to as the S/MIME applet. The configuration of the S/MIME features is done with parameters in the `smime.conf` file and options of Messaging Server.

S/MIME Applet

The following figure shows the S/MIME Applet in relation to other system components.



Logging In for the First Time

When a Convergence user who has permission to use S/MIME logs in to the Messaging Server for the first time, a series of special prompts displays about the S/MIME applet. After answering the prompts with Yes or Always, the S/MIME applet is downloaded to their computer. The applet remains on their machine until they log out of Convergence.

Refer to [Managing Certificates for S/MIME](#) for more information.

How the S/MIME Applet is Downloaded to the Client Machine

The S/MIME applet is downloaded each time a user logs in to Convergence unless caching is enabled for the Java 6 Runtime Environment (JRE) on the user's machine. When caching is enabled, a copy of the S/MIME applet is saved on the user's machine after the initial download which prevents downloading the applet every time the user logs in.

Caching can improve performance so you might direct your users to do the following steps to enable caching for Java 6 Runtime Environment, Version 1.6.x:

To Enable Caching for Java 6 Runtime Environment, Version 1.6

1. Navigate to the Windows Control Panel.
2. Double click the Java Plug-in icon (Java 6 Runtime Environment).
3. Click the Cache tab.
4. Check the Enable Caching checkbox.
5. Click Apply.

After downloading, a user is not aware of the S/MIME applet. It appears that signing, encrypting, or decrypting a message is done by Convergence. Unless an error message pops up, the user also is unaware of the processes to verify a private or public key. Refer to [Verifying Private and Public Keys](#) for more information.

Configuring S/MIME

The configuration file for S/MIME, `smime.conf`, contains descriptive comments and an example of each S/MIME parameter. The `smime.conf` file is included with Messaging Server, located in the directory `msg-svr-base/config/`, where `msg-svr-base` is the directory where Messaging Server is installed.

The following procedure contains the minimum required steps to configure the S/MIME features:

To Configure S/MIME

1. Verify that the basic features of Convergence are working after you install Messaging Server.
2. If you haven't already, create or obtain private-public key pairs, with certificates in standard X.509 v3 format, for all your mail users who have permission to use the S/MIME features.
3. If smart cards are used for keys and certificates:
 - a. Distribute the smart cards to your mail users.
 - b. Ensure that the smart card reading devices and software are properly installed on each client machine where Convergence is accessed.
4. If local key stores of the browsers are used to store keys and certificates, instruct your mail users how to download their key pairs and certificate to the local key store.
5. Ensure that the correct libraries are on the client machines to support smart cards or local key stores. See [Key Access Libraries for the Client Machines](#)
6. Set up your LDAP directory to support S/MIME:
 - a. Store all certificates for the CAs in the LDAP directory, accessible by Directory Server, under the distinguished name for certificate authorities. The LDAP attribute for these certificates is `cacertificate;binary`. Write down the directory information where you store them. You'll need this information for a later step.

See `trustedurl` in the [S/MIME parameter table](#) for an example of specifying LDAP directory information and [Managing Certificates for S/MIME](#) for information to search an LDAP directory.

- b. Store the public keys and certificates in the LDAP directory accessible by Directory Server. The LDAP attribute for public keys and certificates is `usercertificate;binary`. Write down the directory information where you store them. You'll need this information for a later

step.

See [certurl](#) in the [S/MIME parameter table](#) for an example of specifying LDAP directory information and [Managing Certificates for S/MIME](#) for information to search an LDAP directory.

- c. Ensure that all users who send or receive S/MIME messages are given permission to use S/MIME with an LDAP filter in their user entries. A filter is defined with the `mailAllowedServiceAccess` or `mailDomainAllowedServiceAccess` LDAP attributes.

Note: By default, if you do not use `mailAllowedServiceAccess` or `mailDomainAllowedServiceAccess`, all services including `smime`, are allowed. If you explicitly specify services with these attributes, then the services `http` and `smtp`, as well as `smime`, must be specified to give mail users permission to use the S/MIME features.

See [Granting Permission to Use S/MIME Features](#) for more information.

7. Edit the `smime.conf` file with any available text editor. See comments at the beginning of the file for parameter syntax.

All text and example parameters in `smime.conf` are preceded with a comment character (`#`). You can add the parameters you need to `smime.conf` or copy a parameter example to another part of the file and change its value. If you copy and edit an example, be sure to remove the `#` character at the beginning of its line.

Add these parameters to the file, each on its own line:

- a. `trustedurl` (see the [S/MIME parameter table](#))-- set to the LDAP directory information to locate the certificates of the CAs. Use the information you saved from [Step a](#).
- b. `certurl` (see the [S/MIME parameter table](#))-- set to the LDAP directory information to locate the public keys and certificates. Use the information you saved from [Step b](#).
- c. `usersertfilter` (see the [S/MIME parameter table](#)) – set to the value of the example in the `smime.conf` file. The example value is almost always the filter you want. *Copy* the example and delete the `#` character at the beginning of the line.

This parameter specifies a filter definition for the primary, alternate, and equivalent email addresses of a Convergence user to ensure that all of a user's private-public key pairs are found when the key pairs are assigned to different mail addresses.

- d. `sslrootcacertsurl` (see the [S/MIME parameter table](#))-- if you are using SSL for the communications link between the S/MIME applet and Messaging Server, set `sslrootcacertsurl` with the LDAP directory information to locate the certificates of CAs that are used to verify the Messaging Server's SSL certificates. See [Securing Internet Links With SSL](#) for more information.

`checkoverssl` (see the [S/MIME parameter table](#))-- set to 0 if you are not using SSL for the communications link between the S/MIME applet and Messaging Server.

- e. `crlenable` (see the [S/MIME parameter table](#))-- set to 0 to disable CRL checking for now because doing CRL checking might require adding other parameters to the `smime.conf` file.
- f. `logindn` and `loginpw` (see the [S/MIME parameter table](#))-- if the LDAP directory that contains the public keys and CA certificates requires authentication to access it, set these parameters to the distinguished name and password of the LDAP entry that has read permission.

Note: The values of `logindn` and `loginpw` are used whenever the LDAP directory is accessed with the LDAP information specified by the `crlmappingurl`, `sslrootcacertsurl`, or `trustedurl` parameters. See [smime.conf Parameters in Messaging Server and Accessing LDAP for Public Keys, CA certificates and CRLs Using Credentials](#) for more information.

Do not set `logindn` and `loginpw` if authentication is not required to access the LDAP directory.

8. Set the Messaging Server options with `configutil`:
 - a. `local.webmail.smime.enable` – set to 1.
 - b. `local.webmail.cert.enable` – set to 1 if you want to verify certificates against a CRL.

See [Messaging Server configutil Options for SMIME](#) for more information.

9. Enable S/MIME in the Convergence server with `iwcadmin`:

```
/opt/sun/comms/iwc/sbin/iwcadmin -o smime.enable -v true
```
10. Restart GlassFish Server.
11. Convergence is now configured for the S/MIME features. Verify that the S/MIME features are working with the following steps:
 - a. Restart the Messaging Server.
 - b. Check the Messaging Server log file, `msg-svr-base /log/http`, for diagnostic messages relating to S/MIME.
 - c. If any problems were detected for S/MIME, the diagnostic messages help you determine how to correct the problem with the configuration parameters.
 - d. Correct the necessary configuration parameters.
 - e. Repeat Steps a. through d. until there are no more diagnostic messages for S/MIME in the Messaging Server's log file.
 - f. Check that the S/MIME features are working with the following steps:
 - g. Log in to Messaging Server from a client machine. Answer the special prompts for the S/MIME applet with Yes or Always. See [Managing Certificates for S/MIME](#)
 - h. Compose a short message, addressed to yourself.
 - i. Encrypt your message by checking the Encrypt checkbox at the bottom of the Compose window if it is not already checked.
 - j. Click Send to send the encrypted message to yourself. This should exercise most of the mechanisms for keys and certificates.
 - k. If you find problems with the encrypted message, the most likely causes are the values you used for LDAP directory information in the `smime.conf` file and/or the way keys and certificates are stored in the LDAP directory. Check the Messaging Server log for more diagnostic messages.

The remaining S/MIME parameters, summarized in the table below, provide many options you might want to use to further configure your S/MIME environment. See [smime.conf Parameters in Messaging Server](#) for more information about the parameters.

Required Parameters for S/MIME	Parameters for Smart Cards and Local Key Stores	Parameters for CRL Checking	Parameters for Initial Settings and Secured Links
certurl*	platformwin	checkoverssl	alwaysencrypt
logindn		crlaccessfail	alwaysysign
loginpw		crlidir	sslrootcacertsurl
trustedurl*		crlenable	
usercertfilter*		crlmappingurl	
		crlurllogindn	
		crlurlloginpw	
		crlusepastnextupdate	
		readsigncert	
		revocationunknown	
		sendencryptcert	
		sendencryptcertrevoked	
		readsigncert	
		sendsigncertrevoked	
		timestampdelta	

- You must specify a value for these parameters because they have no default value.

Accessing LDAP for Public Keys, CA certificates and CRLs Using Credentials

Public keys, CA certificates, and CRLs required for S/MIME may be stored in an LDAP directory (see previous section). The keys, certificates, and CRLs may be accessible from a single URL or multiple URLs in LDAP. For example, CRLs may be stored in one URL and public keys and certificates may be stored in another. Messaging Server allows you to specify which URL contains the desired CRL or certificate information, as well as the DN and password of the entry that has access to these URLs. These DN/password credentials are optional; if none are specified, LDAP access first tries the HTTP server credentials, and if that fails, it tries accessing it as `anonymous`.

Two pairs of `smime.conf` credential parameters may be set to access the desired URLs: `logindn` and `loginpw`, and `crlurllogindn` and `crlurlloginpw`.

`logindn` and `loginpw` are the credentials used for all URLs in `smime.conf`. They specify the DN and password of the LDAP entry that has read permission for the public keys, their certificates, and the CA certificates as specified by the `certurl` and `trustedurl` parameters.

`crlurllogindn` and `crlurlloginpw` specifies the DN and password of the LDAP entry that has read permission for the resulting URL from the mapping table (see [Accessing a CRL](#) for more information). If these credentials are NOT accepted, LDAP access is denied and no retry with other credentials is attempted. Either both parameters must be specified, or both must be empty. These parameters do not apply to the URLs that come directly from the certificate.

Setting Passwords for Specific URLs

Messaging Server allows you to specifically define the DN/ password pairs for accessing the following `smime.conf` URLs: `certUrl`, `trustedUrl`, `crlmappingUrl`, `sslrootcacertsUrl`.

The syntax is as follows:

```
url_type URL [[CommSuite:URL_DN | URL_password]
```

Example:

```
trustedurl==ldap://mail.siroe.com:389/cn=Directory Manager, ou=people,  
o=siroe.com,o=ugroot?cacertificate?sub?(objectclass=certificationauthority  
|  
cn=Directory manager | boomshakalaka
```

Summary of Using LDAP credentials

This section summarizes the use of LDAP credentials.

- All LDAP credentials are optional; if none are specified, LDAP access first tries the HTTP server credentials, and if that fails, tries `anonymous`.

Two pairs of `smime.conf` parameters are used as credentials for the two sets of URLs that may be specified:

`logindn` & `loginpw` - all URLs in `smime.conf`

`crlurllogindn` & `crlurlloginpw` - all URLs from mapping table

These are known as the default LDAP credential pair.

- Any URL specified in `smime.conf` or via mapping CRL URLs can have an optional local LDAP credential pair specified.
- Credentials are checked in order in which each is specified:
 - 1) Local LDAP credential pair - if specified, only one tried
 - 2) Default LDAP Credential Pair - if specified, and no Local LDAP credential pair, only one tried
 - 3) Server - if neither Local LDAP credential pair nor default LDAP credential pair specified, first tried
 - 4) `anonymous` - last tried only if server fails or none specified
- If a URL has a Local LDAP credential pair specified, it is used first; if the access fails, access is denied.
- If a URL has no Local LDAP credential pair specified, the corresponding default LDAP credential pair is used; if access fails, then access is denied.

Messaging Server configutil Options for SMIME

Oracle Communications Messaging Server configutil Options for S/MIME

To set the three Messaging Server options that apply to S/MIME, do the following on the machine where Messaging Server is installed.

To Set Messaging Server configutil Options for S/MIME

1. Log in as `root`.
2. Change to the `sbin` directory.

```
# cd <msg-svr-base>/sbin
```

where *msg-svr-base* is the directory where Messaging Server is installed.

3. Set the Messaging Server options, described in the following table, as desired for your system. Use the `configutil` utility to set them. Unless stated otherwise, an option is not required to be set.

configutil Options for S/MIME

Parameter	Purpose
local.webmail.cert.enable	<p>Controls whether the process that handles CRL checking should do CRL checking.</p> <p>0 - The process does not check a certificate against a CRL. This is the default.</p> <p>1 - The process checks a certificate against a CRL. When set to 1, ensure that the <code>crlenable</code> parameter in the <code>smime.conf</code> file is set to 1.</p>
local.webmail.cert.port	<p>Specifies a port number on the machine where the Messaging Server runs to use for CRL communication. This port is used locally for that machine only. The value must be greater than 1024. The default is 55443.</p> <p>This is a required option if the default port number is already in use.</p>
local.webmail.smime.enable	<p>Controls whether the S/MIME features are available to Convergence Mail users. Choose one of these values:</p> <p>0 - the S/MIME features are unavailable for Convergence Mail users even though the system is configured with the correct software and hardware components. This is the default.</p> <p>1 - the S/MIME features are available to Convergence Mail users who have permission to use them.</p> <p>Example: <code>configutil -o local.webmail.smime.enable -v 1</code></p>

Messaging Server smime.conf Parameters

smime.conf Parameters in Oracle Communications Messaging Server

The `smime.conf` file is included with the Messaging Server. The file is located in the directory `msg-svr-base/config/`, where `msg-svr-base` is the directory where Messaging Server is installed. All text and parameter examples in the file are preceded with a comment character (`#`).

You can add parameters with your values to the `smime.conf` file or you can edit the parameter examples. If using an example, copy the example to another part of the file, edit the parameter's value, and remove the `#` character at the beginning of the line.

Edit `smime.conf` with any available text editor after you install Messaging Server. The parameters, described in [the following table](#), are not case sensitive and unless otherwise stated, are not required to be set.

S/MIME Configuration Parameters in smime.conf File

Parameter	Purpose
<code>alwaysencrypt</code>	<p>Controls the initial setting for whether all outgoing messages are automatically encrypted for all Convergence users with permission to use S/MIME. Each Convergence user can override this parameter's value for their messages by using the check boxes described in Signature and Encryption Check Boxes in Convergence.</p> <p>Choose one of these values:</p> <p>0 - do not encrypt messages. The encryption check boxes within Convergence are displayed as unchecked. This is the default.</p> <p>1 - always encrypt messages. The encryption check boxes within Convergence are displayed as checked.</p> <p>Example:</p> <pre>alwaysencrypt==1</pre>

<p>alwaysign</p>	<p>Controls the initial setting for whether all outgoing messages are automatically signed for all Convergence users with permission to use S/MIME. Each Convergence user can override this parameter's value for their messages by using the check boxes described in Signature and Encryption Check Boxes in Convergence.</p> <p>Choose one of these values:</p> <p>0 - do not sign messages. The signature checkboxes within Convergence are displayed as unchecked. This is the default.</p> <p>1 - always sign messages. The signature checkboxes within Convergence are displayed as checked.</p> <p>Example:</p> <pre>alwaysign==1</pre>
<p>certurl</p>	<p>Specifies the LDAP directory information to locate the public keys and certificates of Convergence users (the LDAP attribute for public keys is <code>usercertificate;binary</code>). See Managing Certificates for SMIME for more information about certificates.</p> <p>This parameter must point to the highest node in the user/group of the LDAP directory information tree (DIT) that includes all users that are being served by the Messaging Server. This is particularly important for sites with more than one domain; the distinguished name must be the root distinguished name of the user/group tree instead of the subtree that contains users for a single domain.</p> <p>This is a required parameter that you must set.</p> <p>Example:</p> <pre>certurl==ldap://mail.siroe.com:389/ou=people,o=siroe.com,o=ugroot</pre>

checkoverssl	<p>Controls whether an SSL communications link is used when checking a key's certificate against a CRL. See Securing Internet Links With SSL for more information.</p> <p>Choose one of these values:</p> <p>0 - do not use an SSL communications link.</p> <p>1 - use an SSL communications link. This is the default.</p> <p>A problem can occur when a proxy server is used with CRL checking in effect. See Proxy Server and CRL Checking.</p>
crlaccessfail	<p>Specifies how long to wait before the Messaging Server attempts to access a CRL after it has failed to do so after multiple attempts. This parameter has no default values.</p> <p>Syntax:</p> <pre>crlaccessfail==number_of_failures:time_period_for_failures:wait_time_before_retry</pre> <p>where:</p> <p><i>number_of_failures</i> is the number of times that the Messaging Server can fail to access a CRL during the time interval specified by <i>time_period_for_failures</i>. The value must be greater than zero.</p> <p><i>time_period_for_failures</i> is the number of seconds over which the Messaging Server counts the failed attempts to access a CRL. The value must be greater than zero.</p> <p><i>wait_time_before_retry</i> is the number of seconds that the Messaging Server waits, once it detects the limit on failed attempts over the specified time interval, before trying to access the CRL again. The value must be greater than zero.</p> <p>Example:</p> <pre>crlaccessfail==10:60:300</pre> <p>In this example, Messaging Server fails 10 times within a minute to access the CRL. It then waits 5 minutes before attempting to access the CRL again. See Trouble Accessing a CRL</p>
crldir	<p>Specifies the directory information where the Messaging Server downloads a CRL to disk.</p> <p>The default is <i>msg-svr-base/data/store/mbboxlist</i>, where <i>msg-svr-base</i> is the directory where Messaging Server is installed. See Using a Stale CRL for more information.</p>

<p>crlenable</p>	<p>Controls whether a certificate is checked against a CRL. If there is a match, the certificate is considered revoked. The values of the <code>send*revoked</code> parameters in the <code>smime.conf</code> file determine whether a key with a revoked certificate is rejected or used by Convergence. See Verifying Private and Public Keys for more information.</p> <p>Choose one of these values:</p> <p>0- each certificate is not checked against a CRL.</p> <p>1- each certificate is checked against a CRL. This is the default. Ensure that the <code>local.webmail.cert.enable</code> option of the Messaging Server is set to 1, otherwise CRL checking is not done even if <code>crlenable</code> is set to 1.</p>
<p>crlmappingurl</p>	<p>Specifies the LDAP directory information to locate the CRL mapping definitions. This parameter is only required when you have mapping definitions. See Accessing a CRL optionally add the DN and password that has access to the URL.</p> <p>Syntax:</p> <pre>crlmappingurl URL [URL_DN URL_password]</pre> <p>Example:</p> <pre>crlmappingurl==ldap://mail.siroe.com:389/ cn=XYZ Messaging, ou=people, o=mail.siroe.com,o=isp?msgCRLMappingRecord?sub? (objectclass=msgCRLMappingTable) cn=Directory Manager pAsSwOrD</pre>
<p>crlurllogindn</p>	<p>Specifies the distinguished name of the LDAP entry that has read permission for the CRL mapping definitions (not if the entry is directly from the certificate, see Accessing a CRL).</p> <p>If values for <code>crlllogindn</code> and <code>crllloginpw</code> are not specified, the Messaging Server uses the log in values for the HTTP server to gain entry to the LDAP directory. If that fails, Messaging Server attempts to access the LDAP directory anonymously.</p> <p>Example:</p> <pre>crlllogindn==cn=Directory Manager</pre>

<p><code>crlurlloginpw</code></p>	<p>Specifies the password, in ASCII text, for the distinguished name of the <code>crllogindn</code> parameter.</p> <p>If values for <code>crllogindn</code> and <code>crlloginpw</code> are not specified, Messaging Server uses the log in values for the HTTP server to gain entry to the LDAP directory. If that fails, Messaging Server attempts to access the LDAP directory anonymously. The value may be obfuscated with base64 by using <code>\$==</code> instead of <code>==</code> as the delimiter (this feature was introduced in Messaging Server 7 Update 1). Example:</p> <pre> crlloginpw==zippy or crlloginpw\$==emlwcHk= </pre>
<p><code>crlusepastnextupdate</code></p>	<p>Controls whether a CRL is used when the current date is past the date specified in the CRL's next-update field. See Using a Stale CRL for more information.</p> <p>Choose one of these values:</p> <p>0 - do not use the stale CRL.</p> <p>1 - use the stale CRL. This is the default.</p>
<p><code>logindn</code></p>	<p>Specifies the distinguished name of the LDAP entry that has read permission for the public keys and their certificates, and the CA certificates located in the LDAP directory specified by the <code>certurl</code> and <code>trustedurl</code> parameters.</p> <p>If values for <code>logindn</code> and <code>loginpw</code> are not specified, the Messaging Server uses the log in values for the HTTP server to gain entry to the LDAP directory. If that fails, Messaging Server attempts to access the LDAP directory anonymously. Example:</p> <pre> logindn==cn=Directory Manager </pre>

loginpw	<p>Specifies the password, in ASCII text, for the distinguished name of the <code>logindn</code> parameter.</p> <p>If values for <code>logindn</code> and <code>loginpw</code> are not specified, Messaging Server uses the log in values for the HTTP server to gain entry to the LDAP directory. If that fails, Messaging Server attempts to access the LDAP directory anonymously. The value may be obfuscated with base64 by using <code>\$==</code> instead of <code>==</code> as the delimiter (this feature was introduced in Messaging Server 7 Update 1).</p> <p>Example:</p> <pre>loginpw==SkyKing or loginpw\$==U2t5S2luZw==</pre>
platformwin	<p>Specifies one or more library names that are necessary when using smart cards or a local key store on a Windows platform. Change this parameter only if the default value does not work for your client machines. The default is:</p> <pre>platformwin==CAPI:library=capibridge.dll;</pre> <p>See Key Access Libraries for the Client Machines for more information.</p>
readsigncert	<p>Controls whether a public key's certificate is checked against a CRL to verify an S/MIME digital signature when the message is read. (A private key is used to create a digital signature for a message but it cannot be checked against a CRL, so the certificate of the public key associated with the private key is checked against the CRL.) See Verifying Private and Public Keys</p> <p>Choose one of these values:</p> <p>0 - do not check the certificate against a CRL.</p> <p>1 - check the certificate against a CRL. This is the default.</p>
revocationunknown	<p>Determines the action to take when an ambiguous status is returned when checking a certificate against a CRL. In this case, it is not certain whether the certificate is valid or has a revoked status. See Verifying Private and Public Keys for more information.</p> <p>Choose one of these values:</p> <p>ok - treat the certificate as valid.</p> <p>revoked - treat the certificate as revoked. This is the default.</p>

sendencryptcert	<p>Controls whether the certificate of a public key that is used to encrypt an outgoing message is checked against a CRL before using it. See Verifying Private and Public Keys.</p> <p>Choose one of these values:</p> <p>0 - do not check the certificate against a CRL.</p> <p>1 - check the certificate against a CRL. This is the default.</p>
sendencryptcertrevoked	<p>Determines the action to take if the certificate of a public key that is used to encrypt an outgoing message is revoked. See Verifying Private and Public Keys for more information.</p> <p>Choose one of these values:</p> <p>allow - use the public key.</p> <p>disallow - do not use the public key. This is the default.</p>
sendsigncert	<p>Controls whether a public key's certificate is checked against a CRL to determine if a private key can be used to create a digital signature for an outgoing message. (A private key is used for a digital signature but it cannot be checked against a CRL, so the certificate of the public key associated with the private key is checked against the CRL.) See Verifying Private and Public Keys for more information.</p> <p>Choose one of these values:</p> <p>0 - do not check the certificate against a CRL.</p> <p>1 - check the certificate against a CRL. This is the default.</p>
sendsigncertrevoked	<p>Determines the action to take when it is determined that a private key has a revoked status. (A private key is used to create a digital signature for a message but it cannot be checked against a CRL, so the certificate of the public key associated with the private key is checked against the CRL. If the public key certificate is revoked, then its corresponding private key is also revoked.) See Verifying Private and Public Keys for more information.</p> <p>Choose one of these values:</p> <p>allow - use the private key with a revoked status.</p> <p>disallow - do not use the private key with a revoked status. This is the default.</p>

<p>sslrootcacertsurl</p>	<p>Specifies the distinguished name and the LDAP directory information to locate the certificates of valid CAs which are used to verify the Messaging Server's SSL certificates. This is a required parameter when SSL is enabled in the Messaging Server. See Securing Internet Links With SSL for more information.</p> <p>If you have SSL certificates for a proxy server that receives all requests from client application, the CA certificates for those SSL certificates must also be located in the LDAP directory pointed to by this parameter.</p> <p>You can also optionally add the DN and password that has access to the URL. Syntax:</p> <p>crlmappingurl URL [URL_DN URL_password]</p> <p>Example:</p> <pre> sslrootcacertsurl==ldap://mail.siroe .com:389/cn=SSL Root CA Certs,ou=people,o=siroe.com,o=isp? cacertificate; binary?base? (objectclass=certificationauthority) cn=Directory Manager pAsSwOrD </pre>
<p>timestampdelta</p>	<p>Specifies a time interval, in seconds, that is used to determine whether a message's sent time or received time is used when checking a public key's certificate against a CRL.</p> <p>The parameter's default value of zero directs Convergence to always use the received time. See Determining Which Message Time to Use for more information. Example:</p> <pre>timestampdelta==360</pre>

<p>trustedurl</p>	<p>Specifies the distinguished name and LDAP directory information to locate the certificates of valid CAs. This is a required parameter.</p> <p>You can also optionally add the DN and password that has access to the URL. Syntax:</p> <p><code>crlmappingurl URL [URL_DN URL_password]</code></p> <p>Example:</p> <pre>trustedurl==ldap://mail.siroe .com:389/cn=Directory Manager, ou=people, o=siroe.com,o=ugroot?cacertificate?sub? (objectclass=certificationauthority) cn=Directory Manager pAsSwOrD</pre>
<p>usercertfilter</p>	<p>Specifies a filter definition for the primary, alternate, and equivalent email addresses of a Convergence user to ensure that all of a user's private-public key pairs are found when they are assigned to different mail addresses.</p> <p>This parameter is required and has no default values.</p>

Chapter 7. Configuring Horizontal Scalability for Personal Address Book

Configuring Horizontal Scalability for Personal Address Book

Convergence server enables you to scale and support large number of users. Convergence server stores the information of a user's personal address book in the User/Group LDAP. This attribute is denoted by the `psRoot` attribute.

The `psRoot` is an attribute in the user's LDAP that specifies the host of the LDAP server, the port it is listening to port, and the DN where the Address Book entries for the user is stored. `psRoot` is in the form: `ldap://ldap_host:ldap_port/DN`. The value of `psRoot` attribute determines the DB type and DB location.

Here is an example of how a `psRoot` attribute looks in a user's LDAP entry:

```
ldap://siroe.com:389/pipStoreOwner=jsmith,o=siroe.com,o=PiServerDb
```

Where:

- `siroe.com:389` is the hostname and port number of the LDAP server. In this example, the LDAP server listens to port 389.
- `pipStoreOwner=jsmith,o=siroe.com,o=PiServerDb` specifies the DB of the Personal Store.



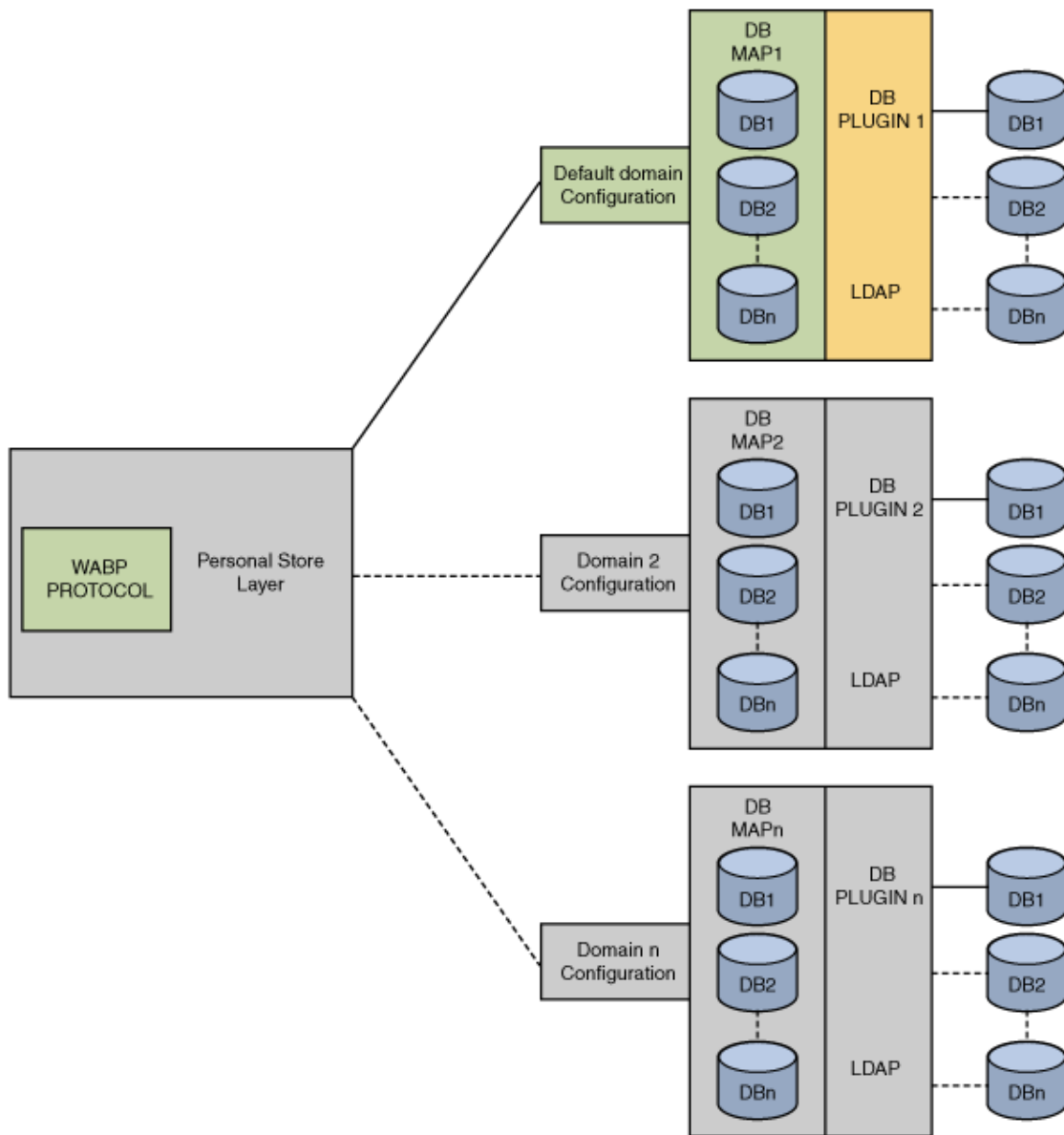
Note

The Address Book Server does not provide any utility to distribute `psRoot` values for users, according to any scalability policy. Administrators need to set a specific policy suited best for the organization and use custom scripts to set the `psRoot` value for that policy.

Horizontal Scalability Architecture

The following are the key components of the Address Book Horizontal Scalability architecture:

- Personal Store
- DBMap
- DB



A Personal Store stores the address book information of a user. It contains the definition of all the address books that a user has created, along with all the entries in those address books. Personal Stores are represented as URLs, which describe the directory instance in which they are located and the DN within that particular directory instance.

A DBMap is a collection of DBs of the same type.

A DB (DataBase) contains a collection of Personal Stores. The address book can access any number of DBs. Every DB is defined by an identifier in configuration file that defines the connection parameters for that DB. A DB of different type points to different DB locations.

The `psRoot` attribute can be turned on or off using the `iwadmin` command-line interface by setting the `ab.useuserspsroot` to `false`. If set to `false`, Convergence uses the `DefaultServer` value that is set in the Convergence configuration.

Set the parameter to `true` to use the user's `psRoot` value. At runtime, the value of `psRoot` attribute is resolved to a directory instance using `ldaphost` and `ldapport`. Based on `ldaphost` and `ldapport`, the Identifier to the database will be resolved. Here Identifier is an arbitrary string that distinguishes one instance from the other.

Setting the psRoot Value Automatically

When a new user logs in, default values are set for the `psRoot` attribute in the user's entry. For new users, a `psRoot` value is constructed by using the `psRoot` pattern and `DefaultServer` defined in the default configuration. For example, when you use the default `psRoot` pattern, the default `psRoot` value is in the format:

```
ldap://<default_server_host>:<port>/piPStoreOwner=%U,o=%D,o=PiServerDb
```

where:

- `%U` is the login ID of the user. For example, `jsmith`.
- `%D` is the domain of the user. For example `siroe.com`.

The following is an example of how to configure horizontal scalability of address book in a deployment where there are two directory servers: `ds1.siroe.com`.

Use following commands to enable horizontal scalability:

To configure personal address book to use directory server `ds1.siroe.com`:

```
iwcadmin -o ab.pstore.[psidentifier1].ldaphost -v ds1.siroe.com
iwcadmin -o ab.pstore.[psidentifier1].ldapport -v 389
iwcadmin -o ab.pstore.[psidentifier1].ldapbinddn -v "cn=Directory
Manager"
iwcadmin -o ab.pstore.[psidentifier1].ldapbindcred -v abbbbc
```

To configure personal address book to use directory server `ds2.siroe.com`:

```
iwcadmin -o ab.pstore.[psidentifier2].ldaphost -v ds2.siroe.com
iwcadmin -o ab.pstore.[psidentifier2].ldapport -v 389
iwcadmin -o ab.pstore.[psidentifier2].ldapbinddn -v "cn=Directory
Manager"
iwcadmin -o ab.pstore.[psidentifier2].ldapbindcred -v aaaaabbbb
```

To enable horizontal scalability, you must set the `ab.useuserpsroot` configuration parameter to `true`:

```
iwcadmin -o ab.useuserpsroot -v true
```

To set the `defaultserver`, you must set the `ab.pstore.defaultserver` configuration parameter to the personal store identifier:

```
iwcadmin -o ab.pstore.defaultserver -v psidentifier2
```

When a new user logs in, default values are set for the `psRoot` attribute in the user's entry. In above example `psidentifier2` is default server. If `psRoot` attribute is not present, `ds2.siroe.com` will be used for personal address book.

Chapter 8. Convergence Address Book JMQ Notification

Convergence Address Book JMQ Notification

Convergence provides a notification module that enables administrators to plug-in a JMS based notification service. The notification module publishes messages to the configured JMS brokers.

Convergence provides a notification service for the Personal Address Book (PAB). The notification module publishes notification messages to a JMS broker when certain state changes occur in a user's PAB. The notification messages are published on a JMS topic or a queue that can be consumed by an appropriate consumer.

This technical note provides an overview of Convergence's address book notification service and provides information about how to configure the notification service.

This article contains the following sections:

- [Convergence Address Book JMQ Notification](#)
 - [Prerequisites for Setting up the Notification Service](#)
 - [Configuring Convergence](#)
 - [Message Queue Notification Service Configuration](#)
 - [Notification Strategies](#)
 - [Setting Event Notification Triggers](#)
 - [Configuring GlassFish Server](#)
 - [Troubleshooting the Notification Service](#)
 - [Data Format used for Notification Service](#)
 - [Message Format: Create Contact](#)
 - [Message Format: Modify Contact](#)
 - [Message Format: Delete Contact](#)
 - [Message Format: Create Contact Photo](#)

Prerequisites for Setting up the Notification Service

This section provides information on the prerequisites for the working with this feature. The administrator must have working knowledge of the following products and technologies:

- Administration knowledge of GlassFish Server - The administrator must create the JMS-based connection factories and destination resources.
- Convergence Administration - The administrator must have working knowledge of administering Convergence. See [Convergence Administration Guide](#) for more information on how to administrate Convergence.

Configuring Convergence

This section contains the following topics:

- [Message Queue Notification Service Configuration](#)
- [Message Format: Create Contact](#)
- [Message Format: Modify Contact](#)
- [Message Format: Delete Contact](#)

- [Message Format: Create Contact Photo](#)

To configure Convergence for address book notification service, you must perform the following high-level steps:

1. Set up the message queue notification service configuration parameters.
2. Choose a notification strategy.
3. Set the Convergence configuration parameters to set notifications.

Message Queue Notification Service Configuration

To make use of the notification service in Convergence, you must first enable Convergence to use the notification service. To do this, enable the following Convergence parameters.

- `notify.service.enable` - Set this parameter to `true` to enable the notification service.

```
# iwadmin -o notify.service.enable -v true
```

The address book notification service publishes notifications to multiple destinations. The destination can be a topic or a queue. Each destination is uniquely identified by a service name. The service name is then resolved Convergence and the notifications are sent to the destination based on the destination type, destination name, and the connection attributes of the service name.

The service name is any unique string. The service name acts as an identifier for a particular destination. For each service name, the various attributes such as the destination type, destination name, and the connection attributes must be set.

- `notify.mq.[serviceName].enable`:
Set this parameter to `true` to enable the notification service for a destination.
For example:

```
# iwadmin -o notify.mq.[serviceName1].enable -v true
```

- `notify.mq.[serviceName].destinationtype`
For each destination, the destination type must be set. The valid values are: `TOPIC` or `QUEUE`.
For example:

```
# iwadmin -o notify.mq.[serviceName1].destinationtype -v TOPIC
```

- `notify.mq.[serviceName].destinationname`
The destination name. This name must match the corresponding JMS connection in the GlassFish Server.
For example:

```
# iwadmin -o notify.mq.[serviceName1].destinationname -v  
destinationName1
```

- `notify.mq.[serviceName].connection`
Connection attribute.

```
# iwadmin -o notify.mq.[serviceName1].connection -v  
<JMS_connection_factory>
```


- `notify.mq.[serviceName1].resourcetype`

This parameter was introduced in **Convergence 3.0.0.0.0**.

Specifies the `resourcetype` and needs to be set to "producer" for address book notifications to work

```
# iwadmin -o notify.mq.[serviceName1].resourcetype -v producer
```

If you do not set this parameter, address book notifications do not work as expected, beginning with Convergence 3.0.0.0.0.

 **Note**


The values for the `destinationtype`, `destinationname`, and `connection` must be the same as the settings for the JMS resources: Connection Factory and JMS resources when configuring GlassFish Server.

Notification Strategies

Convergence provides various notification strategies. You can employ a notification strategy based on how you want to publish and broadcast the notifications. You can set up the following types of notification strategies:

- **User Specific Notification**

Use the user specific notification strategy to trigger notifications to be published based on the state changes of particular contacts in your address books. To enable notification for a per-user, you must set the `abEventNotificationDestination` attribute in the user's LDAP entry to the name of the destination to which the notifications must be published.

 **Note**

The user must have the `SunUCPreferences` object class available in the LDAP.

- **Notification for All Users**

To enable notification for all users, you must set the following parameters:

- - `ab.pstore.notification.destination`
 - `ab.pstore.notification.notifyall`

- **Domain Based Configuration**

If you want to trigger notifications to be published based on the domains, you must set the appropriate domain level attributes.

For example:

```
# iwcaadmin -o ab.{siroe.com}.psrootpattern -v
ldap:///piPStoreOwner=%U,o=%D,o=PiServerDb
# iwcaadmin -o ab.{siroe.com}.pstore.defaultserver -v myldap
# iwcaadmin -o ab.{siroe.com}.pstore.[myldap].ldaphost -v
newLdap.siroe.com
# iwcaadmin -o ab.{siroe.com}.pstore.[myldap].ldapport -v 389
# iwcaadmin -o ab.{siroe.com}.pstore.[myldap].ldapbinddn -v
'cn=Directory Manager'
# iwcaadmin -o ab.{siroe.com}.pstore.[myldap].ldapbindcred -v
<password>
```

The following example shows how to set domain level notifications. In this example, the triggers have been set on the Create Contact, Create Contact Photo, Delete Contact, and Modify Contact actions. You can set the triggers based on your requirements.

```
# iwcaadmin -o ab.{siroe.com}.pstore.notification.destination -v
serviceName1
# iwcaadmin -o ab.{siroe.com}.pstore.notification.event.createcontact -v
true
# iwcaadmin -o
ab.{siroe.com}.pstore.notification.event.createcontactphoto -v true
# iwcaadmin -o ab.{siroe.com}.pstore.notification.event.deletecontact -v
true
# iwcaadmin -o ab.{siroe.com}.pstore.notification.event.modifycontact -v
true
# iwcaadmin -o ab.{siroe.com}.pstore.notification.notifyall -v true
```



Note

You must restart the GlassFish Server on which Convergence is deployed, after making the configuration changes.

Setting Event Notification Triggers

The following types of notification triggers are provided by Convergence:

Table 1-1 : Notification Triggers

Notification Trigger	Configuration Parameter	Description
Create Contact	<code>ab.pstore.notification.event.createcontact</code>	This parameter, when set to <code>true</code> , triggers a notification when a new contact is created.
Delete Contact	<code>ab.pstore.notification.event.deletecontact</code>	This parameter, when set to <code>true</code> triggers a notification when a contact is deleted.
Modify Contact	<code>ab.pstore.notification.event.modifycontact</code>	This parameter, when set to <code>true</code> , triggers a notification when a contact is modified.
Create Contact Photo	<code>ab.pstore.notification.event.createcontactphoto</code>	This parameter, when set to <code>true</code> triggers a notification when a user adds a photo for a contact.

Configuring GlassFish Server

This section provides information about the various configuration steps that need to be performed in GlassFish for the notification service to work. The JMS connection factory and destination resources must be set.

The following examples show how to create the JMS connection factory and destination resources. You can create these either using the `asadmin` command line utility or by using the Admin Console.

1. Create the JMS Connection Factory.

```
# /opt/glassfish3/bin/asadmin --user admin --port 4848
--passwordfile /export/pass create-jms-resource --restype
javax.jms.TopicConnectionFactory --description "example of creating
a JMS connection factory" jms/ConnectionFactory
```

i To configure the JMS connection factory on a remote host, set the appropriate remote host options. Otherwise, the remote host will not receive JMS messages. For more information on setting remote host options, refer to the GlassFish Server help: `asadmin create-jms-resource - help`.

2. Create the JMS Destination Queue.

```
# /opt/glassfish3/bin/asadmin --user admin --port 4848
--passwordfile /export/pass create-jms-resource --restype
javax.jms.Queue jms/Queue
```

3. Create the JMS Destination Topic.

```
# /opt/glassfish3/bin/asadmin --user admin --port 4848
--passwordfile /export/pass create-jms-resource --restype
javax.jms.Topic jms/Topic
```

Troubleshooting the Notification Service

When configuring Convergence for notification, use the notification log levels to troubleshoot any problems that you encounter when working with this feature. You can set the log levels for the notification service. Using the `iwcadmin` command, you can set the logging levels for the `log.NOTIFY.level` parameter. For the list of values that this parameter accepts, see [Convergence Administrative Tasks](#).

Data Format used for Notification Service

This section provides information about the format in which data is passed over as part of the notification message. The notification message must be used by the consumers of the notification service. The notification message contains the vCard of the user along with the following details:

- message
- domain
- bookid
- timestamp
- uid
- operation
- entryid

Message Format: Create Contact

The following is the data format of the notification sent when a new contact is created:

```

Message:BEGIN:VCARD
VERSION:3.0
PROFILE:VCARD
PRODID:Sun Address Book
UID:
FN:user1
N:d;user1;;;
NICKNAME:
ORG:siroe;
TITLE:Mr
ANNIVERSARYDATE:--
BDAY:--
TEL;TYPE=WORK,PREF:
TEL;TYPE=HOME:
TEL;TYPE=CELL:
TEL;TYPE=PAGER:
TEL;TYPE=FAX:
EMAIL;TYPE=INTERNET;TYPE=WORK;TYPE=PREF:user1@siroe.com
EMAIL;TYPE=INTERNET;TYPE=HOME:
EMAIL;TYPE=INTERNET;TYPE=OTHER:
ADR;TYPE=HOME:;;;;
ADR;TYPE=WORK:;;;;
ADR;TYPE=OTHER:;;;;
NOTE:
URL;TYPE=HOME:
URL;TYPE=WORK:
X-IMADDR1:
X-IMSERVICE1:SunIM
X-IMADDR2:
X-IMSERVICE2:AIM
CALURI:
FBURL:
END:VCARD

domain siroe.com
bookid e11dbf2a4c610
timestamp 20090524T205226Z
uid ngc5
operation CreateContact
entryid e12174653ce40

```

Message Format: Modify Contact

The following is the data format of the notification sent when a contact information is modified:

```

Modify Contact:
=====
Message: BEGIN:VCARD
VERSION:3.0
PROFILE:VCARD
PROPID:Sun Address Book
UID:e1218771a5d22
FN:user1 d
N:d;user1;;;
NICKNAME:
ORG:sun;
TITLE:mts
ANNIVERSARYDATE:--
BDAY:--
TEL;TYPE=WORK,PREF:
TEL;TYPE=HOME:
TEL;TYPE=CELL:
TEL;TYPE=PAGER:
TEL;TYPE=FAX:
EMAIL;TYPE=INTERNET;TYPE=WORK;TYPE=PREF:user2@siroe.com
EMAIL;TYPE=INTERNET;TYPE=HOME:user2@siroe.com
EMAIL;TYPE=INTERNET;TYPE=OTHER:
ADR;TYPE=HOME:;;;;;
ADR;TYPE=WORK:;;;;;
ADR;TYPE=OTHER:;;;;;
NOTE:
URL;TYPE=HOME:
URL;TYPE=WORK:
X-IMADDR1:
X-IMSERVICE1:SunIM
X-IMADDR2:
X-IMSERVICE2:AIM
CALURI:
FBURL:
END:VCARD

domain siroe.com
bookid e11dbf2a4c610
timestamp 20090524T205309Z
uid ngc5
operation ModifyContact
entryid e12174653ce40

```

Message Format: Delete Contact

The following is the data format of the notification sent when a contact is deleted:

```
Delete Contact:
=====
Message: null
domain siroe.com
bookid e11dbf2a4c610
timestamp 20090524T205425Z
uid ngc5
operation DeleteContact
entryid e121746661f21
```

Message Format: Create Contact Photo

The following is the data format of the notification sent when a photo is assigned to a contact:

```
Message:
R0lGODlhMgArAHAAACH/C05FVFNDQVBFMi4wAwEAAAAh/glnaWY0ajEyMTYAIfkEBSAABwAsAAZ
siroe.com
bookid e1223b29da380
timestamp 20090702T111156Z
uid ngc2
operation SetContactPhoto
entryid e1223b29daad1
```


Chapter 9. Convergence Reference

Convergence Configuration Properties Reference

This information lists all the configuration parameters that are available in Convergence. Each parameter is described with its name and a description of its purpose. You must use the configuration command-line utility, `iwcadmin` to update the configuration properties for your deployment. To know more about how to use the `iwcadmin` command, see [Overview of the Convergence Command-Line Utility](#).

Whenever you make changes to the configuration files, you must stop and restart the client software because the configuration files are only read at startup. The client restart is required so that the changes you have made to take effect. This information contains the following sections:

- [Global Configuration Properties for Convergence Server](#)
- [LDAP User and Group Configuration Properties for the Convergence Interface](#)
- [Authentication Configuration Properties for Convergence](#)
- [Mail Service Configuration Properties for the Convergence Interface](#)
- [Logging Configuration Properties for the Convergence Interface](#)
- [Calendar Service Configuration Properties for the Convergence Interface](#)
- [CalDAV Service Configuration Properties for the Convergence Interface](#)
- [Indexing and Search Service Configuration Properties for the Convergence Interface](#)
- [Address Book Configuration Properties for the Convergence Interface](#)
- [Deployment Specific Customizable Client Options for the Convergence Interface](#)
- [Admin Service Configuration Properties for the Convergence Interface](#)
- [Single-Sign-On Configuration Properties for the Convergence Interface](#)
- [Instant Messaging Configuration Properties for the Convergence Interface](#)
- [SMIME Configuration Properties for Convergence](#)
- [User Preferences Configuration Properties for the Convergence Interface](#)
- [Address Book JMQ Configuration Properties](#)

When you configure Convergence using the configuration utility, most of the parameters are assigned default values. You can change the default values depending on the changing business needs for your site. You can use the `iwcadmin` command to get the values that are assigned to any of the parameters.

```
iwcadmin -o <parametername>
```

**Note**

In the following configuration properties tables, the Command-Line Option Name found in the left column is the name you put in the `-o` option in the `iwadmin` command-line utility. The property name shown in the right column is how the property is represented in the configuration file. Do not use the property name from the right column for the `-o` option. In addition, the right column is a definition for the option, containing the following details: the name of the property found in the configuration file, the data type for the expected value, the default value if any, whether or not this property is mandatory for proper configuration, and whether or not this property was set by the initial configuration program.

Unless specified, these parameters have a PUBLIC access type. Any RESTRICTED access types are for properties that perform special bulk updates. Use properties with RESTRICTED access types cautiously.

Global Configuration Properties for Convergence Server

This section contains the global configuration properties that define your deployment.

Command-Line Option Name	Description
base.defaultdomain	Default domain to use for user resolution <ul style="list-style-type: none"> • Allowed Pattern/Values: <code>[A-Za-z0-9\-]+\.[A-Za-z0-9\-]+\.</code> • Data Type: String
base.loginseparator	Character to be used as login separator (between userID and domain). It should match any one of the character defined in <code>service.loginseparator</code> of mail and calendar backend service <ul style="list-style-type: none"> • Allowed Pattern/Values: a character • Data Type: String • Default value: <code>@</code>
base.defaultlocale	Default locale to be used <ul style="list-style-type: none"> • Default value: <code>en_us</code> • Data Type: String
base.passivatesession	Enabling this option will allow web container to passivate all active sessions else all active session will be terminated upon session activation event. While typically run in a cluster, this parameter can also be enabled in a non-cluster environment. <ul style="list-style-type: none"> • Default value: <code>false</code> • Data Type: boolean • Allowed Pattern/Values: <code>true</code> or <code>false</code>

base.enablehosteddomain	<p>Whether hosted domains is enabled</p> <ul style="list-style-type: none"> • Data Type: boolean • Allowed Pattern/Values: true or false • Default value: true
base.port	<p>Port number at which the application listens</p> <ul style="list-style-type: none"> • Default value: 8080 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
base.sslport	<p>SSL Port number at which the application listens</p> <ul style="list-style-type: none"> • Default value: 8181 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
base.enableauthonlyssl	<p>SSL can be used only for authentication and the subsequent access via non-ssl</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
base.ipaccessurl	<p>The access URL for this application. The URL must use IP address instead of host name. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default value: null • Allowed Pattern/Value: scheme://IPv4 or IPv6 address:<port> (example: [http://123.456.789.12:8080]) • Data Type: String
base.ipsecurity.enable	<p>IP address along with the token is used for authorization if set to true</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: true or false • Default value: false • Data Type: boolean
base.ignoreurldomain	<p>Prevents the use of the URL domain. Introduced in Convergence 2 Patch 2</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Value: true or false
base.authcookiepath	<p>Cookie path for authorization cookie.</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String

LDAP User and Group Configuration Properties for the Convergence Interface

This section contains the LDAP User and Group configuration properties.

Command-Line Option Name	Description
ugldap.schemaversion	<p>Schema level used by the deployment</p> <ul style="list-style-type: none"> • Default value: 1 • Allowed Pattern/Values: 1 or 2 • Data Type: Integer
ugldap.dcroot	<p>Domain component root suffix</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: (.=([,;+].))? • Data Type: String
ugldap.basedn	<p>Base DN to start the user search from</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: (.=([,;+].))? • Data Type: String
ugldap.ugfilter	<p>User/group filter to apply while user lookup</p> <ul style="list-style-type: none"> • Default value: (uid=%U%V) • Data Type: String
ugldap.domainfilter	<p>Domain filter to apply while domain lookup</p> <ul style="list-style-type: none"> • Default value: (&(objectClass=sunManagedOrganization)(!(sunPreferredDomain=%V)(associatedDomain=%V))) • Data Type: String
ugldap.srchopattrs	<p>Comma-separated list of retrievable LDAP operational attributes</p> <ul style="list-style-type: none"> • Default value: *,isMemberOf • Data Type: String
ugldap.host	<p>Host name of the LDAP service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-\-]+\.[A-Za-z0-9\-\-]*(:[1-9][0-9]*)?+(\.[A-Za-z0-9\-\-]+\.[A-Za-z0-9\-\-]*(:[1-9][0-9]*)?) • Data Type: String


ugldap.port	<p>Port number at which LDAP service listens</p> <ul style="list-style-type: none"> • Default value: 389 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
ugldap.enablessl	<p>Whether LDAP is SSL enabled</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values:true or false
ugldap.minpool	<p>Minimum number of connections in LDAP Pool</p> <ul style="list-style-type: none"> • Default value: 1 • Allowed Pattern/Values: Greater than 0 and less than the maxpool • Data Type: Integer
ugldap.maxpool	<p>Maximum number of connections in LDAP Pool</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than 0 and greater than the minpool • Data Type: Integer
ugldap.timeout	<p>LDAP operation timeout in seconds</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ugldap.refreshinterval	<p>Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ugldap.monitoringinterval	<p>Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down</p> <ul style="list-style-type: none"> • Default value: 60 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ugldap.binddn	<p>The admin DN used for creating LDAP connection pool</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].)?) • Data Type: String

ugldap.bindpwd	<p>The admin DN's password</p> <ul style="list-style-type: none"> • Default Value: Not Applicable • Data Type: String
----------------	---

Authentication Configuration Properties for Convergence


This section contains the properties you can use to configure authentication.


Command-Line Option Name	Description
auth.cert.enable	<p>Enables and disables X509 Certificate-based authentication. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
auth.cert.enablefallback	<p>Enables and disables fallback to form-based login. This option should be set in conjunction with auth.cert.enable. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
auth.ldap.enable	<p>This creates default configuration parameters required to enable LDAP authentication mechanism. Specific parameters can further be modified/created using parameter-specific CLI option.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
auth.am.enable	<p>This creates default configuration parameters required to enable AM authentication mechanism. Specific parameters can further be modified/created using parameter-specific CLI option.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false • Access Type: RESTRICTED

auth.opensso.enable	<p>This creates default configuration parameters required to enable OpenSSO Enterprise authentication mechanism. Specific parameters can further be modified/created using parameter-specific CLI option.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false • Access Type: RESTRICTED <div data-bbox="696 403 1378 644" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> Note</p> <p>As of Communications Suite 7 Update 1, support for Sun OpenSSO Enterprise 8.0 has been deprecated. See: Deprecated Support of Access Manager and Sun OpenSSO.</p> </div>
auth.ldap.loginimpl	<p>An implementation of LoginModule interface (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: Not applicable • Data Type: String
auth.ldap.callbackhandler	<p>An implementation of HttpCallbackHandler class, which extends CallbackHandler (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: com.sun.comms.client.security.auth.AppCallbackHandler • Data Type: String
auth.ldap.schemaversion	<p>The value of this should be same as ugliedap.schemaversion</p> <ul style="list-style-type: none"> • Default value: 2 • Allowed Pattern/Values: 1 or 2 • Data Type: Integer
auth.ldap.dcreot	<p>The value of this should be same as ugliedap.dcreot</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String
auth.ldap.basedn	<p>The value of this should be same as ugliedap.basedn</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String

auth.ldap.ugfilter	<p>The value of this should be same as ugldap.ugfilter</p> <ul style="list-style-type: none"> • Default value: (uid=%U%V) • Data Type: String
auth.ldap.domainfilter	<p>The value of this should be same as ugldap.domainfilter</p> <ul style="list-style-type: none"> • Default value: (&(objectClass=sunManagedOrganization)((sunPreferredDomain=%V)(associatedDomain=%V))) • Data Type: String
auth.ldap.host	<p>Host name of the auth LDAP service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-\]+\(\.[A-Za-z0-9\-\-]+\)*(:[1-9][0-9]*)?\+\(\.[A-Za-z0-9\-\-]+\(\.[A-Za-z0-9\-\-]+\)*(:[1-9][0-9]*)?\)* • Data Type: String
auth.ldap.port	<p>Port number at which auth LDAP service listens</p> <ul style="list-style-type: none"> • Default value: 389 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
auth.ldap.enablessl	<p>Whether auth LDAP is SSL enabled</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Values: true or false • Data Type: boolean
auth.ldap.minpool	<p>Minimum number of connections in LDAP Pool</p> <ul style="list-style-type: none"> • Default value: 1 • Allowed Pattern/Values: Greater than 0 and less than maxpool • Data Type: Integer
auth.ldap.maxpool	<p>Maximum number of connections in LDAP Pool</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than 0 and greater than minpool • Data Type: Integer
auth.ldap.timeout	<p>LDAP operation timeout in seconds</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer

auth.ldap.refreshinterval	<p>Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
auth.ldap.monitoringinterval	<p>Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down</p> <ul style="list-style-type: none"> • Default value: 60 • Allowed Pattern/Values: Greater than or equal 1 • Data Type: Integer
auth.ldap.binddn	<p>The admin DN used for creating LDAP connection pool</p> <ul style="list-style-type: none"> • Default value: Not applicable • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String
auth.ldap.bindpwd	<p>The admin DN's password</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
auth.ldap.enableproxyauth	<p>Enables proxy authentication of the user</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
auth.am.loginimpl	<p>An implementation of LoginModule interface (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: com.sun.comms.client.security.auth.modules.impl.SunLDAPLoginModule • Data Type: String
auth.am.callbackhandler	<p>An implementation of HttpCallbackHandler class, which extends CallbackHandler (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: com.sun.comms.client.security.auth.AppCallbackHandler • Data Type: String
auth.am.cookieName	<p>AM cookie name</p> <ul style="list-style-type: none"> • Default value: iPlanetDirectoryPro • Data Type: String

auth.am.cookieDomain	<p>Domain under which AM cookie is valid</p> <ul style="list-style-type: none"> • Default value: .sun.com • Allowed Pattern/Values: No pattern • Data Type: String
auth.am.indexName	<p>Authentication index name</p> <ul style="list-style-type: none"> • Default value: LDAP • Data Type: String
auth.am.realmMode	<p>This parameter is used to determine whether Access Manager is running in Legacy or Realm mode. The value true implies that Access Manager runs in Realm mode.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
auth.opensso.loginImpl	<p>An implementation of LoginModule interface (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: com.sun.comms.client.security.auth.modules.impl.SunOpenSSOLoginModule • Data Type: String
auth.opensso.callbackHandler	<p>An implementation of HttpCallbackHandler class, which extends CallbackHandler (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: com.sun.comms.client.security.auth.AppCallbackHandler • Data Type: String
auth.opensso.cookieName	<p>OpenSSO cookie name</p> <ul style="list-style-type: none"> • Default value: iPlanetDirectoryPro • Data Type: String <div style="background-color: #e1eef6; padding: 10px; margin-top: 10px;"> <p> Note As of Communications Suite 7 Update 1, support for Sun OpenSSO Enterprise 8.0 has been deprecated. See: Deprecated Support of Access Manager and Sun OpenSSO.</p> </div>

auth.opensso.cookieDomain	<p>Domain under which OpenSSO cookie is valid</p> <ul style="list-style-type: none"> • Default value: .sun.com • Allowed Pattern/Values: [A-Za-z0-9\-\+\(\.[A-Za-z0-9\-\+\)]+ • Data Type: String <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 10px; margin-top: 10px;"> <p> Note As of Communications Suite 7 Update 1, support for Sun OpenSSO Enterprise 8.0 has been deprecated. See: Deprecated Support of Access Manager and Sun OpenSSO.</p> </div>
auth.opensso.datastore	<p>Authentication index name</p> <ul style="list-style-type: none"> • Default value: LDAP • Data Type: String
auth.custom.servicename	<p>Name of service for custom authentication module</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
auth.custom.loginimpl	<p>An implementation of LoginModule interface (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
auth.custom.callbackhandler	<p>An implementation of HttpCallbackHandler class, which extends CallbackHandler (JAAS technology in Java). This property refers to a pluggable custom authentication module</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
auth.misc	<p>Placeholder for custom auth provider configuration</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: user-defined-attribute • Data Type: String
auth.adminuserlogin.enable	<p>Whether proxy admins are allowed to login through webclient</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean

Mail Service Configuration Properties for the Convergence Interface

This sections contains the configuration properties for the Mail Service.

Command-Line Option Name	Description
mail.enable	<p>Whether mail service is enabled or not</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
mail.host	<p>Host name of the backend mail service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-\._]+\.[A-Za-z0-9\-\._]* • Data Type: String
mail.port	<p>Port number at which backend mail service listens</p> <ul style="list-style-type: none"> • Default value: 8990 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
mail.enablemsgpreview	<p>Turns on/off the mail preview pane Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default: true • Data Type: boolean • Allowed Pattern/Values: true or false <p>If mail.enablemsgpreview is true, the user's preference (LDAP attribute: nswmExtendedUserPrefs:mePreviewEnabled=<true/false>) is checked and returned accordingly. In other words, the user can disable mail preview pane, even though it is site-enabled. However, if mail.enablemsgpreview is false, the mail preview pane is disabled, irrespective of user preference.</p>
mail.enablessl	<p>Whether mail sevice is SSL enabled</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Values: true or false • Data Type: boolean
mail.requesttimeout	<p>Timeout value in seconds to use if Mail server does not respond within this time. Zero means never timeout</p> <ul style="list-style-type: none"> • Default value: 180 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0

mail.restrictanyone	<p>Mirror option of store.privatesharedfolders.restrictanyone on the Messaging Server</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Values: true or false • Data Type: boolean
mail.cookieName	<p>Cookie name used by mail service as session identifier</p> <ul style="list-style-type: none"> • Default value: webmailsid • Data Type: String
mail.proxyadminid	<p>Backend mail service's proxy admin UID. Used for proxy-auth to mail service. This should be of form: uid@domain if hosted domains setup is used</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
mail.proxyadminpwd	<p>Backend mail service's proxy admin password. Used for proxy-auth to mail service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
mail.uwcsievecompatible	<p>Specifies whether the sieve should be compatible with Communications Express</p> <ul style="list-style-type: none"> • Default value: true • Allowed Pattern/Values: true or false • Data Type: boolean
mail.spam.folder	<p>Spam folder used to move messages marked as spam by the user</p> <ul style="list-style-type: none"> • Default value: spam • Data Type: String
mail.spam.enableaction	<p>Specifies whether Spam Action (ability to mark/unmark messages as spam) should be enabled</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Values: true or false • Data Type: boolean
mail.pop.refreshinterval	<p>Time interval (in sec) for the client to check the external mail server for new messages</p> <ul style="list-style-type: none"> • Default value: 600 • Allowed Pattern/Values: 0-3600 secs • Data Type: Integer

mail.pop.requesttimeout	<p>Time interval (in sec) to wait for the response for POP requests. Zero means never timeout</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 600 • Data Type: Integer
mail.maxpool	<p>Maximum number of connections per route in a pool; this setting can be used when setting up a connection manager. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default: 100 • Data Type: Integer
mail.pooltimeout	<p>Maximum amount of time (in sec) to wait while retrieving a connection from the pool; this setting can be used when setting up a connection manager. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default: 240 • Data Type: Integer

Logging Configuration Properties for the Convergence Interface

This section describes the command-line properties used for configuring logging.

Command-Line Option Name	Description
log.enableusertrace	<p>Specifies whether user ip-address and session-id should be included in the logs. Log pattern must include %X{ipaddress} and %X{sessionid} to complete this functionality.</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: true or false • Default value: true • Data Type: boolean
log.locationtype	<p>Definition for specifying Log Location Type. Currently supported location type: FILE, CONSOLE (aka STDOUT).</p> <ul style="list-style-type: none"> • Default value: CONSOLE • Allowed Pattern/Values: FILE or CONSOLE • Data Type: String
log.location	<p>The Location value is the location of Log file (and hence is applicable only for FILE type)</p> <ul style="list-style-type: none"> • Default value: /data/logs/iwc.log • Data Type: String

log.adminloglocationtype	<p>Log location type for admin log file</p> <ul style="list-style-type: none"> • Default value: FILE • Allowed Pattern/Values: FILE or CONSOLE • Data Type: String
log.adminloglocation	<p>The location of admin log file (and hence is applicable only for FILE type)</p> <ul style="list-style-type: none"> • Default value: /data/logs/iwc_admin.log • Data Type: String
log.sizetrigger	<p>Set the maximum size in KB, that the log file is allowed to reach before being rolled over to backup files</p> <ul style="list-style-type: none"> • Default value: 2048 • Allowed Pattern/Values: Greater than 0 KB • Data Type: Integer
log.timetrigger	<p>The rolling schedule is specified by this pattern. Set the Date pattern at which the log file will be rolled over to backup files</p> <ul style="list-style-type: none"> • Default value: null • Allowed Pattern/Values: This pattern should follow the SimpleDateFormat conventions. For examples and more details, refer to DailyRollingFileAppender documentation in Apache Log4j project. • Data Type: String
log.maxbackupindex	<p>This option determines how many backup files are kept before the oldest is erased. This option takes a positive integer value. If set to zero, then there will be no backup files and the log file will be truncated when it reaches the sizetrigger value. The maxbackupindex option is considered only if sizetrigger is set and is ignored for timetrigger.</p> <ul style="list-style-type: none"> • Default value: 1 • Data Type: Integer
log.pattern	<p>The log record pattern used by the loggers</p> <ul style="list-style-type: none"> • Default value: %c: %p from %C : Thread %t at time %d{HH:mm:ss,SSS} --- %m %n • Allowed Pattern/Values: The pattern is closely related to the conversion pattern of the printf function in C. For detailed patterns, refer to PatternLayout documentation in Apache Log4j project • Data Type: String
log.DEFAULT.level	<p>Level of Logging</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String

log.CONFIG.level	<p>Level of Logging for Config module</p> <ul style="list-style-type: none"> • Default value: WARN • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.AUTH.level	<p>Level of Logging for Auth module</p> <ul style="list-style-type: none"> • Default value: DEBUG • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.PROXY_MAIL.level	<p>Level of Logging for Proxy Mail module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.ADDRESS_BOOK.level	<p>Level of Logging for Address Book module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.PROXY_CAL.level	<p>Level of Logging for Proxy Cal module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.PROTOCOL.level	<p>Level of Logging for Protocol module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.SIEVE.level	<p>Level of Logging for Sieve module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.NOTIFY.level	<p>Level of logging for notification module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
log.ADMIN.level	<p>Level of Logging for Admin module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String

log.PROXY_ISS.level	<p>Level of Logging for ISS(MISO) proxy module</p> <ul style="list-style-type: none"> • Default value: INFO • Allowed Pattern/Values: OFF ERROR WARN INFO DEBUG • Data Type: String
---------------------	--

Calendar Service Configuration Properties for the Convergence Interface

This section describes the command-line properties used for calendar service.

Command-Line Option Name	Description
cal.autoprovision	<p>Determines if calendar auto-provision on the backend Calendar Server is enabled. This option should be set in conjunction with local.autoprovision in Calendar Server 6.x.</p> <p>Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Allowed Pattern/Value: true or false • Default Value: false • Data Type: boolean <p>cal.autoprovision=true (local.autoprovision in Calendar Server 6.x = yes) Calendar Service is enabled to allow for auto-provisioning by Calendar Server (even if user is provisioned by DA as a mail-only user).</p> <p>cal.autoprovision=false (local.autoprovision in Calendar Server 6.x = no) Checks for the presence of icsCalendarUser objectclass and disallows the service if not present. For deployments that provision mail-only users, this option can be used to disable deployment-wide calendar service.</p> <p>Note that the default value changed to false with Convergence 2 Patch 5.</p>
cal.enable	<p>Whether Calendar service is enabled or not</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Values: true or false • Data Type: boolean
cal.host	<p>Host name of the backend Calendar service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-\]+\.[A-Za-z0-9\-\-]* • Data Type: String
cal.port	<p>Port number at which backend Calendar service listens</p> <ul style="list-style-type: none"> • Default value: 80 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer

cal.enablessl	Whether SSL is enabled for calendar service <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
cal.requesttimeout	Timeout value in seconds to use if Calendar server does not respond within this time. Zero means never timeout <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 180 • Data Type: Integer
cal.proxyadminid	Backend Calendar service's proxy admin UID. Used for proxy-auth to cal service. This should be of form: uid@domain if hosted domains setup is used <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
cal.proxyadminpwd	Backend calendar service's proxy admin password. Used for proxy-auth to calendar service <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
cal.maxpool	Maximum number of connections per route in a pool Introduced in Convergence 2 <ul style="list-style-type: none"> • Default: 100 • Data Type: Integer
cal.pooltimeout	Defines the timeout (seconds) used when retrieving a connection from the pool. Introduced in Convergence 2 <ul style="list-style-type: none"> • Default: 240 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 1

CalDAV Service Configuration Properties for the Convergence Interface

This section describes the command-line properties used for CalDAV service. **Introduced in Convergence 2**

Command-Line Option Name	Description
caldav.enable	Whether CalDAV Calendar service is enabled or not <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false

caldav.host	<p>Host name of the backend CalDAV service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-]+\([\.[A-Za-z0-9\-]+\)* • Data Type: String
caldav.port	<p>Port number at which backend CalDAV service listens</p> <ul style="list-style-type: none"> • Default value: 8080 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
caldav.enablessl	<p>Whether SSL should be used against backend CalDAV service</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
caldav.requesttimeout	<p>Timeout value in seconds to use if CalDAV server does not respond within this time. Zero means never timeout</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 180 • Data Type: Integer
caldav.serviceuri	<p>Context URI at which the WCAP interface in CalDAV service is accessible</p> <ul style="list-style-type: none"> • Default value: /wcap • Data Type: String
caldav.proxyadminid	<p>Backend CalDAV service's proxy admin UID. Used for proxy-auth to cal service. This should be of form: uid@domain if hosted domains setup is used</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
caldav.proxyadminpwd	<p>Backend CalDAV service's proxy admin password. Used for proxy-auth to calendar service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
caldav.davuserattr	<p>Attribute name in the user's LDAP entry indicating the user is a CalDAV user in a co-existence deployment</p> <ul style="list-style-type: none"> • Default value: davstore • Data Type: String

caldav.groupobjectclass	<p>objectclass names of groups to be filtered while searching for Corp-Dir groups. The filter matches with any one of the configured objectclass names to retrieve the results</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String
caldav.autoprovision	<p>Whether CalDAV auto-provision in the backend CalDAV Server is enabled or not.</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: true or false • Default value: false • Data Type: boolean
caldav.davuserobjectclass	<p>Name of the LDAP objectclass which should be present for valid CalDAV users if autoprovisioning is disabled</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Name of the LDAP objectclass • Default value: icsCalendarUser • Data Type: String
caldav.wcapversion	<p>WCAP Version of the CalDAV Service</p> <ul style="list-style-type: none"> • Default value: 7.0 • Data Type: String
caldav.maxpool	<p>Maximum number of connections per route in a pool; this setting can be used when setting up a connection manager.</p> <ul style="list-style-type: none"> • Default: 100 • Allowed Pattern/Values: Greater than 0. • Data Type: Integer
caldav.pooltimeout	<p>Defines the timeout (seconds) used when retrieving a connection from the pool.</p> <ul style="list-style-type: none"> • Default: 240 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer

Indexing and Search Service Configuration Properties for the Convergence Interface

This section describes the command-line properties used for Indexing and Search service.

Command-Line Option Name	Description
--------------------------	-------------

ISS.enable	<p>Whether ISS service is enabled or not</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ISS.host	<p>Host name of the backend ISS service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-\]+\.[A-Za-z0-9\-\-]* • Data Type: String
ISS.port	<p>Port number at which backend ISS service listens</p> <ul style="list-style-type: none"> • Default value: 8080 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
ISS.enablessl	<p>Whether SSL is enabled for ISS service</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ISS.requesttimeout	<p>Timeout value in seconds to use if ISS server does not respond within this time. Zero means never timeout</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 180 • Data Type: Integer
ISS.proxyadminid	<p>Backend ISS service's proxy admin UID. Used for proxy-auth to ISS service. This should be of form: uid@domain if hosted domains setup is used</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
ISS.proxyadminpwd	<p>Backend ISS service's proxy admin password. Used for proxy-auth to ISS service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
ISS.maxpool	<p>Maximum number of connections per route in a pool; this setting can be used when setting up a connection manager. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default: 100 • Data Type: Integer

ISS.pooltimeout	<p>Maximum amount of time (in sec) to wait while retrieving a connection from the pool; this setting can be used when setting up a connection manager. Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default: 240 • Data Type: Integer
-----------------	--

Address Book Configuration Properties for the Convergence Interface

This section contains the address book configuration properties used for Convergence.

Command-Line Option Name	Description
ab.expireperiod	<p>WABP Purge, period (in days) after which the entries get deleted permanently. This is applicable only when <code>enableautopurge</code> is set to true</p> <ul style="list-style-type: none"> • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.maxpostlength	<p>Defines the maximum content-length of a POST command. -1 means no limit.</p> <ul style="list-style-type: none"> • Default value: -1 • Allowed Pattern/Values: -1, 0 or greater than 0 • Data Type: Integer
ab.mycontacttag	<p>Tag name for my contact</p> <ul style="list-style-type: none"> • Default value: My Contact • Data Type: String
ab.myfavoritestag	<p>Tag name for my favorites</p> <ul style="list-style-type: none"> • Default value: My Favorites • Data Type: String
ab.maxphotosize	<p>Maximum allowed photo size in bytes</p> <ul style="list-style-type: none"> • Default value: 102400 • Allowed Pattern/Values: Greater than 0 • Data Type: Integer
ab.maxphotowidth	<p>Limit on dimension (width in pixels) of images being served</p> <ul style="list-style-type: none"> • Default value: 2000 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer

ab.maxphotoheight	<p>Limit on dimension (height in pixels) of images being served</p> <ul style="list-style-type: none"> • Default value: 2000 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ab.exportphoto	<p>If this is enabled it exports contacts with photo data in Vcard 3.0 format</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.importphoto	<p>If this is enabled it imports contacts with photo data in Vcard 3.0 format</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.import.vcard.misc	<p>Specify encoding to be used during import corresponding to each locale</p> <ul style="list-style-type: none"> • Default value: UTF-8 • Data Type: String
ab.export.vcard.misc	<p>Specify encoding to be used during export corresponding to each locale</p> <ul style="list-style-type: none"> • Default value: UTF-8 • Data Type: String
ab.maxpagedsearch	<p>Max number of simultaneous paged search for an instance of PersonalStore</p> <ul style="list-style-type: none"> • Default value: 10 • Allowed Pattern/Values: Greater than 1 • Data Type: Integer
ab.retries	<p>Number of retries to fetch default addressbook when a new user logs in</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer

ab.psrootpattern	<p>Defines a default psRoot pattern for users that dont have the psroot attribute. %U = uid of the user ("jsmith"), %D = domain of the user ("somedomain.com"), %O = most significant part of the domain ("somedomain")</p> <ul style="list-style-type: none"> • Default value: ldap:///piPStoreOwner=%U,o=%D,o=PiServerDb • Allowed Pattern/Values: Starts with ldap:// • Data Type: String
ab.ldapdelay	<p>Amount of delay in number of milliseconds to be introduced to compensate delays due to LDAP updates</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.storecachecount	<p>Enable cache entry count</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.storeentrieslimit	<p>Total number of entries allowed in the user's addressbook.</p> <ul style="list-style-type: none"> • Default value: 1000 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.storequotawarn	<p>Indicate whether quota warning can be issued or not. A positive integer greater than zero indicates a warning else no warning.</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 100 • Data Type: Integer
ab.useuserpsroot	<p>Whether the per User psRoot should be used or not</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.pstore.notification.notifyall	<p>Enable address book notification for all users</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false

ab.pstore. notification.event. createcontact	<p>Enable notification for contact creation</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.pstore. notification.event. modifycontact	<p>Enable notification for contact modification</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.pstore. notification.event. deletecontact	<p>Enable notification for contact deletion</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.pstore. notification.event. createcontactphoto	<p>Enable notification for adding contact photo</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
ab.pstore. notification.destination	<p>Comma seperated list of destination. Used only when notify all users is enabled</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String
ab.pstore.[<i>identifier</i>] .ldappoolmin	<p>Minimum connections to the LDAP server</p> <ul style="list-style-type: none"> • Default value: 1 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.pstore.[<i>identifier</i>] .ldappoolmax	<p>Maximum connections to the LDAP server</p> <ul style="list-style-type: none"> • Default value: 4 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.pstore.[<i>identifier</i>] .ldappooltimeout	<p>Max time (in seconds) to wait for a connection to be freed up</p> <ul style="list-style-type: none"> • Default value: 10 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer


<code>ab.pstore.[<i>identifier</i>].ldappoolrefreshinterval</code>	<p>Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
<code>ab.pstore.[<i>identifier</i>].ldappoolmonitoringinterval</code>	<p>Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down</p> <ul style="list-style-type: none"> • Default value: 60 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
<code>ab.pstore.[<i>identifier</i>].ldaphost</code>	<p>Host name of the LDAP service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: <code>[A-Za-z0-9\-\-]+\(\.[A-Za-z0-9\-\-]\+)*</code> • Data Type: String
<code>ab.pstore.[<i>identifier</i>].ldapport</code>	<p>Port number at which LDAP service listens</p> <ul style="list-style-type: none"> • Default value: 389 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
<code>ab.pstore.[<i>identifier</i>].ldapbinddn</code>	<p>The admin DN used for creating LDAP connection pool. This pool will be used for PStore lookup</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: <code>(.*=.*([\+].*)*)?</code> • Data Type: String
<code>ab.pstore.[<i>identifier</i>].ldapbindcred</code>	<p>The admin DN's password, used for creating LDAP connection pool. This pool will be used for PStore lookup.</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
<code>ab.pstore.[<i>identifier</i>].enableldapssl</code>	<p>Enable LDAP SSL</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false

<p><code>ab.pstore.urlmatch</code></p>	<p>Specifies the type of URL this instance of the plugin is responsible for. This value should be unique and is case sensitive.</p> <ul style="list-style-type: none"> • Default value: ldap:// • Allowed Pattern/Values: Starts with ldap:// • Data Type: String
<p><code>ab.pstore.wildcardsearch</code></p>	<p>wildcardsearch specifies the minimum number of characters that need to be provided in a wildcard search. For example, 0 – entry/displayname=*, 1 – entry/displayname=a*</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
<p><code>ab.pstore.randompaging</code></p>	<p>Randompaging true(default), false specifies if the plugin support access to any page, or if each page must be accessed starting at page 1. If false, the coesrv will loop until it gets to the right page.</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
<p><code>ab.pstore.logintype</code></p>	<p>This can be: anon (anonymous), restricted (login as user who has rights to view/write DB), or proxy (login as user that can 'masquerade')</p> <ul style="list-style-type: none"> • Default value: restricted • Allowed Pattern/Values: anon, restricted, or proxy • Data Type: String
<p><code>ab.pstore.defaultserver</code></p>	<p>Default server (identifier) used for construction PSRoot</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String
<p><code>ab.pstore.displayname</code></p>	<p>Display Name for Personal book</p> <ul style="list-style-type: none"> • Default value: Personal Address Book • Data Type: String
<p><code>ab.pstore.description</code></p>	<p>Description for Personal book</p> <ul style="list-style-type: none"> • Default value: This is your personal Address Book • Data Type: String


<p>ab.pstore.getalldbattr</p>	<p>This defines if all the database attributes should be passed in the LDAP search true or false.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
<p>ab.pstore.lookthru limit</p>	<p>This is the max number of entries to read in any one search. Should be set to max in directory or largest AB possible.</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
<p>ab.pstore.deleteperm</p>	<p>Mark the contact/group as deleted instead of permanently deleting it by setting following parameter as false</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
<p>ab.pstore.allowdupentry</p>	<p>Parameter which, if set to true, allows personal address book entries/groups to have the same name</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
<p>ab.pstore.admingroupdn</p>	<p>DN of admin group. If a user belong to this group then he is eligible to purge all user's contacts which are marked for deletion</p> <ul style="list-style-type: none"> • Default value: null • Allowed Pattern/Values: (.*=.*([:,\+].*)*)? • Data Type: String
<p>ab.pstore.collationrule</p>	<p>Locale on whose basis collation rule should be applied for Personal Address Book</p> <ul style="list-style-type: none"> • Default value: en-US • Data Type: String
<p>ab.pstore.collationsearchfield</p>	<p>Search Fields for which collation rule should be applied. The fields provided here should be disambiguator formatted fields. For example, entry/displayname, person/givenname, and so on.</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String

ab.corpdir.[<i>identifier</i>] .ldappoolmin	<p>Minimum connections to the LDAP server</p> <ul style="list-style-type: none"> • Default value: 1 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[<i>identifier</i>] .ldappoolmax	<p>Maximum connections to the LDAP server</p> <ul style="list-style-type: none"> • Default value: 4 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[<i>identifier</i>] .ldappooltimeout	<p>Max time (in seconds) to wait for a connection to be freed up</p> <ul style="list-style-type: none"> • Default value: 10 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[<i>identifier</i>] .ldappoolrefreshinterval	<p>Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required</p> <ul style="list-style-type: none"> • Default value: 0 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[<i>identifier</i>] .ldappoolmonitoringinterval	<p>Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down</p> <ul style="list-style-type: none"> • Default value: 60 • Data Type: Integer • Allowed Pattern/Values: Greater than 0
ab.corpdir.[<i>identifier</i>] .ldaphost	<p>Host name of the LDAP service</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-\-]+\.[A-Za-z0-9\-\-]* • Data Type: String
ab.corpdir.[<i>identifier</i>] .ldapport	<p>Port number at which LDAP service listens</p> <ul style="list-style-type: none"> • Default value: 389 • Data Type: Integer • Allowed Pattern/Values: 0 to 65535
ab.corpdir.[<i>identifier</i>] .ldapbinddn	<p>The admin DN used for creating LDAP connection pool. This pool will be used for corpdir lookup</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String

<p>ab.corpdir.[<i>identifier</i>] .ldapbindcred</p>	<p>The admin DN's password, used for creating LDAP connection pool. This pool will be used for corpdir lookup.</p> <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .enableldapssl</p>	<p>Enable LDAP SSL</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Value: true or false • Data Type: boolean
<p>ab.corpdir.[<i>identifier</i>].enable</p>	<p>Whether corporate directory is enabled or not</p> <ul style="list-style-type: none"> • Default value: true • Allowed Pattern/Value: true or false • Data Type: boolean
<p>ab.corpdir.[<i>identifier</i>] .urlmatch</p>	<p>Specifies the type of URL this instance of the plugin is responsible for. This value should be unique and is case sensitive.</p> <ul style="list-style-type: none"> • Default value: ldap:// • Allowed Pattern/Values: Starts with ldap:// • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .wildcardsearch</p>	<p>wildcardsearch specifies the minimum number of characters that need to be provided in a wildcard search. For example, 0 – entry/displayname=*, 1 – entry/displayname=a*</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
<p>ab.corpdir.[<i>identifier</i>] .randompaging</p>	<p>Randompaging true(default), false specifies if the plugin support access to any page, or if each page must be accessed starting at page 1 If false, the coresrv will loop until it gets to the right page.</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
<p>ab.corpdir.[<i>identifier</i>] .vlvpaging</p>	<p>Use VLV if DB has a VLV set for the default search type</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false

<p>ab.corpdir.[<i>identifier</i>] .logintype</p>	<p>This can be: anon (anonymous), restricted (login as user who has rights to view/write DB), or proxy (login as user that can 'masquerade')</p> <ul style="list-style-type: none"> • Default value: restricted • Allowed Pattern/Values: anon, restricted, or proxy • Data Type: String <div data-bbox="776 373 1357 747" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> Note If you are performing an anonymous search (specifically, ab.corpdir.[<i>identifier</i>].logintype = anon), you need to set the following additional parameters: ab.corpdir.[<i>identifier</i>].ldaphost = <ldaphost> and ab.corpdir.[<i>identifier</i>].ldapport = <ldapport>.</p> </div>
<p>ab.corpdir.[<i>identifier</i>] .searchfilter</p>	<p>Search filter for corporate directory searches. Syntax: (&(&([<i>filter</i>]) ((objectClass= GROUPOFUNIQUE NAMES) (objectClass=GROUPOFURLS) (objectClass= ICSCALENDARRESOURCE) (objectClass= INETORGPERSO N))) (objectClass=*)) , Where [<i>filter</i>] will be replaced with search criteria. Ex: If search criteria is cn=* then [<i>filter</i>] will be replaced with cn=*</p> <ul style="list-style-type: none"> • Default value: null • Allowed Pattern/Values: Refer RFC 2254 • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .vlvfilter</p>	<p>VLV Search filter for corporate directory searches.</p> <ul style="list-style-type: none"> • Default value: null • Allowed Pattern/Values: Refer RFC 2254 • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .vlvsearchbase</p>	<p>VLV search base dn from where the corporate directory vlv searches are performed.</p> <ul style="list-style-type: none"> • Default value: null • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String

<p>ab.corpdir.[<i>identifier</i>] .vlvsortby</p>	<p>VLV sort by fields for performing corporate directory searches. Multiple fields must be comma separated. For example, entry/displayname,person/surname.</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: XPath of sort by attributes. • Multiple fields must be comma separated. For example, XPath for cn is entry/displayname, sn is person/surname. • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .vlvscope</p>	<p>VLV Search scope used for corporate directory searches.</p> <ul style="list-style-type: none"> • Default value: 2 • Allowed Pattern/Values: 0 1 2 • Data Type: Integer
<p>ab.corpdir.[<i>identifier</i>] .defaultserver</p>	<p>Default server (identifier) used for construction PSRoot</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .displayname</p>	<p>Display Name for corp dir</p> <ul style="list-style-type: none"> • Default Value: Corporate Directory • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .description</p>	<p>Description for corporate directory</p> <ul style="list-style-type: none"> • Default Value: This is your Corporate Directory • Data Type: String

<p>ab.corpdir.[<i>identifier</i>] .searchattr</p>	<p>This defines the attributes to be used while obtaining an entry from DB. Provide the attributes as comma-separated. For example: entry/displayname,@uid . This is required especially for contacts and groups which can have different RDN's to identify them.</p> <ul style="list-style-type: none"> • Default value: entry/displayname • Data Type: String <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> Note Convergence can be configured to search corporate directory on required fields.</p> <p>For example, when the search string is "someone" and if you want to search this string only in the uid, set ab.corpdir.[<i>identifier</i>].searchattr to @uid.</p> <p>Contact is represented by XML element <abperson uid="db:uid"></abperson>. The @ symbol is used to represent the attribute in the XML element. For example, the mapping could be something like the following:</p> <ol style="list-style-type: none"> 1. uid @uid 2. displayname entry/displayname 3. givenname person/givenname 4. surname person/surname <p>In above example to refer uid, use @uid. The symbol @ must be used because the uid is attribute of an element.</p> </div>
<p>ab.corpdir.[<i>identifier</i>].groupoc</p>	<p>Comma separated list of objectclasses to identify group entries</p> <p>Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default Value: (objectclass=groupOfUniqueNames) • Data Type: String
<p>ab.corpdir.[<i>identifier</i>] .resourceoc</p>	<p>Comma separated list of objectclasses to identify resource entries</p> <p>Introduced in Convergence 2</p> <ul style="list-style-type: none"> • Default value: (objectclass=ICSCALENDARRESOURCE) • Data Type: String

<code>ab.corpdir.[<i>identifier</i>].getalldbattr</code>	<p>This defines if all the database attributes should be passed in the LDAP search. Valid values are true or false.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
<code>ab.corpdir.[<i>identifier</i>].lookthrlimit</code>	<p>This is the max number of entries to read in any one search. Should be set to max in directory or largest AB possible.</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: 0 or greater • Data Type: Integer
<code>ab.corpdir.[<i>identifier</i>].collationrule</code>	<p>Locale on whose basis collation rule should be applied for Corporate Directory</p> <ul style="list-style-type: none"> • Default Value: en-US • Data Type: String
<code>ab.corpdir.[<i>identifier</i>].collationsearchfield</code>	<p>Search Fields for which collation rule should be applied. The fields provided here should be disambiguator formatted fields. For example, entry/displayname, person/givenname etc.</p> <ul style="list-style-type: none"> • Default Value: null • Data Type: String
<code>ab.purgetype</code>	<p>Enables WABP purge, which permanently deletes entries marked for deletion. If <code>ab.purgetype</code> is <code>auto</code> then purging happens automatically upon login. If <code>ab.purgetype</code> is <code>manual</code> then purging can be done by invoking the <code>purge_entries.wabp</code> command. Introduced in Convergence 1.3 Patch 17</p> <ul style="list-style-type: none"> • Default value: auto • Allowed Pattern/Values: manual auto • Data Type: String • Access Type: RESTRICTED
<code>ab.purgeinterval</code>	<p>When <code>ab.purgetype</code> is set to <code>auto</code>, this parameter specifies the interval (in days) between purges of the database. Introduced in Convergence 1.3 Patch 17</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer

Deployment Specific Customizable Client Options for the Convergence Interface

You can have deployment-specific customizable client options. These options can also be specified on a

per-hosted domain basis.

Deployment Specific Customizable Client Options for Convergence

Command-Line Option Name	Description
client.updateunreadcount	Whether to update unread count for all folders when 'Get Mail' is clicked. Default is false. <ul style="list-style-type: none">• Allowed Pattern/Values: true or false• Default value: false• Data Type: boolean
client.mailcheckinterval	Time interval (in sec) for the client to check the mail server for new messages <ul style="list-style-type: none">• Default value: 300• Allowed Pattern/Values: 0-3600 secs• Data Type: Integer
client.mailautosaveinterval	Time interval (in sec) to auto-save partially composed emails as a draft. This option is to prevent inadvertent loss of a partially composed message <ul style="list-style-type: none">• Default value: 60• Allowed Pattern/Values: 0-600 secs• Data Type: Integer
client.corpabentriesperpage	Default number of entries per page used for corporate directory search. <ul style="list-style-type: none">• Default value: 100• Allowed Pattern/Values: Greater than or equal to 1• Data Type: Integer
client.dictlocale	Default dictionary used by the site for spell check <ul style="list-style-type: none">• Default value: en-US• Data Type: String
client.antispaurl	Site specified service endpoint, which can permit each site to train their anti-spam service to recognize the message as spam in the future <ul style="list-style-type: none">• Default value: /antispa• Data Type: String
client.autologouttime	Timeout period (in min) to auto log off users (by client) after a predefined period of inactivity <ul style="list-style-type: none">• Default value: 15• Allowed Pattern/Values: Greater than or equal to 0• Data Type: Integer

client.smartznames	<p>Site wide defined set of timezones</p> <ul style="list-style-type: none"> • Default value: "" • Data Type: String
client.enablecustomization	<p>Turn on or off customization service</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
client.enablertfcompose	<p>Turn on/off RTF editing for entire deployment. If it set to false then user's preference to enable/disable rtf editing will be ignored by convergence client. The default value is true.</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
client.enablecorpabautocomplete	<p>Turn on/off Auto completion of addresses from Corporate Address Book.</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
client.misc	<p>This facilitates adding custom client preference. For example, misc.{custom-attribute}></p> <ul style="list-style-type: none"> • Allowed Pattern/Values: user-defined-attribute • Data Type: String
client.mainpage	<p>Location of the static html main page</p> <ul style="list-style-type: none"> • Default value: /iwc_static/layout/main.html • Data Type: String
client.loginpage	<p>Location of the static html login page</p> <ul style="list-style-type: none"> • Default value: /iwc_static/layout/login.html • Data Type: String
client.anoncalviewpage	<p>Location of the static html Anonymous calendar view page</p> <ul style="list-style-type: none"> • Default value: /iwc_static/layout/calendar.html • Data Type: String

client.uploadfilemethod	<p>Enables or disables attachment progress indicator in HTML5 web browsers. Use [iframe html5] method for uploading attachment file, the specified method also determines whether a progress bar can be shown. If 'iframe' method is chosen, no progress bar is shown. If 'html5' method is chosen, a progress bar is shown for HTML 5 browsers. However, non HTML 5 browsers, e.g IE 8 or 9 will revert back to iframe method</p> <p>Introduced in Convergence 2 Patch 4</p> <ul style="list-style-type: none"> • Default Value: html5 • Data Type: String • Allowed Pattern/Values: iframe (hide progress indicator) or html5 (display progress indicator)
client.screennameeditable	<p>Turn on/off editing user's display name through mail's local identity option.</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: true or false • Default value: false • Default value: false • Data Type: boolean
client.changepasswordpage	<p>The URL for changing the user's password after it expires</p> <ul style="list-style-type: none"> • Data Type: String

Admin Service Configuration Properties for the Convergence Interface



This section contains the command-line properties used for administration service.

Command-Line Option Name	Description
admin.enablessl	Whether SSL is enabled for admin service <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
admin.enablemonitoring	Whether monitoring is enabled <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
admin.adminpwd	Application's administrator password. This is used by the CLI/Monitoring mechanism to provide authorized access to application administration <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
admin.keystorepwd	Keystore password for SSL enabled admin server <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String

Single-Sign-On Configuration Properties for the Convergence Interface

This section contains the command-line properties used for single sign-on.

Command-Line Option Name	Description
sso.am.enable	This creates default configuration parameters required to enable AM SSO mechanism. Specific parameters can further be modified/created using parameter-specific CLI option. This flag differs from sso.enable <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false • Access Type: RESTRICTED
sso.ms.enable	This creates default configuration parameters required to enable MS SSO mechanism. Specific parameters can further be modified/created using parameter-specific CLI option. This flag differs from sso.enable <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false • Access Type: RESTRICTED

sso.opensso.enable	<p>This creates default configuration parameters required to enable SSO with Sun OpenSSO Enterprise mechanism. Specific parameters can further be modified/created using parameter-specific CLI option. This flag differs from sso.enable</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false • Access Type: RESTRICTED <div data-bbox="597 436 1377 646" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> Note As of Communications Suite 7 Update 1, support for Sun OpenSSO Enterprise 8.0 has been deprecated. See: Deprecated Support of Access Manager and Sun OpenSSO.</p> </div>
sso.servicename	<p>This specifies if SSO service name (whether AM_SSO or MS_SSO or OPEN_SSO or CUSTOM_SSO) is enabled or not</p> <ul style="list-style-type: none"> • Default value: AM_SSO • Data Type: String
sso.enable	<p>This specifies if SSO service (whether AM or MS SSO or OpenSSO) is enabled or not</p> <ul style="list-style-type: none"> • Default value: false • Allowed Pattern/Values: true or false • Data Type: boolean <div data-bbox="597 1108 1377 1318" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;"> <p> Note As of Communications Suite 7 Update 1, support for Sun OpenSSO Enterprise 8.0 has been deprecated. See: Deprecated Support of Access Manager and Sun OpenSSO.</p> </div>
sso.enablesignoff	<p>Whether single sign off service is enabled or not</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
sso.ssoServiceImpl	<p>SSO implementation provider name</p> <ul style="list-style-type: none"> • Default value: com.sun.comms.client.security.sso.impl.AMSSOProvider • Data Type: String

sso.notifyserviceimpl	Notification service implementation <ul style="list-style-type: none"> • Default value: null • Data Type: String
sso.enablerefreshsso	Whether SSO token refresh is enabled or not <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
sso.refreshinterval	After what percentage of convergence session timeout interval, sso token should be refreshed <ul style="list-style-type: none"> • Default value: 80 • Data Type: Integer
sso.misc	Placeholder for custom sso provider configuration <ul style="list-style-type: none"> • Allowed Pattern/Values: user-defined-attribute • Data Type: String
sso.adminuid	Admin userid for sso provider <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
sso.adminpwd	Admin password for sso provider <ul style="list-style-type: none"> • Default value: Not Applicable • Data Type: String
sso.loginpage	Location of the login page to which the user is redirected to. <ul style="list-style-type: none"> • Default value: null • Data Type: String

Instant Messaging Configuration Properties for the Convergence Interface

This section contains the command-line properties used for Instant Messaging.

Command-Line Option Name	Description
im.enable	Enable or disable IM service <ul style="list-style-type: none"> • Data Type: boolean • Allowed Pattern/Value: true or false

SMIME Configuration Properties for Convergence

This section contains the command-line properties used for SMIME.

Command-Line Option Name	Description
smime.enable	<p>Enable or disable S/MIME service</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Value: true or false

User Preferences Configuration Properties for the Convergence Interface

This section contains the command-line properties for user preferences.

Command-Line Option Name	Description
user.common.defaultapp	<p>The default application to display to user upon login</p> <ul style="list-style-type: none"> • Default value: mail • Allowed Pattern/Values: Name of the service. For example, mail, calendar • Data Type: String
user.common.theme	<p>Specifies the name of default user interface theme used</p> <ul style="list-style-type: none"> • Default value: theme_blue • Data Type: String
user.common.theme	<p>Specifies the name of default user interface theme used</p> <ul style="list-style-type: none"> • Default value: blue_theme • Data Type: String
user.common.defaultmailhandler	<p>Specifies the default mail handler for all mail links</p> <ul style="list-style-type: none"> • Default value: uc • Data Type: String
user.common.dateformat	<p>Specifies date display and input format</p> <ul style="list-style-type: none"> • Default value: M/D/Y • Allowed Pattern/Values: This can be any of M/D/Y, D/M/Y, Y/M/D • Data Type: String
user.common.datedelimiter	<p>Delimiter is the character that separates date, month and year in the date</p> <ul style="list-style-type: none"> • Default value: / • Allowed Pattern/Values: This can be any of -, / or . • Data Type: String

user.common.timeformat	<p>Specifies the time display format</p> <ul style="list-style-type: none"> • Default value: 12 • Allowed Pattern/Values: This can be any of 12 or 24 • Data Type: Integer
user.common.timezone	<p>Specifies the time zone used to normalize all time/date information in the client</p> <ul style="list-style-type: none"> • Default value: America/Los_Angeles • Data Type: String
user.common.enablesmartTZ	<p>Allows the end user to enable or disable the smart Time zone feature for the client</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Value: true or false
user.ab.name	<p>Specifies the name of address book</p> <ul style="list-style-type: none"> • Default value: Personal Address Book • Data Type: String
user.ab.description	<p>Specifies the description of address book</p> <ul style="list-style-type: none"> • Default value: This is the personal address book • Data Type: String
user.ab.entriesperpage	<p>Specifies the number of entries to be displayed per page</p> <ul style="list-style-type: none"> • Allowed Pattern/Values: Greater than or equal to 1 • Default value: 100 • Data Type: Integer
user.cal.defaultview	<p>Calendar view to be presented at log in</p> <ul style="list-style-type: none"> • Default value: dayview • Allowed Pattern/Values: This can be any of dayview, weekview, monthview, next7view, agendaview • Data Type: String
user.cal.daystart	<p>Start time hour for displaying calendar information</p> <ul style="list-style-type: none"> • Default value: 9 • Allowed Pattern/Values: Value of the hour in 24 hr format (0 - 23 hrs) • Data Type: Integer

user.cal.dayend	<p>End time hour for displaying calendar information</p> <ul style="list-style-type: none"> • Default value: 18 • Allowed Pattern/Values: Value of the hour in 24 hr format (0 - 23 hrs) • Data Type: Integer
user.cal.weekfirstday	<p>First day of the week to be displayed on user's calendar</p> <ul style="list-style-type: none"> • Default value: 1 • Allowed Pattern/Values: Valid values are 1 through 7. 1 - Sunday, 2 - Monday. etc. • Data Type: Integer
user.cal.weekenddays	<p>Specifies the weekend days</p> <ul style="list-style-type: none"> • Default value: 1,7 • Allowed Pattern/Values: Valid values are 1 through 7. 1 - Sunday, 2 - Monday. etc. • Data Type: String
user.cal.reminderinterval	<p>Amount of time before the event that an alarm should be sent</p> <ul style="list-style-type: none"> • Default value: -PT0H30M • Data Type: String
user.cal.enablenotify	<p>Enables/disables email notifications being sent for the event reminder</p> <ul style="list-style-type: none"> • Default value: 0 • Allowed Pattern/Values: 0 - disable, 1 - enable • Data Type: Integer
user.cal.enablesmsnotify	<p>Enables/disables sms notifications being sent for the event reminder</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.cal.enableinvitenotify	<p>Enables/disables email notifications being sent when the calendar receives an invitation</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.cal.eventfilter	<p>Specifies the type of events to be displayed</p> <ul style="list-style-type: none"> • Default value: null • Data Type: String

user.mail.deleteonlogout	<p>Specifies if mails marked as deleted has to be removed when user logs out of application</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.mail.autospellcheck	<p>Specifies if auto spell check is enabled</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.mail.blockimages	<p>Specifies if images in the incoming mail should be shown or blocked</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.mail.mailspage	<p>Specifies the number of mails to display per page</p> <ul style="list-style-type: none"> • Default value: 20 • Data Type: Integer
user.mail.sortorder	<p>Specifies the sorting order</p> <ul style="list-style-type: none"> • Default value: R • Data Type: String
user.mail.sortbycol	<p>Specifies which column to be used to sort the mails</p> <ul style="list-style-type: none"> • Default value: 6 • Data Type: Integer
user.mail.enablertfcompose	<p>Specifies if compose window should use RTF</p> <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
user.mail.displaycol	<p>Specifies which columns to display in mail view</p> <ul style="list-style-type: none"> • Default value: 2,1,4,3,5,6,0,7 • Data Type: String
user.im.defaultgroup	<p>Default group to which the new contacts are added</p> <ul style="list-style-type: none"> • Default value: Friends • Data Type: String

user.im.enableidlewait	<p>Change my status to idle when I am inactive</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.im.idlewaittime	<p>Change my status to idle when I am inactive for this many minutes</p> <ul style="list-style-type: none"> • Default value: 10 • Data Type: Integer
user.im.enableawaywait	<p>Change my status to away when I am inactive</p> <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
user.im.awaywaittime	<p>Change my status to away when I am inactive for this many minutes</p> <ul style="list-style-type: none"> • Default value: 10 • Data Type: Integer
user.im.chatfont	<p>Default text font in chat window</p> <ul style="list-style-type: none"> • Default value: Arial • Data Type: String
user.im.chattypface	<p>Default font typeface in chat window</p> <ul style="list-style-type: none"> • Default value: Italic • Data Type: String
user.im.fontsize	<p>Default font size in chat window</p> <ul style="list-style-type: none"> • Default value: 10 • Data Type: Integer
user.im.fontcolor	<p>Default font color in chat window</p> <ul style="list-style-type: none"> • Default value: #000000 • Data Type: String
user.im.bgcolor	<p>Default background color in chat window</p> <ul style="list-style-type: none"> • Default value: #ffffff • Data Type: String

user.im.showpane	Stores user preference of state of IM pane Introduced in Convergence 2 <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
user.im.lastpresencemsg	Last presence message to persist upon logout Introduced in Convergence 2 <ul style="list-style-type: none"> • Default value: "" • Data Type: String
user.im.lastpresencestatus	Status string indicating presence Introduced in Convergence 2 <ul style="list-style-type: none"> • Default value: online • Data Type: String • Allowed Pattern/Values: online, offline, away, invisible
user.im.persistpresence	Determines whether to retain user's presence upon logout Introduced in Convergence 2 <ul style="list-style-type: none"> • Default value: true • Data Type: boolean • Allowed Pattern/Values: true or false
user.smime.sendsigned	Default option whether to digitally sign an outgoing message <ul style="list-style-type: none"> • Default value: no • Allowed Pattern/Values: Value can be yes or no • Data Type: String
user.smime.sendencrypted	Default option whether to encrypt an outgoing message <ul style="list-style-type: none"> • Default value: no • Allowed Pattern/Values: Value can be yes or no • Data Type: String
user.smime.enablepreview	Default option whether to preview an outgoing message <ul style="list-style-type: none"> • Default value: no • Allowed Pattern/Values: Value can be yes or no • Data Type: String

Address Book JMQ Configuration Properties

This section contains the command-line properties for the JMQ Address Book notification parameters.

Command-Line Option Name	Description
notify.service.enable	Enable or disable notification service <ul style="list-style-type: none"> • Default value: false • Data Type: boolean • Allowed Pattern/Values: true or false
notify.service.mq.threadpoolsize	The number of threads to be created in the publisher/subscriber service. This parameter is optional. <ul style="list-style-type: none"> • Default value: 3 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
notify.mq.[%serviceName%].servicename	The name used to identify this service. Setting this to blank deletes this service. <ul style="list-style-type: none"> • Data Type: String
notify.mq.[%serviceName%].enable	Enable or disable notification service associated with this service name <ul style="list-style-type: none"> • Data Type: boolean • Allowed Pattern/Value: true or false
notify.mq.[%serviceName%].destinationtype	The destination-type(Topic or Queue) of the destination associated with this service <ul style="list-style-type: none"> • Allowed Pattern/Values: TOPIC or QUEUE • Data Type: String

Chapter 10. Convergence Troubleshooting

Troubleshooting the Convergence Interface

This information describes how to resolve problems you encounter in your deployment. The primary method is to capture log information when possible.

Configuring Log Levels to Gather Information

This section covers how to configure log levels for the Convergence server. Log levels can be set by using the `iwcadmin` command-line utility.

For more information on the command-line utility, see [Overview of the Convergence Command Line Utility](#).

The following are the log configuration parameters:

- **LogLocation** : Path to the directory where the log file is stored.
- **LogPattern** : Declares the information and format to specify what to log and in what format. For more information about how to specify the LogPattern, see the Log4J specification at : [Log4J Specification \(http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html\)](http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html)
- **LogRotation**: Log rotation specifies the policy for rolling over logs to a new location. This release includes the following policies:
 - **SizeTrigger** policy: SizeTrigger is defined as the number of bytes of log information to accumulate before rolling the log over to a new location.
 - **TimeTrigger** policy: TimeTrigger is defined as the time of day to roll over the log to a new log location. The value is expressed as a `SimpleDatePattern`.
- **Logger**: The initial system Logger value is `DEFAULT`, that takes the default LogLevel. However, each module in Convergence can control the logging level of its own logs. For example, the authentication module might name its logger `AUTH` and set the log level to `WARN`. To know more about the various logging levels, see [What are the different Log Levels?](#).

Logging levels (`LogLevel`) are set using a predefined default set of log levels. For example:

- `DEBUG`
- `INFO`
- `WARN`
- `ERROR`
- `OFF`.

The `DEBUG` level is the most verbose level. Do not to use this for everyday logging as it negatively impacts the server's performance. However, you should use this level when you need to trap as much information about a recurring problem. After capturing the required log data, you should return the log level to a lesser level of log setting.

Chapter 11. Enabling Services for Convergence

Enabling Core Services for Convergence

Convergence provides access to the following supported core services:

- Mail
- Calendar
- Address Book
- Instant Messaging

Convergence allows you to provide services for a specified set of users or domains. You might want to provide or disable services at the following levels:

- The entire Convergence installation
- An individual domain (or set of domains)
- An individual user (or set of users)

The following sections describe how to enable and disable services at different levels:

- [Enabling Services for the Entire Convergence Installation](#)
- [Enabling Services for an Individual User or Domain](#)
- [Using the Delegated Administrator Utility \(commadmin\) to Manage Services](#)
- [Using the Delegated Administrator Console to Manage Services](#)
- [Enabling and Disabling Services with Direct LDAP Provisioning](#)
- [Enabling and Configuring IM Service After Initial Configuration of Convergence](#)

Enabling Services for the Entire Convergence Installation

The address book service is enabled by default. You can enable or disable any of the other services without customizing Convergence.

After you install Convergence, you must initially configure the software by running the `init-config` utility. When you run `init-config`, you can enable and configure mail, calendar, and instant messaging services for the entire installation. You can enable any combination of these services. Thus, the "default" setting for whether a service is enabled or not depends on whether you select it for configuration when you run `init-config`. For details, see [Completing the Convergence Installation: Initial Configuration](#).

After the initial configuration, you can enable or disable a service for your entire Convergence deployment. This encompasses all domains in the deployment and all users under the domains.


For Convergence 1.x, use the `iwadmin` utility to set the following options to `true` or `false`:

- `mail.enable`
- `cal.enable`
- `im.enable`

Beginning with Convergence 2.x, use the `iwadmin` utility to set the following options to `true` or `false`:

- `mail.enable`
- `cal.enable` (Calendar 6.3)
- `caldav.enable` (Calendar 7)

- `im.enable`
- `iss.enable`

 **Note**

In a calendar server co-existence scenario, be sure to set both `cal.enable` (Calendar 6.3) and `caldav.enable` (Calendar 7) parameters.

Enabling Services for an Individual User or Domain

To enable or disable a service for a user or domain, you must set the appropriate LDAP attributes for that service in the user entry or domain entry in the LDAP. If you are running Delegated Administrator, you can use the Delegated Administrator console or utility to set the LDAP attributes that determine service availability.

For detailed descriptions of the Delegated Administrator command-line utility, see [Command-Line Utilities](#) in the Delegated Administrator 6.4 Administration Guide.


Managing Access to Communications Suite Services Through LDAP

WARNING: Managing services through LDAP affects users' access to the entire Communications Suite. This is a very different conceptual territory than controlling the services available through Convergence, the client. You need to check the following functions while managing access to services in the LDAP:

1. Providing the Communications Suite services themselves. You do this by installing and configuring Messaging Server, Calendar Server, and Instant Messaging. The Address Book is provided when you configure Convergence.
2. Managing the services available to users and domains in the LDAP directory. When you change a user's access to a service in the LDAP directory, you affect that user's access to Messaging Server, Calendar Server, or Instant Messaging, no matter which clients that user may use to access these services.
Similarly, when you change domain-level services in LDAP, you affect the access to Communications Suite services for all users in the domain.
3. Managing the services available in Convergence. This affects Convergence users only.

To enable a service for an individual domain or user, you must perform all three preceding tasks. To make a service available to one Convergence user, you must enable that service for the entire Convergence installation. See [Enabling Services for the Entire Convergence Installation](#).

The **WARNING** really pertains to *disabling* a service for domains and users in LDAP. When you disable LDAP service attributes, those user's access to the Communications Suite service is also disabled. All clients are disabled for those users, not only Convergence.

 **Note**

In Delegated Administrator version 6.4, Communications Suite 6 release, you can enable and disable mail and calendar service, but you cannot use Delegated Administrator to add or delete Instant Messaging service. For Instant Messaging service, you must use direct LDAP provisioning tools.

To enable customization for an individual user or domain, see [Enabling Customization for Users and Domains](#).

Using the Delegated Administrator Utility (commadmin) to Manage Services

For detailed descriptions of the Delegated Administrator command-line utility, see [Command-Line Utilities](#) in the Delegated Administrator 6.4 Administration Guide.

To Create a Domain with a Service

To create a domain with mail or calendar service, use the `commadmin domain create` command. The following example creates the `siroe.com` domain with mail and calendar service:

```
commadmin domain create -D <username> -d siroe.com -n sesta.com -w
bolton -S mail,cal
-H mailhost.sesta.com
```

To Add a Service to an Existing Domain

To add mail or calendar service to an existing domain, use the `commadmin domain modify` command. The following example adds mail and calendar service to the `varrius.com` domain:

```
commadmin domain modify -D chris -w bolton -n sesta.com -d varrius.com
-S mail, cal
```

To Delete a Service From a Domain

To disable mail or calendar service in a domain, use the `commadmin domain delete` command. The following example disables mail and calendar service from the `florizel.com` domain:

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com
-S mail,cal
```

To Create a User with a Service

To create a user with mail or calendar service, use the `commadmin user create` command. The following example creates the user `smith` with mail and calendar service.

```
commadmin user create -D chris -n sesta.com -w secret -F smith -l john
-L major -W secret -S mail,cal -H mailhost.siroe.com
```

To Enable a Service for an Existing User

To add mail or calendar service to an existing user, use the `commadmin user modify` command. The following example adds mail and calendar service to the user `smith`.

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith -A
description:"new description" -S mail,cal -H mailhost.siroe.com
```

To Disable a Service for a User

To disable mail or calendar service for a user, use the `commadmin user delete` command. The

following example deletes mail and calendar service from the user smith.

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail,  
cal
```

Using the Delegated Administrator Console to Manage Services

In the Delegated Administrator Console, you can manage services by means of service packages. Sets of service packages are allocated to an organization or domain, and then the service packages are assigned to individual users. The service packages provide mail and calendar services to users.

For information about service packages and how to use them, see [Service Packages](#) in the Delegated Administrator 6.4 Administration Guide.

For detailed instructions about creating, adding, and disabling services through the Delegated Administrator console, see the online help in the Delegated Administrator console.



Note

To manage domain-level (organization-level) services in the Delegated Administrator console, you must log in as a Top-Level Administrator.

Enabling and Disabling Services with Direct LDAP Provisioning

You can configure mail, calendar, and instant messaging services by setting the appropriate LDAP user and domain attributes. You can use direct LDAP tools or provisioning scripts (if they have been developed at your site).

LDAP Attributes for Mail Service

To enable mail service to an individual user, set the following attribute in the user's entry in the User/Group tree:

```
mailUserStatus: active
```

To disable a user's mail service, set

```
mailUserStatus: deleted
```

To enable mail service to an individual domain, set the following attribute in the domain entry:

```
mailDomainStatus: active
```

To disable access to mail service for all users in the domain, set

```
mailDomainStatus: deleted
```

LDAP Attributes for Calendar Service

To enable calendar service to an an individual user, set the following attribute in the user's entry in the User/Group tree:

```
icsStatus: active
```



Note

When the `icsStatus` attribute is used in a user entry, it must be associated with the `icsCalendarUser` object class.

To disable a user's calendar service, set

```
icsStatus: deleted
```

To enable the calendar service to an individual domain, set the following attribute in the domain entry:

```
icsStatus: active
```



Note

When the `icsStatus` attribute is used in a domain entry, it must be associated with the `icsCalendarDomain` object class.

To disable access to calendar service for all users in the domain, set

```
icsStatus: deleted
```

LDAP Attributes for Instant Messaging Service

To enable instant messaging service to an individual user, you can use the `imadmin assign services` command, or you can add the following instant messaging object classes in the user's LDAP entry in the User/Group tree:

```
sunIMUser  
sunPresenceUser
```

To disable access to instant messaging service for a user, remove the above object classes from the user's LDAP entry.

Enabling and Configuring IM Service After Initial Configuration of Convergence

To enable IM service after having configured Convergence, perform the following steps:

1. Set the `im.enable=true` using `iwadmin`.
2. Edit the `httpbind.conf` file present in the `/var/opt/sun/comms/iwc/config` directory and set the IM server name, domain name, component JID's, and password for `httpbind` and `avatar`.

Note

- The component `jid` and password should match the ones specified in the `iim.conf` file. See [Configuration Changes Required on IM Server Side](#).
- The passwords for the `httpbind` and the `avatar` component must be encrypted. For information on generating the encrypted password, see the section [Verifying Passwords in Convergence](#).

3. Restart the GlassFish Server.
4. Type the following:

```
/opt/sun/comms/im/sbin/imadmin assign_services
```

to add IM object classes to the users.

Chapter 12. Enhancing Corporate Directory Search for Convergence by Using VLV Indexing in Directory Server

Enhancing Corporate Directory Search for Convergence by Using VLV Indexing in Directory Server

Virtual List View (VLV) index, also known as browsing index, is similar to indexes or views in a database. Create the VLV indexes to reduce the time taken to search the LDAP entries. If a Directory Server deployment contains several LDAP entries, then searching the entries takes considerably more time. Directory Server enables you to create indexes that reduce the search time.

The following topics provide information about how you can create VLV indexes and configure Convergence to use the VLV indexing feature of Directory Server.

- [Creating the VLV Index in Directory Server 6.3](#)
- [Generating Indexes](#)
- [Configuring Convergence](#)
- [Verifying the VLV Settings](#)

Creating the VLV Index in Directory Server 6.3

You must set the following parameters in the `ldif` file to enable VLV indexes in Directory Server.

- `search_base`
- `vlv_search_filter`
- `vlv_sort_attribute`
- `vlv_scope`



Note:

If multiple back-end user/group Directory Servers are configured for a system, you will need to create indexes for each user/group Directory Server instance.

You require the Directory Server settings information before setting the VLV browsing indexes. Directory Server settings are present in the `dse.ldif` file in the `<directory_server_root>/config` directory. Note the value of the `cn` attribute.

The following is a code sample of the `dse.ldif` file:

dse.ldif

```
dn: cn=isp,cn=ldbm database,cn=plugins,cn=config
objectClass: top
objectClass: extensibleObject
objectClass: nsBackendInstance
cn: isp
creatorsName: cn=directory manager
modifiersName: cn=directory manager
entrydn: cn=isp,cn=ldbm database,cn=plugins,cn=config
numSubordinates: 4
nsslapd-suffix: o=isp
nsslapd-cachesize: -1
nsslapd-cachememsize: 10485760
nsslapd-readonly: off
nsslapd-require-index: off
nsslapd-directory: /var/opt/SUNWdsee/dsins1/db/isp
```



Create two files in a temporary location after you identify the required Directory Server setting entries. For example, `tmp1.vlv` and `tmp2.vlv`. These files must contain information about various indexes and search options that you can create on Directory Server.

The `tmp1.vlv` file should have the following parameters.

temp1.vlv

```
dn: cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvSearch
cn: <browsing-index>
vlvbase: o=isp
vlvscope: 2
vlvfilter: (&(mail=*)(cn=*))
aci: (targetattr="*)(version 3.0; acl "VLV for Anonymous";
allow (read,search,compare) userdn="ldap:///anyone";)
```

The parameters setting for the file `temp1.vlv` are listed in the following table:

Parameters	Settings
<browsing-index>	Any name
<database-name>	Same as the existing database name that is given when directory server is configured by running directory preparation tool (<code>comm_dssetup.pl</code>). This database name should not be changed.
<code>vlvbase</code>	Value from which you want the search to proceed. For example, instead of <code>dc=example,dc=siroe,dc=com</code> you can provide a subtree <code>o=example.siroe.com,dc=example,dc=siroe,dc=com</code> .
<code>vlvscope</code>	Similar to the LDAP protocol scoping number:
	0 -Indicates searching only the base level entry
	1 - Indicates searching only the entries at one level below the search base. If you set <code>vlvScope</code> to 1, you must create a <code>vlvSearch</code> or <code>vlvIndex</code> for each organization unit (<code>ou</code>) where you want a VLV index.
	2 - Indicates searching of the entries at all levels and all its descendants.
<code>vlvfilter</code>	<p>Filter that is used to match and filter results. When you perform a search, only those LDAP entries that have both <code>mail</code> and <code>cn</code> attributes defined are returned. Some of the entries might not have <code>mail</code> attribute. If they do not have the <code>mail</code> attribute, modify the <code>vlvfilter</code> as <code>((mail=*)(cn=*))</code>.</p> <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p> Note: The OR operator is used instead of the AND operator.</p> </div> <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p> Note: Only include contacts (for example: <code>objectclass=inetorgperson</code>) while creating the vlv index so that the address book search excludes groups, resources and any other entries that are not contacts. This is mandatory for Convergence 2.</p> </div> <p>Leave an extra blank line after the last line in both the <code>temp1.vlv</code> and <code>temp2.vlv</code> files to make sure that all the entries in the files are read when the LDAP is modified.</p>

The `temp2.vlv` file should have the following parameters:

temp2.vlv

```
dn: cn=Sort by cn,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Sort by cn
vlvSort: cn
```

The temp1.vlv and temp2.vlv files specify what to index and the parameter by which results must be sorted. You need to create multiple indexes by creating below more files : temp3.vlv , temp4.vlv, temp5.vlv, temp6.vlv, temp7.vlv, temp8.vlv and temp9.vlv.

The temp3.vlv file should have the following parameters:

temp3.vlv

```
dn: cn=Reverse Sort by cn,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Reverse Sort by cn
vlvSort: -cn
```

The temp4.vlv file should have the following parameters:

"temp4.vlv"

```
dn: cn=Sort by sn,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Sort by sn
vlvSort: sn
```

The temp5.vlv file should have the following parameters:

temp5.vlv

```
dn: cn=Reverse Sort by sn,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Reverse Sort by sn
vlvSort: -sn
```

The temp6.vlv file should have the following parameters:

temp6.vlv

```
dn: cn=Sort by mail,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Sort by mail
vlvSort: mail
```

The temp7.vlv file should have the following parameters:

temp7.vlv

```
dn: cn=Reverse Sort by
mail,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Reverse Sort by mail
vlvSort: -mail
```

The temp8.vlv file should have the following parameters:

temp8.vlv

```
dn: cn=Sort by givenname,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Sort by givenname
vlvSort: givenname
```

The temp9.vlv file should have the following parameters:

temp9.vlv

```
dn: cn=Reverse Sort by
givenname,cn=<browsing-index>,cn=<database-name>,cn=ldbm
database,cn=plugins,cn=config
changetype: add
objectClass: top
objectClass: vlvIndex
cn: Reverse Sort by givenname
vlvSort: -givenname
```

To modify the LDAP using tmp1.vlv and tmp2.vlv type the following command:

```
# ldapmodify -h <directory-server-fully-qualified-host-name> -p
<directory-server-port-number> -D "cn=Directory Manager" -f
<relative-or-absolute-path-to>/templ.vlv
# ldapmodify -h <directory-server-fully-qualified-host-name> -p
<directory-server-port-number> -D "cn=Directory Manager" -f
<relative-or-absolute-path-to>/temp2.vlv
```

Similarly, you can modify the LDAP by using all other `.vlv` files:

Generating Indexes

Generate the indexes for the settings to take effect. Perform the following steps during a scheduled change window to restart Directory Server.

Perform the following steps to generate the indexes:

1. Change the directory to the Directory Server installation.

```
cd /opt/SUNWdsee/ds6/bin
```

2. Stop the Directory Server instance.

```
./dsadm stop /var/opt/SUNWdsee/dsins1/
```

3. Populate the index entries by using the `dsadm reindex` command. The `reindex` option requires you to provide the `vlv_sort_attribute`, the path to the Directory Server instance, and the value of the user group base.

```
./dsadm reindex -l -t "Sort by cn" /var/opt/SUNWdsee/dsins1/
"o=isp"
```

4. Start the Directory Server instance.

```
./dsadm start /var/opt/SUNWdsee/dsins1/
```

If you require multiple sort attributes for `tmp3.vlv` and `tmp4.vlv`, generate indexes for each of `cn`, `sn`, and `mail`.

Configuring Convergence

You need to configure Convergence to use the indexes after generating the indexes for Directory Server. Set the following Convergence related parameters:

- `ab.corpdir.[CommSuite:default].vlvfilter`
- `ab.corpdir.[CommSuite:default].vlvscope`
- `ab.corpdir.[CommSuite:default].vlvpaging`
- `ab.corpdir.[CommSuite:default].vlvsortby`
- `ab.corpdir.[CommSuite:default].vlvsearchbase`
- `ab.corpdir.[CommSuite:default].vlvsortby`

Type the following command:

```
iwcadmin -u <adminuserid> -o ab.corpdir.[default].vlvfilter -v  
"(&(mail=*)(cn=*))"
```



Note

The value for the `-v` switch is `(&(mail=*)(cn=*))`. This value should exactly match with the value provided in the Directory Server settings and the match should be a string match. It cannot even be `(&(cn=*)(mail=*))` because interchanging the `mail` and `cn` attributes causes a mismatch with the settings in the Directory Server.

Type the following commands:

```
# iwcadmin -u <adminuserid> -o ab.corpdir.[default].vlvscope -v 2  
# iwcadmin -u <adminuserid> -o ab.corpdir.[default].vlvpaging -v true  
# iwcadmin -u <adminuserid> -o ab.corpdir.[default].vlvsortby -v  
"entry/displayname,person/surname,email,person/givenname"  
# iwcadmin -u <adminuserid> -o ab.corpdir.[default].vlvsearchbase -v  
"o=isp"
```



Note

- The default corporate directory is used in the previous commands. The same set of commands apply to the nondefault corporate address book `ab.corpdir.[<identifier>].vlvscope` or the domain based corporate address book `ab.{<identifier>}.corpdir.[<identifier>].vlvscope`.
- The purpose of the parameter `vlvsortby` is that in case the server does not receive any `sortby` attribute from the client, the search results are sorted by the value set for this parameter. This applies only when VLV is setup.
- You must restart the application after making any configuration changes in Convergence.
- When you search a Corporate Address Book, you will see a drop down list in the Convergence client interface with the following search attributes:
 - Display name
 - Email
 - First name
 - Last name
- You must have VLV indexes set up for these attributes to work. If VLV is not set, the default search is done by Display name.

Verifying the VLV Settings

1. For the VLV search to be active when you search the corporate directory, the following four entities sent by the Convergence server should match with the values in Directory Server:
 - Search base
 - Search scope
 - VLV filter
 - Sort attribute



Note

Convergence only supports `cn`.

2. Log in to Convergence and type a search command in the corporate directory to check the Directory Server access log files.

The two cases A and B with corresponding access log files of Directory Server are shown:

```
ldapsearch -D "cn=Directory Manager" -w password -b
dc=example,dc=com -x -S cn -G "0:3:name1" "(|(mail=*)(cn=*))" sn cn
```

Directory Server Access Log file A

```
[02/Dec/2008:12:46:52 +0100] conn=53 op=1 msgId=2 - SRCH
base="dc=example,dc=com" scope=2 filter="(|(mail=*)(cn=*))"
attrs="sn cn"
[02/Dec/2008:12:46:52 +0100] conn=53 op=1 msgId=2 - SORT cn
[02/Dec/2008:12:46:52 +0100] conn=53 op=1 msgId=2 - VLV 0:3:rao
128:156 (0)
[02/Dec/2008:12:46:52 +0100] conn=53 op=1 msgId=2 - RESULT err=0
tag=101 nentries=4 etime=0
```

```
ldapsearch -D "cn=Directory Manager" -w password -b
dc=example,dc=com -x -S sn -G "0:3:name1" "(|(sn=*)(cn=*))" sn cn
```

Directory Server Access Log file B

```
[02/Dec/2008:12:45:34 +0100] conn=52 op=1 msgId=2 - SRCH
base="dc=example,dc=com" scope=2 filter="(|(sn=*)(cn=*))" attrs="sn
cn"
[02/Dec/2008:12:45:34 +0100] conn=52 op=1 msgId=2 - SORT sn (156)
[02/Dec/2008:12:45:34 +0100] conn=52 op=1 msgId=2 - VLV 0:3:name1
97:156 (0)
[02/Dec/2008:12:45:34 +0100] conn=52 op=1 msgId=2 - RESULT err=0
tag=101 nentries=4 etime=0 notes=U
```

Searches in A and B might vary based on the `-S` sort attribute. In this case, VLV is setup with `cn` as the sort attribute.

VLV index is used only if `vlvSort`, `vlvbase`, `vlvscope`, and `vlvfilter` are matched with the given attributes. In case A all the attributes are matched. Hence the VLV index is used. In case B the VLV Index is not used as the sort attribute passed is `sn` whereas the setup has `cn`. See the `notes=U` in the Log file B displays that the search was unindexed. You can still continue to search with the `-S` server sort option. It will always be unindexed if no VLV Index is present that matches the specific search. Also notice the line "VLV 0:3:rao" which means that a VLV search was performed and from the point where a match was found 3 other entries were returned apart from the match. The zero before 3 signifies that no entries above the match in the sort order are returned.

To illustrate this further :

Assume that the Directory Server has a VLV in the following sorted order :

```

person1 age1 address1 email1@siroe.com
person2 age2 address2 email2@siroe.com
person3 age3 address3 email3@siroe.com
person4 age4 address4 email4@siroe.com
person5 age5 address5 email5@siroe.com
person6 age6 address6 email6@siroe.com
person7 age7 address7 email7@siroe.com
person8 age8 address8 email8@siroe.com

```

Search for cn=person4 with the range as 1:3:person4.

```

person1 age1 address1 email1@siroe.com
                                person2 age2 address2 email2@siroe.com
                                person3 age3 address3 email3@siroe.com <-----
Search match --->              person4 age4 address4 email4@siroe.com
|
                                person5 age5 address5 email5@siroe.com
| Range of results returned
                                person6 age6 address6 email6@siroe.com
|
                                person7 age7 address7 email7@siroe.com <-----
                                person8 age8 address8 email8@siroe.com

```

Since you have searched for 1:3:person4, the results returned are one entry before the match, three entries after the match, and the match entry itself.

To verify, type the following command on the Directory Server to view the results:

```

# ldapsearch -h <directory-server-fully-qualified-host-name> -p
<directory-server-port-number> -TD "cn=directory manager" -w
<directory-manager-password> -b <search-base> -s <search-scope> -x -S
<sort-attribute> -G
"<number-of-results-before-match>:<number-of-results-after-match>:<search-s
<vlv-filter>

```

For example:

```

ldapsearch -h siroe.com -TD "cn=directory manager" -w password -b
"dc=siroe,dc=siroe,dc=com" -s sub -x -S cn -G "1:3:person4"
"(&(mail=*)(cn=*))"

```

The results displayed should match the results in Convergence.

The parameters `ab.corpdir.[CommSuite:default].searchattr` and `ab.corpdir.[CommSuite:default].searchfilter` are not involved in the VLV search.

Same as the existing database name that is given when directory server is configured by running directory preparation tool (`comm_dssetup.pl`). This database name should not be changed.

Chapter 13. Writing a Custom Authentication Module for Convergence

Writing a Custom Authentication Module for Convergence

For Convergence 2.x and earlier. To write a custom authentication module beginning with Convergence 3.0.0.0.0, see [Writing a Custom Authentication Module Beginning with Convergence 3.0.0.0.0](#).

Convergence server provides an interface that enables you to create custom user authentication in the form of a customizable Java-based authentication module. The custom authentication module allows an organization to use a non-Oracle LDAP mechanism (for example, an RDBMS, flat-text file or third-party LDAP server) to provide authentication functionality.



Note

By default, Convergence uses Directory Server for authentication store. For information about administering the default authentication feature, see [Authentication](#).

Basic Concepts

This section defines the terms used in this article. In addition to this, this section also describes the authentication framework architecture and its components.

The following are the definitions of terms used in this article:

Convergence uses the following repositories to store user data. They are:

- **User Authentication Store:** Contains user credentials. Such as user id, password, domain information, and an unique identifier to identify the user in the User or Group LDAP store.
- **User/Group LDAP Store (UG LDAP):** Contains user preferences such as timezone that the user is in, language preference, and user theme. Convergence uses Schema 1 or Schema 2 to store user information in the User or Group LDAP.

Convergence Authentication Framework

This section describes how the authentication framework works in Sun Convergence.

1. The authentication module first authenticates the user in the authentication store using the configured authentication module. The default authentication module that works by default is Sun Java System Directory Server.
2. On successful authentication, the authentication module gets the user specific attributes like user id, the domain of the user, organization, and a unique identifier.
3. The authentication framework loads the user from the User Group LDAP using the user id (`userID`) and domain name (`userDomain`).

Contracts Defined by the Authentication Module

Before designing a solution for the custom authentication module, you must be aware of the contracts

that the Convergence authentication framework needs for successful transfer of information between the authentication store, the Convergence authentication framework, and UG LDAP.

- The authentication module must provide a mechanism to identify a user in the UG LDAP after successful authentication. The custom authentication can have any authentication store that can use any type of identifier to authenticate the user. The authentication mechanism should provide a relationship between the authenticated user and UG LDAP. After successful authentication, the authentication module should provide a unique identifier to locate the user in the UG LDAP. For example, if both authentication store and UG LDAP use the same identifier to locate the user, after successful authentication, the authentication module must set `userID` and `userDomain` parameters in the HTTP request by using callback handler objects. These parameters are used by UG LDAP filter to load the user from the UG LDAP. In our example, the user id (example `scott`) is the unique identifier used to locate the user in UG LDAP.
- All the custom authentication modules must implement the following three classes:
 - `JAAS LoginModule` interface. Convergence uses `JAAS LoginModule` as an interface for all its login modules. The custom authentication module must implement this interface. Although the authentication module uses the JAAS framework for authentication, it does not use all the advanced capabilities like authentication chaining, and multiple login modules.
 - `HttpCallbackHandler`. An abstract class that implements the `CallbackHandler` of JAAS. This class must be implemented to handle custom callbacks. All custom authentication modules must implement this class to handle custom callbacks.
 - Convergence uses the `JAAS LoginCallback` and `CallbackHandler` interface to get and set information between the authentication module and Convergence application. Since Convergence is a web application, authentication is performed through HTTP based request and response. Convergence provides an abstract class: `HttpCallbackHandler`, which implements `CallbackHandler` interface of JAAS.
- After successful authentication, the authentication module must set the `UserPrincipal` object in the `Subject`. This can be done in commit method of login module. `UserPrincipal` must be created using `loginID` of the user.
- Custom authentication modules must not create HTTP session(`HTTPSession`) object. Convergence authentication framework takes care of initializing the session.

About the Sample Application

This article describes the various files that are created for the custom authentication module to work. Use this as a reference to create other custom authentication modules to suite your enterprise' needs. The sample authentication module can be used as is by copying the source files and following the steps as mentioned in the following sections.



Caution

If you need to change the core class file names provided in this article, note that you must appropriately refactor the code. Some of the files use objects created by other core classes of the custom authentication module.

This example describes an authentication module for a file based user data store. The following is a sample set of data that could be used to store user information in the data store.

userinfo.txt

```
smith:test:siroe.com
jack:test:siroe.com
scott:test123:siroe.com
```

In the example, each attribute is separated by a colon. For example, the first record of the file provides information about the user id `smith` whose password is `test` with domain `siroe.com`.

Implementing the classes Required for the File base Authentication Store

This section describes the classes that are used to implement the authentication module for a file based user store. The following are the core class:

1. `SunTestLoginModule.java`
2. `SunTestAuthCallBack.java`
3. `AppTestCallbackHandler.java`

SunTestLoginModule.java

```
package com.sun.comms.test;

import com.sun.comms.client.logging.IwcLogger;
import com.sun.comms.client.security.auth.UserPrincipal;
import java.io.BufferedReader;
import java.io.File;
import java.io.FileReader;
import java.io.IOException;
import java.util.Map;
import javax.security.auth.Subject;
import javax.security.auth.callback.Callback;
import javax.security.auth.callback.CallbackHandler;
import javax.security.auth.login.FailedLoginException;
import javax.security.auth.login.LoginException;
import javax.security.auth.spi.LoginModule;
import org.apache.commons.logging.Log;
import com.sun.comms.test.SunTestAuthCallBack;

public class SunTestLoginModule implements LoginModule {

    private Subject subject;
    private CallbackHandler cbh;
    private Map sharedState;
    private Map options;
    private boolean succeeded;
    private UserPrincipal up;
    private SunTestAuthCallBack mcb = null;
    private String credFile = "";
    private final static Log logger =
IwcLogger.getLogger(IwcLogger.AUTH_LOGGER);

    public void initialize(Subject subject, CallbackHandler
callbackHandler, Map<String, ?> sharedState, Map<String, ?> options) {
        this.subject = subject;
        this.cbh = callbackHandler;
        this.sharedState = sharedState;
        this.options = options;
        credFile = (String) options.get("CredentialFile");
```

```

    }

    public boolean login() throws LoginException {
        Callback[] callbacks = new Callback[1];
        mcb = new SunTestAuthCallBack();
        callbacks[0] = mcb;

        if (cbh == null) {
            throw new LoginException("Error: no CallbackHandler
available " +
                "to gather authentication information from the
user");
        }

        try {
            // Get userid and pwd from request
            cbh.handle(callbacks);
        } catch (Exception ex) {
            throw new LoginException("SunTestLoginModule: login
failed");
        }

        String[] userInfo = attemptLogin();

        if (userInfo != null && userInfo.length==3) {
            mcb.setUserInfo(userInfo[0], userInfo[2]);
            succeeded = true;
            return true;
        } else {
            System.err.println("Unable to find user entry");
            throw new FailedLoginException("Unable to find user entry");
        }
    }

    private String[] attemptLogin() throws LoginException {

        if(credFile==null)
            throw new LoginException("User database file is not set
configuration.");

        File loginFile = null;
        String userID = mcb.getUserName();
        String userPwd = mcb.getUserPwd();

        if (userID == null || userPwd == null) {
            throw new LoginException("Required user credential not
found");
        }

        try {
            loginFile = new File(credFile);
            if (loginFile.exists()) {

                BufferedReader reader = new BufferedReader(new
FileReader(loginFile));
                String userEntry = null;

```

```

        while ((userEntry = reader.readLine()) != null) {
            String[] usrAcc = userEntry.split(":");
            if (usrAcc != null && usrAcc.length == 3) {
                if (userID.equals(usrAcc[0]) &&
userPwd.equals(usrAcc[1])) {
                    return usrAcc;
                }
            }
        }
    } else {
        System.err.println("Unable to find user database file "
+ credFile);
        throw new LoginException("Unable to find user database
file " + credFile);
    }
    } catch (IOException ex) {
        System.err.println("Unable to load user database file " +
credFile);
        throw new LoginException("Unable to load user database file
" + credFile);
    }
    return null;
}

public boolean commit() throws LoginException {
    if (succeeded == false) {
        return false;
    } else {
        // add a Principal (authenticated identity) to the Subject
        UserPrincipal userPrincipal = new
UserPrincipal(mcb.getUserName());

        if (!subject.getPrincipals().contains(userPrincipal)) {
            subject.getPrincipals().add(userPrincipal);
        }
    }
    return true;
}

public boolean abort() throws LoginException {
    return true;
}

public boolean logout() throws LoginException {

```

```
        return true;
    }
}
```

SunTestAuthCallBack.java

```
package com.sun.comms.test;

import com.sun.comms.client.security.auth.LoginCallback;
import java.io.Serializable;
import java.net.InetAddress;
import java.net.UnknownHostException;
import java.util.Locale;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

public class SunTestAuthCallBack implements LoginCallback, Serializable
{

    HttpServletRequest req;
    HttpServletResponse res;
    String username = null;
    String pwd = null;

    protected String name = null;
    protected String host = null;
    protected String user = null;
    protected String userDomain = null;
    protected Locale locale = null;
    protected String serverName = null;

    SunTestAuthCallBack(){

    }

    public void setData(HttpServletRequest request,HttpServletResponse
response){
        this.req = request;
        this.res = response;
        username = (String)req.getParameter("username");
        pwd = (String)req.getParameter("password");

    }

    public String getUserName(){
        return username;
    }

    public String getUserPwd(){
        return pwd;
    }
}
```

```

public void setUserInfo(String uid,String domain){
    req.setAttribute("loginID", uid);
    req.setAttribute("userDomain", domain);
}

public boolean setData(Object obj) {
    throw new UnsupportedOperationException("Not supported yet.");
}

public Locale getLocale() {

    if (locale == null)
        return Locale.getDefault();

    return locale;
}

/**
 * set the client locale
 */

public void setLocale(Locale locale) {
    if (locale != null)
        this.locale = locale;
}

/**
 * get the host name of the machine running the console.
 * this may be required for auditing purposes
 */

public String getHost() {

if (host == null) {
    try {
        host = InetAddress.getLocalHost().getHostName();
    } catch (UnknownHostException ukhe) {
        host = null;
    }
}

    return host;
}

/**
 * set the host name of the machine
 */

public void setHost(String host) {
    if (host != null)

```

```

        this.host = host;
    }
}

```

AppTestCallbackHandler.java

```

package com.sun.comms.test;

import com.sun.comms.client.logging.IwcLogger;
import com.sun.comms.client.security.auth.modules.HttpCallbackHandler;
import java.io.IOException;
import javax.security.auth.callback.Callback;
import javax.security.auth.callback.UnsupportedCallbackException;
import org.apache.commons.logging.Log;
import com.sun.comms.test.SunTestAuthCallBack;

public class AppTestCallbackHandler extends HttpCallbackHandler {
    private final static Log logger =
IwcLogger.getLogger(IwcLogger.AUTH_LOGGER);
    public void handle(Callback[] callbacks) throws IOException,
UnsupportedCallbackException {
        if (callbacks == null) {
            throw new IOException("Empty or null callback array");
        }

        for (int i = 0; i < callbacks.length; i++) {
            if (callbacks[i] instanceof SunTestAuthCallBack ) {
                SunTestAuthCallBack nc =
(SunTestAuthCallBack)callbacks[i];
                nc.setData(request, response);
                System.err.println("request and response set in
AppTestCallbackHandler");
            }else
                System.err.println("Callback objects are not instance of
SunTestAuthCallBack");
        }
    }
}

```

How the implementation works

For every authentication request, the Convergence authentication framework reads the configured login module class name, call back handler class name and executes it using JAAS framework.

The JAAS framework calls the `initialize()` method by passing all the required arguments. One of the arguments we are interested here is the Map option of the `initialize()` method. Convergence's authentication framework populates this object with all Misc parameters of `CustomJAASService` configuration.

In this example, we pass the directory location of user database `CredentialFile` as part of Misc parameter to `SunTestLoginModule`.

The other arguments are:

- Subject `subject` - represents Subject that is being authenticated.
- CallbackHandler `callbackHandler` - Object that is responsible for handling custom callbacks.
- Map `sharedState` - Not used by Convergence and hence ignore it.

After successful initialization, the login module obtains all the required information about the callback handler and all the required configuration. The JAAS framework then invokes the `login()` method. This method performs the authentication, which is module specific. In this sample, `login()` method first creates callback object(s):

```
Callback[] callbacks = new Callback[1];
mcb = new SunTestAuthCallBack();
```

The call back object is aware of how to obtain the authentication related information such as the username, password, and so on. This is returned as a HTTP request. Once call back objects are created, it passes callback objects to `CallBackHandler`'s `handle` method.

```
cbh.handle(callbacks);
```

callbackhandler knows how to handle call back objects. For example, the method used for callback object, the data to be passed to it, and so on.

the `handle()` method of callback handler then calls callback object's `setData()` by passing request and response objects:

```
SunTestAuthCallBack nc = (SunTestAuthCallBack)callbacks[i];
nc.setData(request, response);
```

Now, the `Callback`'s `setData()` extracts the required information from request and response. In this sample, it gets request parameter `username` and `password` from request.

```
this.req = request;
this.res = response;
username = (String)req.getParameter("username");
pwd = (String)req.getParameter("password");
```

The callback object now has all information that is required to authentication the user from the HTTP request. Now `login` method() calls an internal method `attemptLogin()`. This method obtains login information from the callback object:

```
String userID = mcb.getUserName();
String userPwd = mcb.getUserPwd();
```

and loads the user database file and performs authentication. If authentication is successful this method returns `String` array with `userID` and `userDomain`, which is identifier to locate user in UG LDAP:

If `attemptLogin()` method is successful, `login()` method sets `userID` and `userDomain` info back into HTTP request by calling callback object's `setUserInfo()` method:

```
mcb.setUserInfo(userInfo[0], userInfo[2]);
```


Here, `userInfo[0]` is unique identified to locate user in UG LDAP. For example, `uid` and `userInfo[2]` is domain/organization name in UG LDAP under which user entry is available. This method sets this information as parameters in the HTTP request attribute:

```
public void setUserInfo(String uid,String domain){
    req.setAttribute("loginID", uid);
    req.setAttribute("userDomain", domain);
}
```

The authentication framework uses the `loginID` and `userDomain` to get the information from the request. All custom modules must use same names for these parameters. This is mandatory for Convergence' authentication framework.

and `login()` method returns `true`.

Now JAAS framework will call `commit()` method of `LoginModule`, where `UserPrincipal` object is populated into authenticated `Subject` object. This is mandatory for Convergence' authentication framework.

```
UserPrincipal userPrincipal = new UserPrincipal(mcb.getUserName());

if (!subject.getPrincipals().contains(userPrincipal)) {
    subject.getPrincipals().add(userPrincipal);
}
```

Here, `UserPrincipal` object takes `userName` of the user, which is nothing but unique identifier used to locate user entry in UG LDAP.

On successful completion of the `commit()` method, the control goes back to Convergence' authentication framework. This step marks the end of the authentication process. The authentication framework now has all the required information like: `loginID`, `userDomain` and authenticated `Subject` with `UserPrincipal` objects. The Convergence authentication framework then loads the user from the UG LDAP.

Compiling the sample custom module

Caution

If you need to change the core class file names provided in this article, note that you must appropriately refactor the code. Some of the files use objects created by other core classes of the custom authentication module.

Note

The paths used in the following example may differ for your installation

1. Create `/com/sun/comms/test` directory under `/<some_dir>`.

Note

The JAR file must be created by following the Java packaging layout rules. For example, the classes in this sample are packaged as `com.sun.comms`. So the Java files must be copied under the directory structure `:com/sun/comms`.

2. Copy the sample code provided earlier into the files `AppTestCallbackHandler.java`, `SunTestAuthCallBack.java`, and `SunTestLoginModule.java` under `<some_dir>/com/sun/comms/test` directory.
3. Compile the java class files.

```
# cd /<some_dir>/com/sun/comms/test
# javac -classpath
/opt/sun/comms/iwc/web-src/server/WEB-INF/lib/iwc.jar:/opt/sun/comms/
SunTestAuthCallBack.java SunTestLoginModule.java
```

4. Create a JAR archive.

```
cd /<some_dir>
#jar -cvf SunTestLogin.jar com
```

Note

If your custom authentication module requires any additional jar files or classes, these must be bundled along with the jar file.

5. Add the JAR file to deployed Convergence's libraries using Application Server's `asadmin` command.

```
asadmin set
server.applications.web-module.Convergence.libraries=<path-of-customA
```

Note

The custom authentication module must be on the system that can be accessed by Application Server. It is best to place the JAR archive on a location outside of the Convergence installation or deployed directories. To know more see [Application-Specific Class Loading in the Sun Java System Application Server 9.1 Developer's Guide](#).

Configuring the Sample Custom Authentication Module

This section describes the steps to configure the custom authentication module with Convergence. Since this example comes bundled with Convergence server, all you need to do to use this is to configure Convergence by setting the appropriate configuration parameters. The following are the instructions to enable the custom authentication module to use a file based authentication store.

1. Set the `auth.custom.service` name parameter in Convergence to indicate that a custom authentication module is being used.

```
./iwcadmin -o auth.custom.servicename -v "JAAS_CUSTOM"
```

2. Set the `auth.custom.loginimpl` parameter to the login module implementation created for custom authentication module.

```
./iwcadmin -o auth.custom.loginimpl -v
"com.sun.comms.test.SunTestLoginModule"
```

3. Set the `auth.custom.callbackhandler` parameter to the custom callback handler used for

the custom authentication module.

```
./iwcadmin -o auth.custom.callbackhandler -v  
"com.sun.comms.test.AppTestCallbackHandler"
```

4. Set the `auth.misc.CredentialFile` parameter to the directory where the authentication store is available. In this case, the authentication store is a file.



"Note"

Here, the value of `auth.misc.CredentialFile` is case sensitive. While reading these parameters inside custom authentication module the name should match the configuration.

```
./iwcadmin -o auth.misc.CredentialFile -v  
"/var/opt/SUNWiwc/config/userinfo.txt"
```

If you have created a custom authentication module for a different authentication store, you must follow the steps described below to enable the authentication module to work with Convergence.

1. Compile the custom authentication module source files and bundle them as a Java archive. See [Compiling the sample custom module](#).
2. Configure Convergence to use the custom authentication module by using the steps in section [Configuring the sample custom module](#). See
 - a. Set the `auth.custom.service` configuration parameter to "JAAS_CUSTOM".
 - b. Set the `auth.custom.loginimpl` configuration parameter to the custom login module implementation of the authentication module
 - c. Set the `auth.custom.callbackhandler` to the call back handler of the custom authentication module.
 - d. Set any miscellaneous parameters that you have used for your custom authentication module by setting the `auth.misc` configuration parameter.
3. Deploy the custom module. See [Deploying the Authentication Module in Application Server](#).

Deploying the Authentication Module in Application Server

Since the authentication module is in application server's classpath, restart the applicaiton server so that the module is updated in Application Server's classpath.

1. Restart application server.

```
# /opt/SUNWappserver/bin/asadmin stop-domain domain1  
# /opt/SUNWappserver/bin/asadmin start-domain domain1
```

Debugging and Troubleshooting the Custom Authentication Module

This section provides instructions on how to debug and troubleshoot the authentication module. For more information on debugging, see [Troubleshooting Convergence](#).

1. Set Convergence logging to `DEBUG` level.

```
# ./iwcadmin -o log.AUTH.level -v DEBUG
```

2. Restart the application server.

```
# /opt/SUNWappserver/bin/asadmin stop-domain domain1
# /opt/SUNWappserver/bin/asadmin start-domain domain1
```

3. Use the `tail` command to see the log messages generated.

```
# tail -f /var/opt/sun/comms/iwc/logs/iwc.log
```

Disabling the Custom Authentication Module

To change the custom authentication module to the default authentication module (LDAP) run following command.

```
./iwcadmin -o auth.ldap.enable -v true
```

Restart the application server to ensure that the changes take effect in your deployment.

```
# /root/glassfish3/bin/asadmin stop-domain domain1
# /root/glassfish3/bin/asadmin start-domain domain1
```

Summary

This section provides a recap of how to create a custom authentication module.

- Every custom authentication module should implement the following three classes:
 - o A class that implements LoginModule interface
 - o A class that extends HttpCallBackHandler class
 - o A(set of) class that implements Callback interface
 - o If your custom authentication module requires other classes that are specific to your implementation of the authentication module, the classes must be implemented.
- The `iwc.jar` should be there in classpath, while developing custom authentication module as it uses few Convergence specific classes like `HttpCallBackHandler` and `UserPrincipal`.
- As a best practice, it is good to bundle all dependent classes in a jar file. These should be made available in the web container's class path.
- Implementation of LoginModule interface and HttpCallBackHandler class needs to be configured using the command line interface.
- Any additional configuration specific to custom authentication module can be configured as Misc parameter using CLI
- The custom authentication module must set two HTTP request attributes, `userid` and `userDomain` after successful authentication.
- The `userDomain` must be a valid domain entry in UG LDAP under which, Convergence can uniquely locate user entry by using user id as an identifier.
- The custom authentication module must create `UserPrincipal` object using `userid` and set it in `Subject` after successful authentication.

References

[Schema Reference Guide](#)
[JAAS tutorial](#)

Chapter 14. Convergence Configuration Example - Creating an Authentication Realm in Access Manager

Convergence Configuration Example - Creating an Authentication Realm in Access Manager

Support for this Feature has been Deprecated

Access Manager is only supported on Convergence 2.x and earlier. For details, refer to [Deprecated Features in the Communications Suite](#).

These examples describe different Convergence configuration scenarios to create an authentication realm in Access Manager.



Note

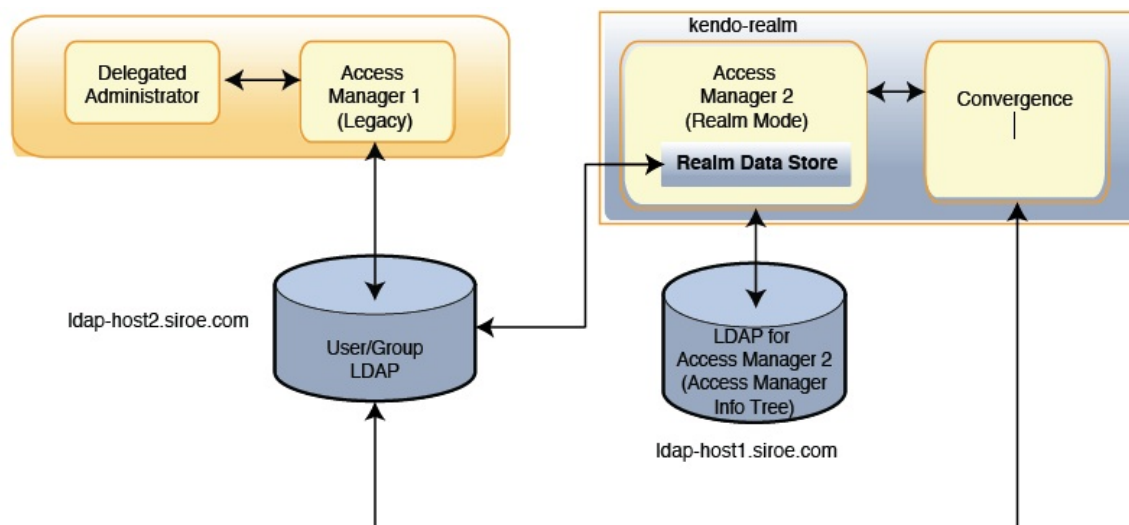
You can also use the following examples to configure Convergence with OpenSSO.

Topics:

- [Example: Access Manager DIT and User DIT are on Different LDAP Hosts](#)
- [Example: Access Manager DIT and User DIT are on the Same LDAP Host](#)

Example: Access Manager DIT and User DIT are on Different LDAP Hosts

In this example, an Access Manager authentication realm called `kendo-realm` is created with a DNS mapping for `siroe.com`. It uses two LDAP hosts: `ldap-host1.siroe.com` and `ldap-host2.siroe.com`. The LDAP host, `ldap-host1.siroe.com` holds the Access Manager DIT and `ldap-host2.siroe.com` host contains the User DIT.



Steps to Create an Authentication Realm in Access Manager when the Access Manager DIT and User DIT are on Different LDAP Hosts:

- [Installing Access Manager](#)
- [Configuring Data Stores](#)
- [Configuring Subjects Tab](#)
- [Configuring Authentication Tab](#)
- [Configuring Authentication Chaining](#)

Installing Access Manager

1. Install Access Manager (See [Get the Software](#) for the most up-to-date Access Manager version). Select Configure Now, select Realm Mode, and enter `ldap-host1.siroe.com` as the LDAP host.
2. Login to Access Manager Server as `amadmin` and create a new realm called `kendo-realm`.
3. After selecting `kendo-realm`, add a DNS mapping called `siroe.com`.

Configuring Data Stores

1. Change to the Data Stores tab and delete `amSDK1` plugin. Create a new data store plugin called `kendoDS`.
2. Select Directory Server with Access Manager Schema. Click Next.
3. Remove the current value from LDAP Server and add the new value for the `ldap-host2.siroe.com:389`.
4. Set the following LDAP credentials: Bind DN to `cn=Directory Manager`, LDAP Bind Password, and LDAP Organization DN to `o=siroe.com,dc=siroe,dc=com`. Save your updates.

Configuring Subjects Tab

- Go to Subjects tab under `kendo-realm` realm and verify all users in the `siroe.com` domain are listed.

Configuring Authentication Tab

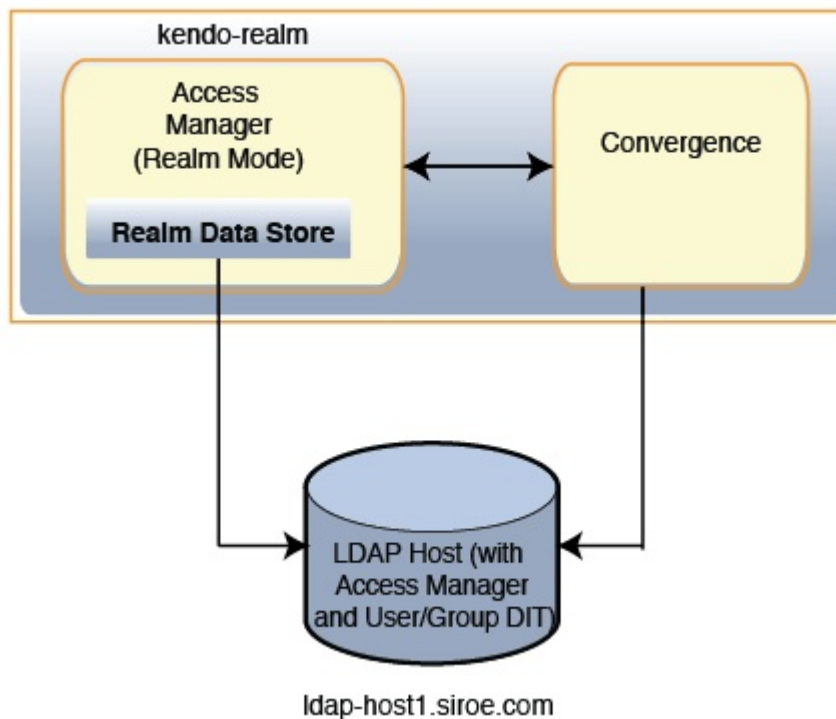
1. Go to Authentication tab under `kendo-realm` realm, scroll to Module Instances, click LDAP, remove the existing LDAP hosts and add new value `ldap-host2.siroe.com:389`.
2. Set the following LDAP credentials: LDAP Bind DN to `cn=Directory Manager`, LDAP Bind Password, and DN to Start User Search to `dc=siroe,dc=com`. Save your updates.

Configuring Authentication Chaining

1. Scroll to Authentication Chaining.
2. Click `ldapService`.
3. Ensure that instance is LDAP and criteria is required.
4. Log out from your Access Manager session.

Example: Access Manager DIT and User DIT are on the Same LDAP Host

In this example, an Access Manager authentication realm called `kendo-realm` is created, with a DNS mapping for `siroe.com`. It will use one LDAP host (`ldap-host1.siroe.com`) which will hold both the Access Manager DIT and the User DIT.



Steps to Create an Authentication Realm in Access Manager when the Access Manager DIT and User DIT are on the Same LDAP Host:

- Installing Access Manager
- Configuring Data Stores
- Configuring Subjects Tab
- Configuring Authentication Tab
- Configuring Authentication Chaining

Installing Access Manager

1. Install Access Manager (See [Get the Software](#) for the most up-to-date Access Manager version). Select Configure Now, select Realm Mode, and enter `ldap-host1.siroe.com` as the LDAP host. To set
2. Login to Access Manager Server as `amadmin` and create a new realm called `kendo-realm`.
3. After selecting `kendo-realm`, add a DNS mapping called `siroe.com`.

Configuring Data Stores

- Change to the Data Stores tab, click the `amsdk1` data store and enter `o=siroe.com, dc=siroe, dc=com` as the Organization DN. Save your updates.

Configuring Subjects Tab

- Go to Subjects tab under `kendo-realm` realm and verify all users in the `siroe.com` domain are listed.

Configuring Authentication Tab

1. Go to Authentication tab under `kendo-realm` realm, scroll to Module Instances, click LDAP.
2. Set the following LDAP credentials: LDAP Bind DN to `cn=Directory Manager`, LDAP Bind Password, and DN to Start User Search to `dc=siroe,dc=com`. Save your updates.

Configuring Authentication Chaining

1. Scroll to Authentication Chaining.
2. Click `ldapService`.
3. Ensure that instance is LDAP and criteria is required.
4. Log out from your Access Manager session.

Chapter 15. Writing a Pluggable SSO Module for Convergence

Writing a Custom SSO Module for Convergence

This information describes how to write a pluggable custom Single Sign-On (SSO) module for Convergence. Convergence offers two Single Sign-on mechanisms:

- Access Manager SSO (Legacy Mode and Realm mode). For details, see [How do I set up Access Manager SSO?](#)
- Messaging SSO (also referred to as Trusted Circle SSO). For details, see [Single Sign-on](#).



Note

By itself, the pluggable custom SSO module is not an SSO provider nor is it a replacement for any identity or access management services. Instead, the pluggable custom SSO module allows a site to use SSO between Convergence and another web application, where they all use the same SSO provider for identity or access management.

Topics:

- [SSO Mechanism in Convergence](#)
- [Implementing the Custom SSO Module](#)
- [Configuration](#)
- [Custom SSO Implementation Example](#)
- [Summary](#)

If you want your deployment to use a different SSO mechanism, you need to write and implement an SSO module. Internally, Convergence uses a proxy-auth mechanism to perform SSO with Communications Suite back-end servers. The back-end servers are: Messaging Server, Calendar Server, and Instant Messaging. Convergence enables you to write custom SSO modules to provide Single Sign-On.

SSO Mechanism in Convergence

As with any SSO-aware application, when a user is authenticated by using Access Manager for example, Convergence loads the authentication module to validate the user. On successful validation, the user is allowed to access the application. If the validation is not successful, the user is redirected to the login page.

Implementing the Custom SSO Module

Before designing a solution for the custom SSO module, Convergence SSO provider framework needs to be implemented:

- All custom SSO modules must implement SSOProvider interface.
- Convergence uses LDAP (Schema 1 or Schema 2) to store user data. This is called UG LDAP.
- UG LDAP uses the LDAP filter to identify user in UG LDAP.
- The SSO provider must provide the UG LDAP user identifier and domain identifier.
- After SSO validation the implementation must provide valid `uid` and valid domain/organization of the user in UG LDAP. This information will be obtained by SSO framework by invoking `getUId()`

- and `getDomain()` method of custom SSO Provider.
- The SSO implementation can use any other class that requires custom SSO module to work.

To write a custom SSO module:

1. Convergence defines a set of interfaces and class that need to be implemented. They are:
 - `SSOProvider.java`
 - `SSOListener.java`

Note
SSOProvider and SSOListener interfaces have to be implemented by the same class.

2. Configure the SSO module using the `iwadmin` command-line utility.

SSOProvider.java

```
package com.sun.comms.client.security.sso;

import java.util.Properties;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

/**
 * Custom SSO provider must implement this interface.
 */
public interface SSOProvider {
    /**
     * SSO framework in Convergence will invoke this method by passing
     all required SSO configuration, that are configured in configuration.
     * Implementation can store this info for future use. keys in
     initConfig are case sensitive.
     */
    public void init(Properties initConfig);

    /**
     * This method will be invoked by SSO framework after calling init()
     method. Implementation can have SSO validation code here.
     * If SSO validation or Single-Sign-On is successful, this method
     should return true.
     * If SSO validation succeeds implementation must not create http
     session here. It is taken care by SSO framework
     */
    public boolean SingleSignOn(HttpServletRequest
    request,HttpServletResponse response) throws SingleSignOnException;

    /**
     * This method will be invoked by SSO framework when user logs out
     of application and Single-Sign-Off is enabled in configuration.
     * If SSO validation or Single-Sign-Off is successful, this method
     should return true.
     * Implementation can perform SSO provider specific Single-Sign-Off
     here like cleanup SSO cookies in response.
     */
}
```

```

public boolean SingleSignOff(HttpServletRequest
request,HttpServletResponse response) throws SingleSignOffException;

/**
 * This method will be called by SSO framework if Single-Sign-On
succeeds. Implementation must provide a uid (user identifier) of the
user
 * in UG LDAP. This will be used by framework to load authenticated
user from UG LDAP.
 */
public String getUid();

/**
 * This method will be called by SSO framework if Single-Sign-On
succeeds. Implementation must provide a domain/organization (domain
identifier) of the user
 * in UG LDAP. Framework will use this to locate the user under this
domain in UG LDAP.
 */
public String getDomain();

/**
 * How much more time SSO token is valid with SSO Provider.
Currently not used by framework and hence can be ignored.
 */
public long getTimeLeft();

```

```
}
```

SSOListener.java

```
package com.sun.comms.client.security.sso;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;

/**
 * If SSO provider needs to perform some post Single-Sign-On operation.
 * This interface must be implemented.
 */
public interface SSOListener {
    /**
     * This method will be invoked by framework if Single-Sign-On
     * operation succeeded, user entry is loaded and http session is created.
     * Implementation can do postSignOn related tasks here e.g.
     * registering token listener for sso token notification etc.
     *
     * @param request - Http request for single sign on
     * @param response - Http response for single sign on
     * @param session- Convergence session that is created after
     * successful single sign on
     */
    public void postSignOn(HttpServletRequest
    request,HttpServletResponse response,HttpSession session);
}
```

SingleSignOffException - Exception thrown if SingleSignOff fails for any abnormal condition.

SingleSignOnException - Exception thrown if SingleSignOn fails for any abnormal condition.



Note

While implementing the custom SSO module, `iwcc.jar` should be available in the classpath of development environment. The `iwcc.jar` file requires SSO module classes.

Configuration

Once the required classes for the SSO module are created, you must configure it to work with Convergence server. To configure the SSO module, perform the following operations:

1. Configure the SSO module using the `iwccadmin` command:

```

iwadmin -W /location/pwdFile -o sso.enable -v "true"
iwadmin -W /location/pwdFile -o sso.enablesignoff -v "true"
iwadmin -W /location/pwdFile -o sso.servicename -v CUSTOM_SSO
iwadmin -W /location/pwdFile -o sso.ssoserviceimpl -v
"com.client.sample.CustomSSOProvider"
iwadmin -W /location/pwdFile -o sso.misc.<configname1> -v
"ConfigVal1"
iwadmin -W /location/pwdFile -o sso.misc.<configname2> -v
"ConfigVal2"

```



Note

All the miscellaneous configuration parameters such as <configname1> and <configname2> are case sensitive. These parameters should match the in the SSOProvider classes' init() method.

2. Create a jar file with all custom classes and supporting classes.
3. Copy the jar file to the Convergence
\$glassfish3InstallDir/glassfish/domains/domain1/applications/Convergence/
directory.

To Enable the sso.notifyserviceimpl Parameter

In addition, you might choose to enable the `sso.notifyserviceimpl` parameter, which can be any user defined class that is capable of listening to events from an SSO provider such as Access Manager. The class name is available through configuration properties passed to the custom SSOProvider implementation class (for example: `NotificationServiceImplementation` as key). In a custom SSO Provider implementation, you can obtain the class name, create the object, and register it as a listener for SSO events such as token expiration, single sign off notification, and so forth. This implementation is an SSO Provider specific class like `AMSDK`; it is different from `SSOListener`.

Custom SSO Implementation Example

The following template is an actual customer's configuration for a custom SSO implementation:

CustomSSOProvider.java

```

**** BEGIN com/client/sample/CustomSSOProvider.java ****

package com.client.sample;

import com.sun.comms.client.logging.IwcLogger;
import com.sun.comms.client.security.sso.SSOProvider;
import com.sun.comms.client.security.sso.SSOListener;
import com.sun.comms.client.security.sso.RenewSSO;
import com.sun.comms.client.security.sso.SingleSignOffException;
import com.sun.comms.client.security.sso.SingleSignOnException;
import com.sun.comms.client.security.sso.GeneralSSOException;
import javax.servlet.http.Cookie;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import javax.servlet.http.HttpSession;

```

```

import java.util.Properties;
import org.apache.commons.logging.Log;

public class CustomSSOProvider
implements SSOProvider,SSOListener,RenewSSO
{

    private static final Log logger =
IwcLogger.getLogger(IwcLogger.AUTH_LOGGER);

    public CustomSSOProvider() {
        logger.debug("Custom SSO Provider created");
    }

    public void init(Properties props)
    {
        logger.debug("init() called");
    }

    public String getDomain()
    {
        logger.debug("getDomain() called");
        return "domain.com";
    }

    public long getTimeLeft()
    {
        logger.debug("getTimeLeft() called");
        return 3600;
    }

    public String getUid()
    {
        logger.debug("getUid() called");
        return "uid";
    }

    public void refreshSSO(HttpServletRequest request,HttpServletResponse
response)
        throws GeneralSSOException {
        logger.debug("refreshSSO() called");
    }

    public boolean SingleSignOn(HttpServletRequest request,
HttpServletResponse response)
        throws SingleSignOnException
    {
        logger.debug("SingleSignOn() called");
        return true;
    }

    public void postSignOn(HttpServletRequest request, HttpServletResponse
response, HttpSession session) {
        String sessionid = session.getId();
        String token = (String) session.getAttribute("USER_TOKEN");
        String cookieValue = "jid=" + sessionid + ":token=" + token;;
    }
}

```

```

    logger.debug("postSignOn() called - create a new cookie SSOIwcAuth="
+ cookieValue);

    Cookie cookie = new Cookie("SSOIwcAuth", cookieValue);
    cookie.setPath("/");
    cookie.setDomain(".example.com");
    response.addCookie(cookie);
}

public boolean SingleSignOff(HttpServletRequest request,
HttpServletRequest response)
    throws SingleSignOffException
{
    logger.debug("SingleSignOff() called");
    return true;
}
}

**** END com/client/sample/CustomSSOProvider.java ****

[/tmp/test]$ cat compile.sh
#!/usr/bin/bash

echo "Compiling...."
/usr/jdk/instances/jdk1.6.0/bin/javac -classpath \
/opt/sun/comms/iwc/web-src/server/WEB-INF/lib/commons-logging-1.1.jar:/opt/
\
com/client/sample/CustomSSOProvider.java

```



```
echo "Creating JAR file"  
/usr/jdk/instances/jdk1.6.0/bin/jar -cvf customssso.jar \  
com/client/sample/CustomSSOProvider.class
```

Summary

Convergence enables you to write your own custom SSO authentication modules. To write a custom SSO module, the Convergence SSO framework requires that you implement the following interfaces:

- `SSOProvider`
- `SSOListener`

Additionally, you can also use other classes that help you to implement the SSO module. Finally, you need to configure Convergence to use the custom SSO module that you created using the `iwcadmin` command.

Chapter 16. Administering Convergence Display Name to Map to LDAP displayName

Administering Convergence Display Name to Map to LDAP displayName

The following information describes how to administer the Convergence Display Name to map to LDAP displayName:

- [To Configure Convergence Display Name](#)
- [To Configure the Corporate Address Book to Perform displayName Search](#)

To Configure Convergence Display Name

The following table describes new configuration parameters that have been added for display name mapping enhancements to the Convergence display name.

Table: Configuration parameters for Mapping Convergence Display Name from cn to LDAP displayName

Property	Description
general.screenname	Defines the LDAP attribute used for the screenname, also referred to as displayname. Located in the <code>useroption-mappings.properties</code> file.
ScreenNameEditable	Determines if the display name in the Options page is editable or not. Default is false.

With these configuration parameters, you are able to modify the Convergence display name in the following ways:

1. If the LDAP displayName parameter does not contain a value, use the cn attribute as a fall back. If the user modifies the Convergence display name, then the LDAP displayName attribute is populated.
2. The ability to edit the Convergence display name is disabled by default. To enable it, set the following `iwcadmin` command:

```
iwcadmin -o client.screennameeditable -v true
```

To Configure the Corporate Address Book to Perform displayName Search

To configure the corporate address book for search, modify the following parameters by editing the `config/templates/ab/corp-dir/xlate-inetorgperson.xml` file:

1. Search displayName and cn where displayName has a different LDAP attribute from cn. Modify:

```
<entry>
...
<displayname>db:your_ldap_displayname_attribute</displayname>
<cn>db:your_ldap_cn_attribute</cn>
...
</entry>
```

2. Search `displayName` only where `displayName` has a different LDAP attribute from `cn`.
In this scenario, no modification is required.
3. Search `displayName` only where `displayName` has the same LDAP attribute `cn`.
In this scenario, no modification is required.

Chapter 17. Setting Up Multiple Corporate Directories in Convergence

Setting Up Multiple Corporate Directories in Convergence

Topics:

- [Adding a Corporate Directory](#)
- [Configuring Multiple Corporate Directories](#)
- [Disabling Corporate Directory \(Newly Added or Default\)](#)

Adding a Corporate Directory

To add a corporate directory or to use the directory server other than the user group directory server, set the following configuration parameters:

- `ab.corpdir.[<identifier>].ldaphost`
- `ab.corpdir.[<identifier>].ldapport`
- `ab.corpdir.[<identifier>].ldapbinddn`
- `ab.corpdir.[<identifier>].ldapbindcred`

The following example has the configuration parameters settings:

```
iwcadmin -W /location/mypasswordfile -o ab.corpdir.[default].ldaphost
-v host.example.com
iwcadmin -W /location/mypasswordfile -o ab.corpdir.[default].ldapport
-v 400
iwcadmin -W /location/mypasswordfile -o ab.corpdir.[default].ldapbinddn
-v "cn=Directory Manager"
iwcadmin -W /location/mypasswordfile -o
ab.corpdir.[default].ldapbindcred -v xyzxyz
```

The corporate directory can be configured with multiple directory servers. In the above example `default` is used to identify corporate directory configuration for `host.example.com`.



Note

For a single corporate directory configuration, you must use `default` as the identifier.

Configuring Multiple Corporate Directories

1. To configure multiple corporate address books, set following parameters:

```
ab.corpdir.[<identifier1>].ldaphost
ab.corpdir.[<identifier1>].ldapport
ab.corpdir.[<identifier1>].ldapbinddn
ab.corpdir.[<identifier1>].ldapbindcred
ab.corpdir.[<identifier1>].urlmatch
ab.corpdir.[<identifier1>].searchattr
ab.corpdir.[<identifier1>].displayname
```

**Note**

The value for the `urlmatch` configuration parameter must be unique.

- To search from Root: `ldap://corp-directory1`
- To search from dn `ou=people,o=ab.org`:
`ldap://somehost:390/ou=people,o=ab.org`

Format for `urlmatch` is `ldap://<unique_value>` or `ldap://host:port/DN`:

For example:

```
-o ab.corpdir.[corpdir1].ldaphost -v budgie.india.example.com
-o ab.corpdir.[corpdir1].ldapport -v 389
-o ab.corpdir.[corpdir1].ldapbinddn -v "cn=Directory Manager"
-o ab.corpdir.[corpdir1].ldapbindcred -v netscape
-o ab.corpdir.[corpdir1].urlmatch -v ldap://corpdir1
-o ab.corpdir.[corpdir1].searchattr -v entry/displayname,@uid
-o ab.corpdir.[corpdir1].lookthru limit -v 3000
-o ab.corpdir.[corpdir1].displayname -v "Second Corporate Book"
```

2. Restart Application Server.

Note

In some cases, the corporate directories might not display. The workaround is to set the `urlmatch` configuration parameter, beginning with the default URL match value (`ldap://corpdirectory`). For example, for an organization adding multiple address books from three different entities: `CommerceDept`, `IntlTradeDiv`, and `DivofEmployment`, the `urlmatch` is set to the following:

```
ab.corpdir.[CommerceDept].urlmatch =
ldap://corpdirectorycommerce \\
/ou=People,ou=CommerceDepartment,
o=cat.example.gov,dc=divemp,dc=gov
ab.corpdir.[IntlTradeDiv].urlmatch =
ldap://corpdirectoryitd \\
/ou=People,ou=ITD,ou=CommerceDepartment,
o=cat.example.gov,dc=divemp,dc=gov
ab.corpdir.[DivofEmployment].urlmatch =
ldap://corpdirectorydivemp \\
/ou=People,ou=DivofEmployment,ou=CommerceDept,
o=cat.example.gov,dc=divemp,dc=gov
```

Note

Even though the Corporate Directories are properly set up and work as designed, they may display errors in the `iwcc.log` or the Firebug log. See: [12296971](#).

Disabling Corporate Directory (Newly Added or Default)

To disable a corporate directory, set the following Convergence parameter to `false`:

```
ab.corpdir.[<identifier>].enable
```

Chapter 18. Convergence Performance Tuning

Tuning Sun GlassFish Server to Enhance Convergence Performance

These performance tuning guidelines are for Convergence 2.x and earlier.

Contributed by Russ Petruzzelli

Russ Petruzzelli is an engineer currently conducting performance tests on Convergence.

This document contains the following sections:

- [Convergence Performance Tuning Overview](#)
- [Tuning Sun GlassFish Server Config Parameters](#)
 - [Tuning Parameters for HTTP Service-Request Processing](#)
 - [Tuning Parameters for the HTTP Listener](#)
 - [Configuring Sun GlassFish Server to Compress Files Sent to the Client](#)
- [Enhancing Browser-Side Caching of Static Files](#)
- [Tuning the JVM Options](#)
 - [Activating the Garbage Collection Log](#)
 - [Invoking the Java HotSpot Server VM](#)
 - [Tuning the JVM Heap Size](#)
 - [Setting Garbage Collection Algorithms](#)
 - [Setting the Permanent Generation Size](#)
 - [Tuning the JVM RMI GC Interval Parameters](#)
 - [Sample List of JVM Options](#)
- [Miscellaneous Performance Tuning Tips](#)
- [Additional Tuning Tips](#)

Convergence Performance Tuning Overview

Recent advances in storage, servers, and Java have affected how one tunes web containers for middleware. There are systems with multi-threaded chips having 32 effective processors, operating systems with virtualized containers like Solaris zones, and file systems like ZFS that can spread files out over many disks. Java 1.6 can automatically adjust itself based on dynamic conditions. The tuning options available are many, and you must choose what works for you.

The tuning guidance presented here offers options to examine and configure. However, these options do not address specific hardware configurations and are not guaranteed to improve performance for any particular hardware configuration, performance load, or type of load on your system.

Try out the options and tips that apply to your deployment, test their impact on performance, and tweak the option values as needed.

Performance Tuning for Sun GlassFish Server

The Convergence application itself is a Java application bundled into a war file that runs inside a web container. Currently, the supported web container is the Sun GlassFish Server 2.1.1. This document describes how to optimize the GlassFish server environment to allow Convergence to deliver the best possible performance.

**Note**

Beginning with Convergence 2, Sun GlassFish Server 2.1.1 is required.

For information about how the Convergence components are deployed to GlassFish server, see [Introduction to the Convergence Service](#).

In general, you can follow the tuning information in the *Sun Java System Application Server 9.1 Performance Tuning Guide*. Additional references are listed at the end of this document.

Use Sun GlassFish Server's administration browser interface or command-line interface rather than directly editing the `domain.xml` file to make the changes described below. The changes do not take effect until the domain instance has been restarted. Hardware is assumed to have at least 2 CPUs and 2G of memory (a Server-Class machine).

Make the modifications described below to GlassFish Server domain/config/port in which Convergence is running. The operating system in these examples is Solaris 10. These instructions use GlassFish Server's administration browser interface where possible. If you want to use the command-line interface, see the [asadmin utility](#).

Tuning Sun GlassFish Server Config Parameters


This section contains the following topics:

- [Tuning Parameters for HTTP Service-Request Processing](#)
- [Tuning Parameters for the HTTP Listener](#)
- [Configuring Sun GlassFish Server to Compress Files Sent to the Client](#)

Tuning Parameters for HTTP Service-Request Processing

On the Request Processing tab in the HTTP Service page tune the following HTTP Request Processing settings. (To navigate to this page, in the GlassFish Admin Console, select **Configuration > HTTP Service**.)

- **Thread Count: 40 ## General Range: 20-80**
- **Initial Thread Count: 8**
- **Thread Increment: 2**
- **Request Timeout: 20** (Change this setting from the default value of 30 seconds.)
- **Buffer Length: 16384** (Change this setting from the default of 8192 kilobytes.)

 Here is good information from [Scott Oaks's blog](#):

The request threads run HTTP requests. You want "just enough" of those: enough to keep the machine busy, but not so many that they compete for CPU resources – if they compete for CPU resources, then your throughput will suffer greatly. Too many request processing threads is often a big performance problem...

How many is "just enough"? It depends, of course – in a case where HTTP requests don't use any external resource and are hence CPU bound, you want only as many HTTP request processing threads as you have CPUs on the machine. But if the HTTP request makes a database call (even indirectly, like by using a JPA entity), the request will block while waiting for the database, and you could profitably run another thread. So this takes some trial and error, but start with the same number of threads as you have CPU and increase them until you no longer see an improvement in throughput.

Since Convergence communicates extensively with back-end messaging and calendar resources request blocking could be an issue. You will need to monitor your own deployment and adjust the Thread Count accordingly.

Tuning Parameters for the HTTP Listener

Increase the HTTP listener acceptor-threads. The default value is: `acceptor-threads="1"`.

In the HTTP Service section of the GlassFish Server Admin Console, on the listener for the port for Convergence (such as 8080):

Start with a value of 2, monitor the performance, and consider increasing to 4 or more.

To configure this setting, select the following items in the GlassFish Server Admin Console:

Configuration > HTTP Service > HTTP Listeners > Listener1.

(`HTTP-listener-1` is assumed to be in use for Convergence.)

Take these steps:

- Increase the acceptor-threads value to the number of CPUs on the system. (This has not been tested beyond 4.)
- If you have only one interface (NIC), change the default 0.0.0.0 IP address to your IP for the host. For example: `192.18.75.103`.

Configuring Sun GlassFish Server to Compress Files Sent to the Client

You can improve server response times by reducing the size of the HTTP response. One way is to compress file size by using the gzip utility. Not all files should be compressed (for example, images and some PDF files), but many files are compatible with this method.

To decide if this technique is right for you, search the Web for "gzip best practices" to find out more information. If you choose to implement this practice, realize that the server does more work to compress files into gzip format, which might impact the server's scalability under heavy loads.

To compress files sent to the client by using the GlassFish Server Administration Console:

1. In a browser, connect to the GlassFish Server Administration Console. GZIP is turned on by adding additional properties to the `http-listener` element.
2. In the Administration Console, navigate to the HTTP Listeners:

Configuration >> HTTP Service >> HTTP Listeners

3. Add the following properties the `httplistener` for Convergence (normally `httplistener1`):

```
compression on
minCompressionSize 1000
compressableMimeType
"text/html,text/xml,text/css,text/javascript,text/json"
```

Alternatively, you can use the command line to compress files sent to the client by running the following commands:

```
asadmin set server.http-service.http-listener.http-listener-1.property
.compression=on
asadmin set server.http-service.http-listener.http-listener-1.property
.minCompressionSize=1000
asadmin set server.http-service.http-listener.http-listener-1.property
.compressableMimeType="text/html,text/xml,text/css,text/javascript,text/js"
```

For more information, see [http-listener](#) in the *Sun Java System Application Server 9.1 Administration Reference*.

Enhancing Browser-Side Caching of Static Files

This section explains how to use *Expires headers* to enable long-term caching of static files in the browser.

When this feature is implemented, GlassFish Server includes the Expires header in the HTTP response. The Expires header allows files cached in the browser to remain in cache for the time specified in the `ExpiresFilter.class` file.

Task Summary

To enable Expires headers, you must perform these tasks:

- Modify the Convergence application's web-configuration file deployed to the GlassFish Server's domain directory
- Install a new class file

To Enable Expires Headers

The following steps assume that Convergence is configured in the GlassFish Server's `domain1` directory. (By default, the GlassFish Server's domain directory on Solaris is `/opt/SUNWappserver/domains/domain1`).

Take these steps:

1. Add the following filter rule to the `<app_server_base>/domains/domain1/config/default-web.xml` file, directly below the existing Servlet Mappings rules:

```

<!-- Enable Expires Headers for Convergence files -->
<filter>
  <filter-name>ExpiresFilter</filter-name>
  <filter-class>iwc.ExpiresFilter</filter-class>
</filter>
<filter-mapping>
  <filter-name>ExpiresFilter</filter-name>
  <url-pattern>/iwc_static/js/*</url-pattern>
  <url-pattern>/iwc_static/layout/*</url-pattern>
  <dispatcher>REQUEST</dispatcher>
  <dispatcher>FORWARD</dispatcher>
</filter-mapping>

```

2. Create a subdirectory named `iwc` under `<app_server_base>/domains/domain1/lib/classes` directory.
3. Copy the `ExpiresFilter.class` file to the directory `<app_server_base>/domains/domain1/lib/classes/iwc`.
4. Restart the GlassFish Server.



Note

The `ExpiresFilter.class` file has a two-year expiration time set. The Java source code is provided if you desire to set your own time interval. Modify the line `c.set(c.get(Calendar.YEAR)+2, c.get(Calendar.MONTH))` as desired.



Note

The `ExpiresFilter.class` file and Java source code provided here have been copied from the original files and modified. This code is not supported or maintained by Oracle. For more information about the history of this filter, visit the author's blog [here](#).

Tuning the JVM Options

This section contains the following topics:

- [Activating the Garbage Collection Log](#)
- [Invoking the Java HotSpot Server VM](#)
- [Tuning the JVM Heap Size](#)
- [Setting Garbage Collection Algorithms](#)
- [Setting the Permanent Generation Size](#)
- [Tuning the JVM RMI GC Interval Parameters](#)
- [Sample List of JVM Options](#)

Activating the Garbage Collection Log

This log has negligible impact on server performance and provides valuable debugging and performance history data.

Add the following entry, using your own path. For example:

```
<jvm-options>-Xloggc:/opt/SUNWappserver/domains/domain1/logs/gclog</jvm-opt
```

Note: This log is overwritten each time the server is restarted.

Invoking the Java HotSpot Server VM

Make sure that the JVM options in the `domain.xml` file for the GlassFish Server instance specify `-server`, not `-client`:

```
<jvm-options>-server</jvm-options>
```

Server Class machines are defined as having at least 2 CPUs and 2 GB of memory.

Remove the `-client` option if present and add the `-server` option. You can verify what mode the server actually started with by running:

```
grep 'HotSpot' server.log"*,
```

This will show either `...Client VM...` or `...Server VM....`

Activating the 64-bit JVM Mode



Note

Glassfish Enterprise Server is not supported on 64-bit JVMs on Red Hat Linux. See [Supported Platforms](#) for more information.

To configure and activate a 64-bit JVM, take these steps:

1. On Solaris, you can verify that the operating system kernel is running in 64-bit mode by running:

```
/usr/bin/isainfo -kv
```

2. If needed, download and install the 64-bit jvm files on the JVM instance used by the GlassFish Server on the machine. Verify the 64-bit files are available by running:

```
"/<appserver_java_dir>/java -d64 -version"
```

3. On the GlassFish Server, replace the JVM option, `-server` (or `-client`), with `-d64`



Note

It is recommended that you run the latest version of the JDK with Convergence. Currently, that is JDK 1.6 Update 12. JDK 1.6 Update 12 contains updates that improve performance over previous JDK releases.

Tuning the JVM Heap Size

In the GlassFish Server Admin Console, under **Common Tasks**, select **Application Server >> JVM Settings Tab >> JVM Options Sub-Tab >> Add/Modify** the options...

The min and max heap size options are: `-XmsNNNNm` and `-XmxNNNNm`.

Generally, set max heap as large as possible given the available memory on your machine. (Setting the min equal to the max improves jvm efficiency.) Total memory used is equal to the (JVM native heap space) + (Java Heap) + (Permanent Generation space). Leave room for the operating system and any other applications running on the machine too. Don't forget to reserve memory for the OS and avoid memory swapping at all costs.

For example, you could set the heap size options to

```
<jvm-options>-Xms2048m -Xmx2048m</jvm-options>
```



Note

JVMs running in 32-bit mode are limited to 4GB of memory. Convergence is installed (but not activated) with the full 64-bit JVM files.)

Setting Garbage Collection Algorithms

To increase the stability and predictability of the heap size and the ratios of its configuration, you can explicitly set the following parameters:

- `-XX:+UseParallelGC`. --This parameter is used by default on a machine qualifying as Server Class. This default collector is sufficient.
- `-XX:+UseParallelOldGC`. --This statement makes the tenured generation run GC in parallel, too. This is the default in JDK 6. In `jdk1.5_u6` and greater you need to explicitly specify this option.
- `-XX:-UseAdaptiveSizePolicy`. --Turn **off** GC ergonomics. Note the minus sign in this statement. Specify `min` and `max` values explicitly. See the summary below.
- `-XX:NewRatio=1` -- Optimize the Young Generation Size. Using a ratio (as opposed to setting a numerical size with `NewSize`) allows for the maximum possible young generation size relative to the overall heap, no matter your `MaxHeap` size.

Tests show that most of the objects created for Convergence are short-lived, thus benefiting from a larger young generation size.



Note

To reduce full GC time, see: [When Tuning Convergence, What are the Recommendations for Reducing Full GC Time?](#)

The `NewRatio` means {New:Old}. So, when `NewRatio=1`, then `new:old = 1:1`. Therefore, the young generation size = 1/2 of the total Java heap. The young generation size can never be larger than half the overall heap because - in the worst case - all the young generation space could be promoted to the old generation. Therefore, the old generation must be at least as large as the young generation size.

For more information about the `NewRatio` option, refer to:

<http://java.sun.com/javase/technologies/hotspot/vmoptions.jsp>. Monitor your own heap usage with the Jconsole monitor.

Setting the Permanent Generation Size

Be aware that `MaxPermSize` may need to be increased. JVM Efficiency is improved by setting `PermSize` equal to `MaxPermSize`. Start with the default, observe `PermSpace` usage and adjust accordingly:

```
<jvm-options>-XX:PermSize=192m -XX:MaxPermSize=192m</jvm-options>
```

Use a tool such as `jconsole` or `VisualVM` to determine how best to optimize your own system. For more details, see [Miscellaneous Tips](#), below.

Tuning the JVM RMI GC Interval Parameters

It is better if full Garbage Collections (GCs) on the Java heap do not occur frequently and are not called explicitly. It is best to let the JVM decide when to do full garbage collections.

Unfortunately, the GlassFish Server has a couple of JVM options for RMI applications that invoke full GCs often. If you are not running any applications using RMI, you should increase the `rmi.dgc...` values, or configure them never to occur.

The default intervals are:

- Before JDK 1.6: 1 minute
- JDK 1.6: 1 hour

These intervals are increased to 10 hours:

```
<jvm-options>-Dsun.rmi.dgc.server.gcInterval=36000000</jvm-options>  
<jvm-options>-Dsun.rmi.dgc.client.gcInterval=36000000</jvm-options>
```



Note

Removing them entirely from the `domain.xml` file will cause the full GCs to occur at the default interval.

You can also use either of the following two options to prevent the full GCs invoked for RMI:

- Disable explicit GC by adding:

```
<jvm-options>-XX:+DisableExplicitGC</jvm-options>
```

- Use the 1.6 JVM and set:

```
-XX:+UseConcMarkSweepGC  
-XX:+ExplicitGCInvokesConcurrent
```

`ExplicitGCInvokesConcurrent` is only available in JVM 1.6+.

Ramifications of Disabling Explicit GCs

You should also consider the ramifications of disabling explicit GCs. When another application is connecting to the Application Server with RMI, memory for objects in the Application Server's heap will not be released and the calling application will not be able to release the reference to that object, thus

possibly causing memory overflow on the other application.

Sample List of JVM Options

The following list is a sample section of the `domain.xml` file's JVM options:

```
<jvm-options>-server</jvm-options>
<jvm-options>-XX:+DisableExplicitGC</jvm-options>
<jvm-options>-XX:+UseParallelGC</jvm-options>
<jvm-options>-XX:+UseParallelOldGC</jvm-options>
<jvm-options>-XX:-UseAdaptiveSizePolicy</jvm-options>
<jvm-options>-Xms1024M -Xmx1024M</jvm-options>
<jvm-options>-XX:NewRatio=1</jvm-options>
<jvm-options>-XX:PermSize=192M</jvm-options>
<jvm-options>-XX:MaxPermSize=192M</jvm-options>
<jvm-options>-Xloggc:/opt/SUNWappserver/domains/domain1/logs/gclog</jvm-opt
```

Miscellaneous Performance Tuning Tips

Class Data Sharing

Class data sharing (CDS) is a new feature in J2SE 5.0. CDS applies only when the "Java HotSpot Client VM" is used. Since we recommend using the "Java HotSpot Server VM," this feature does not apply.

Inspect Settings

Inspect your settings with the following commands:

To see all Java processes running on your machine:

```
jps -mlvV
```

To view your settings in effect for the JVM for the GlassFish Server:

```
jmap -heap <java-process-id for the app server>.
```

Monitoring the JVM

JConsole is a built-in JVM monitoring tool in Java 1.5 and higher. On the SUT, set the display variable to your local machine and run the following command: `jconsole`

For more information, read the following articles:

- [Using JConsole to Monitor Applications](#)
- [Monitoring and Management Using JMX](#)
- [VisualVM - The All-In-One Java Troubleshooting Tool](#)

UseConcMarkSweepGC

The intrepid system administrator may want to consider using `UseConcMarkSweepGC` instead of `UseParallelGC`. For details, see [Tuning Garbage Collection with the 5.0 Java Virtual Machine](#).

New GC Algorithm

Look out for a new GC algorithm in Java 1.7 called G1. It is estimated to be released in 2009.

Additional Tuning Tips

You can find detailed guidance and additional performance tuning tips in these documents:

- [Sun Java System Application Server 9.1 Performance Tuning Guide](#)
- [Java Virtual Machines](#)
- [Frequently Asked Questions About the Java HotSpot VM](#)

Additional References

- [Planning a Convergence Sizing Strategy](#)
- [Tuning Garbage Collection with the 5.0 Java Virtual Machine](#)
- [Ergonomics in the 5.0 Java Virtual Machine](#)
- [J2SE 5.0 Performance White Paper](#)
- ["Monitoring and Management Tools" in JDK Tools and Utilities](#)
- [Java HotSpot VM Options](#)
- [Jon Masamitsu's Weblog: Rationale for GC settings](#)

ExpiresFilter.java

ExpiresFilter.java

ExpiresFilter.java

```
package iwc;

import java.io.IOException;
import java.text.SimpleDateFormat;
import java.util.Calendar;
import java.util.Date;
import java.util.TimeZone;
import javax.servlet.Filter;
import javax.servlet.FilterChain;
import javax.servlet.FilterConfig;
import javax.servlet.ServletException;
import javax.servlet.ServletRequest;
import javax.servlet.ServletResponse;
import javax.servlet.http.HttpServletResponse;

/**
 * The expires filter adds the expires HTTP header based on the
 * deployment policy.
 * Many sites have a fixed deployment schedule where deployments take
 * place
 * based on timed regular intervals. This filter adds the expires header
 * of the
 * next possible deployment time, to support browser caching.
 * @author Chris Webster
 */
public class ExpiresFilter implements Filter {

    private FilterConfig filterConfig;
    private String expires;
    private long nextDeploymentTime;

    public ExpiresFilter() {
        expires = nextDeploymentTime();
    }

    private String nextDeploymentTime() {
        // assume next deployment is M-F at 09:45
        Calendar c = Calendar.getInstance();

        int dayOffset = 1;

        if (c.get(Calendar.DAY_OF_WEEK) == Calendar.FRIDAY) {
            dayOffset+=2;
        }
    }
}
```

```

    if (c.get(Calendar.DAY_OF_WEEK) == Calendar.SATURDAY) {
        dayOffset++;
    }

    c.add(Calendar.DAY_OF_MONTH, dayOffset);
    c.set(c.get(Calendar.YEAR)+2, c.get(Calendar.MONTH),
        c.get(Calendar.DAY_OF_MONTH), 9, 45);

    nextDeploymentTime = c.getTimeInMillis();

    String pattern = "EEE, dd MMM yyyy HH:mm:ss z";
    SimpleDateFormat sdf = new SimpleDateFormat(pattern);
    sdf.setTimeZone(TimeZone.getTimeZone("GMT"));
    return sdf.format(c.getTime());
}

private void addCacheHeaders(ServletRequest request, ServletResponse
response)
    throws IOException, ServletException {

    HttpServletResponse sr = (HttpServletResponse) response;
    sr.setHeader("Expires", expires);
    long now = (new Date()).getTime();

    long expireTime = nextDeploymentTime - now;
    expireTime /= 1000;
    sr.setHeader("Cache-Control", "max-age="+
        Long.toString(expireTime)+";public;must-revalidate;");
}

/**
 *
 * @param request The servlet request we are processing
 * @param response The servlet response we are creating
 * @param chain The filter chain we are processing
 *
 * @exception IOException if an input/output error occurs
 * @exception ServletException if a servlet error occurs
 */
public void doFilter(ServletRequest request, ServletResponse response,
    FilterChain chain)
    throws IOException, ServletException {

    addCacheHeaders(request, response);
    chain.doFilter(request, response);
}

/**
 * Return the filter configuration object for this filter.
 */
private FilterConfig getFilterConfig() {
    return filterConfig;
}

/**
 * Set the filter configuration object for this filter.

```

```

*
* @param filterConfig The filter configuration object
*/
private void setFilterConfig(FilterConfig filterConfig) {
    this.filterConfig = filterConfig;
}

/**
 * Destroy method for this filter
 *
 */
public void destroy() {
}

/**
 * Init method for this filter
 *
 */
public void init(FilterConfig filterConfig) {
    setFilterConfig(filterConfig);
}

/**
 * Return a String representation of this object.
 */
@Override
public String toString() {
    if (getFilterConfig() == null) {
        return ("ExpiresFilter()");
    }
    StringBuffer sb = new StringBuffer("ExpiresFilter(");
    sb.append(getFilterConfig());
    sb.append(")");
    return (sb.toString());
}
}

```

}

Chapter 19. Convergence Cluster Deployment Example

Convergence Cluster Deployment Example

This article describes how to deploy and configure Convergence on a GlassFish Server cluster. The cluster feature enables you to create highly available and scalable deployment architectures.

Topics:

- [About This Deployment Example](#)
- [Prerequisites and Deployment Example Architecture](#)
- [Setting up the Cluster](#)
- [Deploying Convergence on the GlassFish Server Cluster](#)
- [Client Files](#)
- [Adding a Convergence Patch in a Cluster Deployment](#)
- [Known Issues](#)

About This Deployment Example

This example assumes that you are familiar with the following tasks:

- Installing and configuring Convergence. See [Communications Suite 7.0.6 Installation Guide](#) for information about installing and configuring Convergence.
- Setting up clusters using GlassFish Server. For more information on clustering in GlassFish Server, refer to:
 - [Clustering in GlassFish Version 2](#)



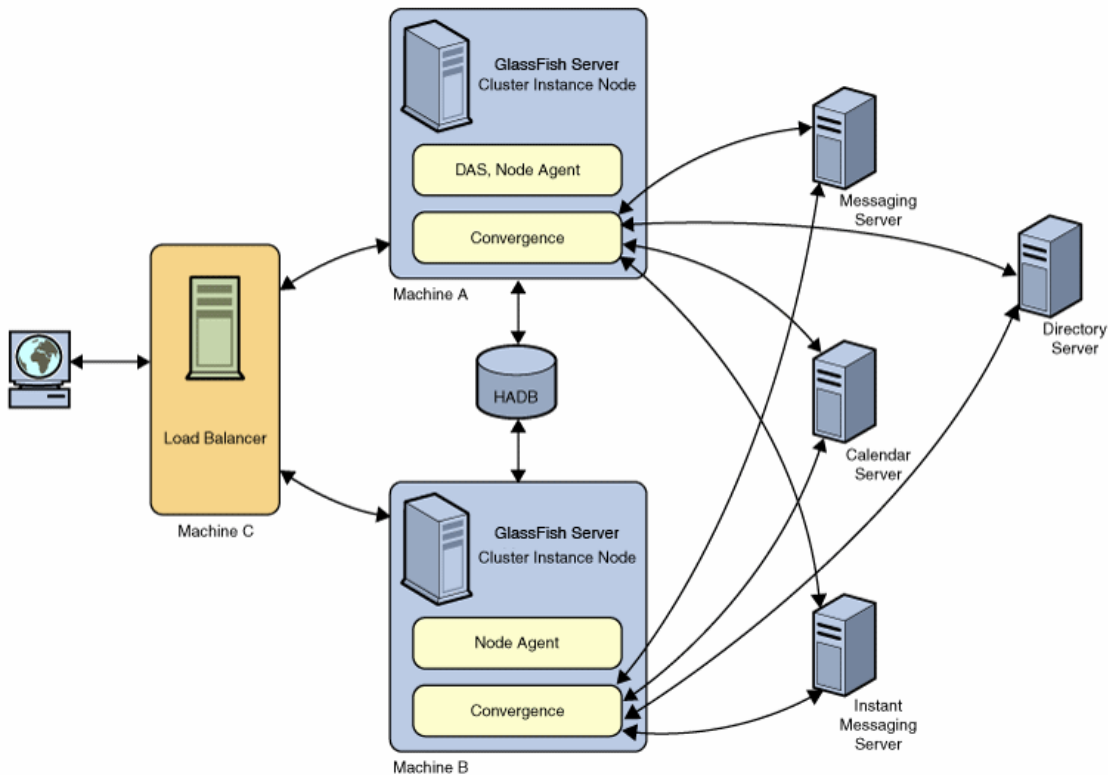
Note

Beginning with Convergence 2, the supported web container is GlassFish Server. However, the Application Server 9.1 documents listed in this deployment example are still relevant.

Prerequisites and Deployment Example Architecture

The hardware and software requirements for configuring Convergence in a GlassFish Server cluster is the same as configuring a default Convergence deployment. However, additionally you will need to install Oracle iPlanet Web Server. In this example, web server is used as a load balancer.

The next figure shows the deployment architecture:



In the above deployment architecture, Machine A and Machine B are part of the cluster. Machine A is configured with Domain Administration Server (DAS) and node agent. Machine B is configured with node agent. The cluster uses HADB for storing session-specific information.

Machine C is an instance of web server, on which a load balancer plug-in is configured by using the Machine A and Machine B information. The load balancer plug-in is available as part of the GlassFish Server installer. The load balancer routes all incoming requests to the backend cluster instances.

Setting up the Cluster

Follow these steps to set up the cluster:

1. Start the domain administration server on Machine A.
2. Start node agents on Machine A and B.
3. Create a cluster using the `asadmin` command-line utility.
4. Create the GlassFish Server instances by using the `asadmin` command.
5. Create the HADB database for the cluster.

For more information about setting up and working with clusters, see [Working with Clusters](#) in the *Java System Application Server 9.1 High Availability Administration Guide*.

Deploying Convergence on the GlassFish Server Cluster

Deploying Convergence on a cluster is different from deploying Convergence on a single instance of GlassFish Server. After installing Convergence, you must run the `init-config` command to configure Convergence. During configuration, you must supply details at appropriate stages (detailed below) in the configuration wizard, as described in the [Convergence Initial Configuration Documentation](#).

The following sections provide information on the details you must provide in in the initial configuration wizard for a clustered setup.

**Note**

Do not run the `init-config` command on each cluster instance host. Run `init-config` only on the host running DAS.

Panel 2: Select the directory to store configuration and data files.

Select the directory where you want to store the configuration and data files. The default data and configuration directory is located in the `/var/opt/sun/comms/iwc` directory.

**Note**

The data and configuration information must exist on the same path on all the instances in the cluster. If you make changes to any of the configuration on one instance of the cluster, the same change has to be made to the other cluster instances.

You can also have the configuration and data directories on a networked mounted file system that is accessible to all instances of the cluster. This is currently not supported due to a requirement of unique Instant Messaging Component JID in the Instant Messaging gateway configuration (`httpbind.conf`). See [Known Issues](#).

Panel 5: Configuration Details

In this panel, you must type the **Server Target Name** as the name of the cluster. The cluster name is mandatory in a cluster setup.

**Note**

While specifying the Server Target Name to install Convergence, if you choose to deploy and configure Convergence on an instance other than DAS (instance name: 'server'), then the content `iwc_static` is not copied to the `app-base-dir/nodeagent/node/instance/docroot`. This is because of a timestamp issue described in a GlassFish Server RFE (6871360).

Meanwhile, the workaround is to change the target instance (as shown below) by using the GlassFish Server Admin Console, after installation is completed:

Select Applications > Web applications > Convergence > Target tab > Manage Targets button.

Failure to do so causes Convergence to become unavailable, resulting in an HTTP return code 404.

Panel 6: Administration Instance Details

In this panel, you must select the **Secure Administration Instance** check box. Due to a known issue in GlassFish Server, this check box must be selected for the Convergence configuration tool to deploy Convergence on the cluster. see [Known Issues](#).

**Note**

You must restart the cluster after deploying Convergence on the cluster, see [Working with Clusters](#).

Set the Session Passivation parameter to true

In a default Convergence deployment, the user sessions are not passivated. That is, the session information does not persist in a store. The `base.passivatesession` configuration parameter that controls session passivation is set to `false` by default. In a clustered environment, this parameter should be set to `true` so that user sessions are maintained.

Type the following command to enable session passivation:

```
iwcaadmin -w password -o base.passivatesession -v true
```



Note

You must restart the cluster if you change the configuration settings using the `iwcaadmin` command.

Client Files

When Convergence is installed, the static files are copied in the GlassFish server `docroot` directory. This directory contains all the JavaScript, HTML, CSS files that display the user interface. In a clustered environment, you must have the `iwc_static` folder on all instances of the cluster. You must configure the load balancer to set the target context root for each cluster instance. The following section shows the portion of the load balancer's configuration file:

```
<web-module context-root="/iwc" disable-timeout-in-minutes="30"
enabled="true"/>
<web-module context-root="/iwc_static" disable-timeout-in-minutes="30"
enabled="true"/>
```

Adding a Convergence Patch in a Cluster Deployment

This section describes how to add a Convergence patch in a cluster deployment. The following steps have to be completed each time you add a new Convergence patch:

1. **Add the Convergence patch only to the DAS system.** Be sure to first backup any customizations stored in the `/opt/SUNWappserver/domains/domain1/docroot/iwc_static/layout/` directory.
2. After the `patchadd` process has completed on the DAS system, copy the Convergence configuration folder from DAS to all other instances in the cluster.
3. In each instance of the cluster, modify `httpbind.conf` to ensure that the IM JIDs are unique.
4. Make sure that the `iwc_static` folder in each instance of the cluster is the latest version.
5. Restart the cluster.

Known Issues

This section describes the known issues, limitations, and suggested workarounds when Convergence is deployed in a clustered environment.

GlassFish Server Fails to Deploy Convergence on the Cluster in a Non-Secure mode

If Convergence is deployed in a cluster in a non-secure mode, the GlassFish Server fails to deploy Convergence. This is a known issue with GlassFish Server.

Workaround: Deploy Convergence in a secure mode. To do this, you must enable the **Secure Administration Server Instance** check box as described in the section [Panel 6: Administration Instance Details](#).

Instant Messaging Component JID

Convergence communicates with the Instant Messaging (IM) Server using the IM HTTP Gateway. The IM HTTP Gateway is a part of Convergence. All instant messaging requests are routed through the gateway. Every Gateway is associated with a unique identifier, known as component JID. The instant messaging client gateway connects to the Instant Messaging server using this component JID. When configuring Convergence on a clustered environment, the Instant Messenger component JID values on the cluster instances should be unique. This is because the Instant Messaging server can only serve one unique component JID request at a time. If your cluster instances connect to the Instant Messaging server using the same component JID, the Instant Messaging server cannot serve requests and the connection to the instant messaging client is lost.

Workaround: When configuring the instances of a cluster, you must provide separate component JIDs for each cluster instance. For more information about how to work with Instant Messaging HTTP Bind Gateways, see [Using the Instant Messaging XMPP/HTTP Gateway](#) in [Oracle Communications Instant Messaging Server Administration Guide](#).

Chapter 20. Setting Up and Managing Convergence Security

Setting Up and Managing Convergence Security

This information provides an overview about security for the Convergence product. It also provides links to security topics that provide more in-depth information for configuring and administering Convergence security.

Topics:

- [Overview of Convergence](#)
- [Secure Installation and Configuration](#)
- [Security Features](#)
- [Security Considerations for Developers](#)

Overview of Convergence

For an overview of the features in Convergence, see [Introduction to Convergence Software](#). To see Convergence's high-level architecture, see [Overview of Convergence](#). For information on general security principals, such as security methods, common security threats, and analyzing your security needs, see [Designing for Security](#). For an overview of operating system security, see [Oracle Solaris Security for System Administrators](#).

Secure Installation and Configuration

This section outlines the planning process for a secure installation and configuration:

- [Installation Overview](#)
- [Installing Infrastructure Components](#)
- [Installing Convergence Components](#)
- [Post Installation Configuration](#)

Installation Overview

This section outlines the planning process for a secure installation and describes recommended deployment topologies for the systems.

Understanding Your Environment

To better understand your security needs, ask yourself the following questions:

1. Which resources am I protecting?
In a Convergence production environment, consider which of the following resources you want to protect and what level of security you must provide:
 - GlassFish Server
 - Convergence Server
 - Protocols: HTTP, WMAP, `mshhttpd`, WCAP, LDAP, and XMPP
 - Dependent Products: Directory Server, Index Search Service, Messaging Server, Calendar Server, and Instant Messaging Server. Be sure to check the security policies governing

these dependent products.

2. From whom am I protecting the resources?

In general, resources must be protected from everyone on the Internet. But should the Convergence 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.

3. What will happen if the 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 to users who use Convergence. Understanding the security ramifications of each resource help you protect it properly.

Deployment Topologies

You can deploy Convergence on a single host or on multiple hosts, splitting up the components into multiple web and index hosts. For more information, see the following information:

- [Convergence Deployment Planning](#)
- [Developing a Communications Suite Logical Architecture](#).

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture. For more information on addressing network infrastructure concerns, see [Determining Your Communications Suite Network Infrastructure Needs](#).

Installing Infrastructure Components

Installing GlassFish Server

Convergence is deployed on GlassFish Server. For information on how to install and configure GlassFish Server, see [Oracle GlassFish Server 3.1.2 Installation Guide](#). To operate GlassFish Server in secure mode, see [Secure Administration Overview](#). For more GlassFish Server security best practices, see: [Oracle GlassFish Server 3.1.2 Security Guide](#).

The GlassFish Server installation prompts for the following authentication and security protocols:

- Administration User and Administration User password
- master password for SSL certificate
- port number for HTTPS port
- secure administration server instance

Note

Be sure that the Secure Administration Server Instance is enabled during GlassFish server installation. If you do not run the GlassFish Server `asadmin` program in secure mode, then you are unable to run the Convergence `init-config` program in secure mode without running into errors. Therefore, install and configure GlassFish Server and Convergence in secure mode.

It is important to minimize the GlassFish installation by not installing components that you are not using and do not intend to use. During GlassFish installation, be sure to enter `no` when asked to install the following components:

- High Availability Database Server
- Load Balancing Plugin
- Sample Applications

Installing Convergence Components

See [Installation Scenario - Convergence 3.0.0.1.0](#).

Assuming you are installing the Messaging Server webmail server component on the same host as Convergence, the Messaging Server installation prompts for credentials of the following:

- system user who will own the configuration files
- system group that will own the configuration files (of which system user is a part)
- Directory Server manager (bind DN and password)
- password for Messaging Server accounts

The Convergence installation and initial configuration prompts for authentication credentials of the following:

- User/Group Directory Server manager (bind DN and password)
- Webmail SSL port number
- Webmail Administration user ID and password
- Access in SSL mode between Messaging Server and Convergence
- Calendar Server SSL port number
- Calendar Administration user ID and password
- Access in SSL mode between Calendar Server and Convergence
- IM Httpbind component JID and password
- IM Avatar component JID and password
- Convergence administrator user name and password

Post Installation Configuration

To configure Convergence to access ISS, see [Convergence Administrative Tasks](#). If you want a secure connection between Convergence and ISS, set the Convergence `ISS.enablessl` parameter to `true`, for example:

```
iwcadmin -o ISS.enablessl -v true
```

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

Security Features

This section outlines the specific security mechanisms offered by Convergence:

- [Managing Security of Passwords](#)
- [Administering Encryption for Secure Authentication](#)
- [Enabling Single Sign-on for Security](#)
- [Instructing End Users on Mail Encryption](#)
- [Detecting Security Attacks or Insecure Use](#)

In addition to encryption-based features and single sign-on, you can best secure your Convergence deployment by ensuring that the components connected to Convergence are securely installed and configured. For more information on general security guidelines for Communication Suite products, see: [Planning a Convergence Security Strategy](#).

Managing Security of Passwords

Beginning in Convergence 3.0.0.0.0, the `-w <password>` option for `iwcadmin`, the Convergence

administration command-line utility, has been removed. Instead, you are prompted for your password after you enter the `iwadmin` command and options.

For batch or automated scripts, you can continue to use the `-w <passwdfile>` flag as long as the `<passwdfile>` is encrypted. To encrypt a password file, use the following `iwadmin` command and option:

```
iwadmin -o admin.adminpwd
```

Administering Encryption for Secure Authentication

For information on encryption-based security, such as SSL, certificate-based authentication, and S/MIME, see:

- [SSL in Convergence](#)
- [Setting up Cert-based Authentication](#)
- [Administering S/MIME](#)

Enabling Single Sign-on for Security

For information on SSO, see:

- [Single Sign-on \(SSO\)](#)

Instructing End Users on Mail Encryption

For end user instructions on security, specifically S/MIME, see:

The following page describes how end users can encrypt their mail as long as S/MIME is enabled. Topics include: logging in for the first time, signature and encryption settings, and enabling the Java console:

[Configuring and Sending Encrypted Mail - Instructions for Convergence End Users](#)

Detecting Security Attacks or Insecure Use

Components, on which Convergence is dependent, are required to be securely installed, configured, administered, and monitored. In the event of a potential attack on the system, refer to the following best practices:

- [Messaging Server Best Practices for Fighting Email Spam](#)
- [How Can I Throttle \(Rate Limit\) Email Delivery?](#)
- [How Can I Prevent Denial of Service \(DoS\) Attacks in Messaging Server?](#)
- [Tools for Managing Security on GlassFish Server](#)
- [Managing Password Security on GlassFish Server](#)

Repeated login failures could be indicative of an external party trying to gain access to an account. For example, you see such activity in LDAP server logs. In OID it is recorded as: 'Bind failure' in the access logs [%home%/OID/logs/access.txt]. For more information, refer to [Directory Server Logging](#).

Security Considerations for Developers

This section lists pages for writing custom modules for authentication and for single sign-on features:

- [Writing a Pluggable SSO Module for Convergence](#)

- [Writing a Custom Authentication Module for Convergence](#)