Oracle® Communications Convergence

System Administrator's Guide

3.0.3
F99828-01
August 2024

Oracle Communications Convergence System Administrator's Guide, 3.0.3

F99828-01

Contents

Preface

Audience ix
Documentation Accessibility ix
Diversity and Inclusion ix

1 Overview of Convergence

About Convergence 1-1
Convergence Deployment Architecture 1-1
- Convergence Client Components 1-3
- Convergence Static Components 1-3
- Convergence Domain Components 1-4

Directory Placeholders Used in This Guide 1-4

2 Using the Convergence Administration Utility

About the Convergence Administration Utility 2-1
Administration Utility Options 2-1
- Command-Line Utility Syntax 2-1
- Managing Security of Passwords 2-3
- Command-line Options 2-3

Setting and Unsetting Configuration Parameters 2-4
Running the Administration Utility in Batch Mode 2-4

3 Convergence Administrative Tasks

Authentication 3-1
- Setting Up Account for End User 3-1
  - Constructing a Filter for Email Address Login 3-1
  - Enabling Email Address Login on Convergence Server 3-2
  - Activating mailAlternateAddress (optional) 3-2
  - Enabling Email Address Login for Back-End Servers 3-2
- Resetting Convergence User Password 3-2
- Configuring Multi-factor Authentication using Oracle Mobile Authenticator 3-4

Configuring Directory Server Authentication in Convergence 3-7
Configuring Convergence for Multiple Directory Servers 3-7
Configuring LDAP Over SSL 3-8
Logging 3-8
Enabling Logging 3-9
About Log Levels 3-9
Setting and Unsetting the Appender Reference for the Components of Convergence 3-10
Specifying the Logging properties for an individual Component 3-10
Specify the Log File Location 3-11
About Log Rotation Policies 3-11
Logging User IP Address and Session Tracking Information 3-12
Sample Convergence Logging Session 3-12
Adding Username to the Log Pattern 3-13
About SSL in Convergence 3-13
Configuring SSL in Convergence 3-13
Configuring Authentication Only SSL in Convergence 3-14
Enabling SSL for Back-End Servers 3-14
Enabling SSL for Messaging Server 3-14
Enabling SSL for Calendar Server 3-14
Enabling SSL for Convergence Address Book 3-14
Enabling SSL for Contacts Server Address Book 3-14
Enabling SSL for the Directory Server 3-14
Redirecting Convergence HTTP Sessions to HTTPS 3-15
Enabling HTTP Strict Transport Security 3-15
Configuring the Convergence Display Name 3-15
Configuring the Corporate Address Book to Perform displayName Search 3-16
Configuring Convergence to Hide Global Time Zone Selection from Options 3-16
Configuring Convergence to Prevent Host Header Attack 3-16
Preventing Host Header Attack in a Single Domain 3-16
Preventing Host Header Attack in Multiple Domains 3-17
About Single Sign-On 3-17
Configuring Convergence for SSO with Oracle Access Manager 3-17
Setting Up Oracle Access Manager 3-17
Enabling SSO with Oracle Access Manager 3-19
Sample Custom Logout Redirect Script 3-20
Configuring Convergence for Trusted Circle SSO 3-21
Writing a Custom SSO Module 3-22
Directory Server Services for Convergence 3-22
Configuring Directory Server Failover 3-22
Configuration Management 3-22
Configuring Convergence to use SSL for Configuration Management 3-22
Changing Convergence Administrator Password 3-23

Deployment-Specific Customizable Client Options for Convergence 3-23
Customizing the Login URL and Page for a Specific Domain 3-23
Configuring Another Page for Changing Password 3-23
User's Password is About to Expire 3-24
User's Password is Expired 3-24
User's Password is Reset by Administrator 3-24
Configuring Another Page for Changing Password for users of a specific domain 3-24
User's Password is About to Expire 3-25
User's Password is Expired 3-25
User's Password is Reset by Administrator 3-26
Setting the Auto Logout Time 3-27
Verifying passwords in Convergence 3-27
Creating a Directory Server User to Manage Convergence 3-28
Configuring VLV Browsing Indexes for Directory Server 3-29
Applying the VLV Browsing Index Settings 3-29
Generate the Indexes 3-30
Handling Invalid Session Redirects in Convergence 3-31

4 Enabling Core Services for Convergence

Enabling Services for the Entire Convergence Installation 4-1
Enabling Services for an Individual User or Domain 4-2
Managing Service Access Through the Directory Server 4-2
Enabling and Disabling Services with Directory Server Provisioning 4-2
Directory Server Attributes for Mail Service 4-2
Directory Server Attributes for Calendar Service 4-3

5 Mail Service Administration

Managing Attachment Previewing 5-1
About Outside In Transformation Server and the Outside In Proxy 5-1
Configuring File Directory Access 5-3
Managing Attachment Life Cycles 5-4
Supporting Extended Character Locales 5-4
Customizing Transformation Blacklist 5-4
About HTML Filtering 5-4
Enabling and Disabling HTML Filtering 5-5
Configuring HTML Filtering in Convergence 5-6
Restricting Attachment Types for End-Users 5-9
Restricting Number of Emails that can be sent to Recipients in a Defined Time Period 5-9
Enabling Anti-Spam 5-10
Configuring Convergence to Combat Spam 5-10

Configuring Messaging Server to Combat Spam 5-10
Disabling Rich Text Formatting 5-11
Enabling Sound Alerts 5-11

6 Address Book Service Administration

Configuring Horizontal Scalability for the Personal Address Book 6-1
Horizontal Scalability Architecture 6-1
Setting the psRoot Value Automatically 6-2
Configuring Address Book to Use Different Directory Server from the User Group Server 6-3
Configuring the Corporate Directory 6-3
Enabling Address Autocomplete for the Corporate Directory 6-4
Setting Up Domain-Based Configuration for Address Book 6-4
Disabling the Corporate Directory in Specific Domains 6-6
Changing the Default Corporate Directory Search Filter in Address Book 6-6
Configuring Virtual List View for Convergence Corporate Directory 6-6
About Supported vCard Standards 6-7
Changing the Locale Character Set for Importing or Exporting vCard Entries 6-7
Enabling Contact Export and Import with Photo in vCard 6-9
Hiding Administrator Accounts in the Default Domain Corporate Directory 6-9
About Personal Address Book Contacts Deleted by the End User 6-9
Enhancing Corporate Directory Search Using VLV Indexing 6-9
Creating the VLV Index in the Directory Server 6-10
Generating Indexes 6-10
Configuring Convergence 6-12
Verifying the VLV Settings 6-13

7 Calendar Service Administration

Enabling CalDAV Service 7-1
Enabling SMS Calendar Notifications in Convergence 7-2
Hiding or Showing the SMS Option in the Notifications Tab in Calendar Options and in the Reminder Dialog Box 7-2
Reserving Calendar Resources 7-3
Creating a Calendar Resource in Corporate Directory 7-3
Viewing Event Invitation and Task Details in Anonymous Calendar in Convergence 7-4

8 Contacts Server Administration

Enabling Contacts Server Service 8-1

9 Configuring Convergence to Use Proxy Authentication

Configuring Convergence for Proxy Authentication 9-1
Proxy Authentication Request 9-2

10 Convergence Properties Reference

Global Convergence Configuration Properties 10-1

11 Monitoring Convergence

Overview of Monitoring Convergence 11-1
Enabling Convergence Monitoring 11-1
Configuring Convergence for JMX Monitoring 11-2
Using Jconsole for Convergence Monitoring 11-2
About Convergence JMX Metrics 11-3
Using the iwcmetrics Command for Convergence Monitoring 11-4
About Convergence Non-JMX Metrics 11-5

12 Troubleshooting Convergence

Configuring Log Levels to Gather Information 12-1

13 Setting Up Multiple Corporate Directories

Adding a Corporate Directory 13-1
Configuring Multiple Corporate Directories 13-1
Disabling Corporate Directory (Newly Added or Default) 13-2

14 Overview of Add-on Services in Convergence

About the Add-on Framework 14-1
About the Add-On Configuration Files 14-1
add-ons.properties 14-1
addon_name.json 14-2
addon_name.properties 14-2
Configuring Convergence for SMS 14-3
Configuring One-Way SMS for Convergence 14-3
Configuring Messaging Server for One-Way SMS 14-3
Configuring the SMS Add-on Service in the Convergence UI 14-3
Configuring the Advertising Add-On Service in Convergence 14-3
About the Advertising Add-On Service 14-3
Configuring Advertising for Convergence 14-4

Enabling the Advertising Add-On Service 14-4
Displaying Ads in a Skyscraper Panel 14-5
Parameters for Configuring Skyscraper Panels in the advertising.json File 14-5
Displaying Ads in an Ad Box 14-6

15 Tuning Oracle WebLogic Server to Enhance Convergence Performance

Convergence Performance Tuning Overview 15-1
Tuning Oracle WebLogic Server Configuration Parameters 15-1
Configuring Oracle WebLogic Server to Compress Client Files 15-1
Enhancing Browser Caching of Static Files for Oracle WebLogic Server 15-2
Tuning the JVM Heap Size 15-2
Setting Garbage Collection Algorithms 15-2
Miscellaneous Performance Tuning Tips 15-3

A ExpiresFilter.java Reference

B Glossary

Preface

This guide explains how to administer Oracle Communications Convergence and its accompanying software components.

Audience

This document is intended for Convergence system administrators. This guide assumes that you have a working knowledge of the following concepts:

- Oracle WebLogic Server administration
- Directory server management
- Structure and use of a lightweight directory access protocol (LDAP) directory
- Secure Sockets Layer (SSL) for a secured communications
- System administration and networking
- General deployment architecture

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Overview of Convergence

This chapter provides an overview of Oracle Communications Convergence.

About Convergence

Convergence is an interactive web-based communication client that delivers messaging, calendar, and address book services.

Convergence delivers its services using the capabilities common within the most popular types of web browsers, including Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome.

Convergence is also highly customizable, making it as much a development platform as a client.

The Convergence messaging service provides:

- Compose, reply, forward, and other typical email functions
- Spell check
- Message and attachment search (subject, sender, and so on)
- Mail management: deleting, moving, marking messages
- Quota

The Convergence calendar service provides:

- Create, edit, delete events and tasks, and other typical calendar functions
- Check availability, schedule meetings with others
- Sharing calendars

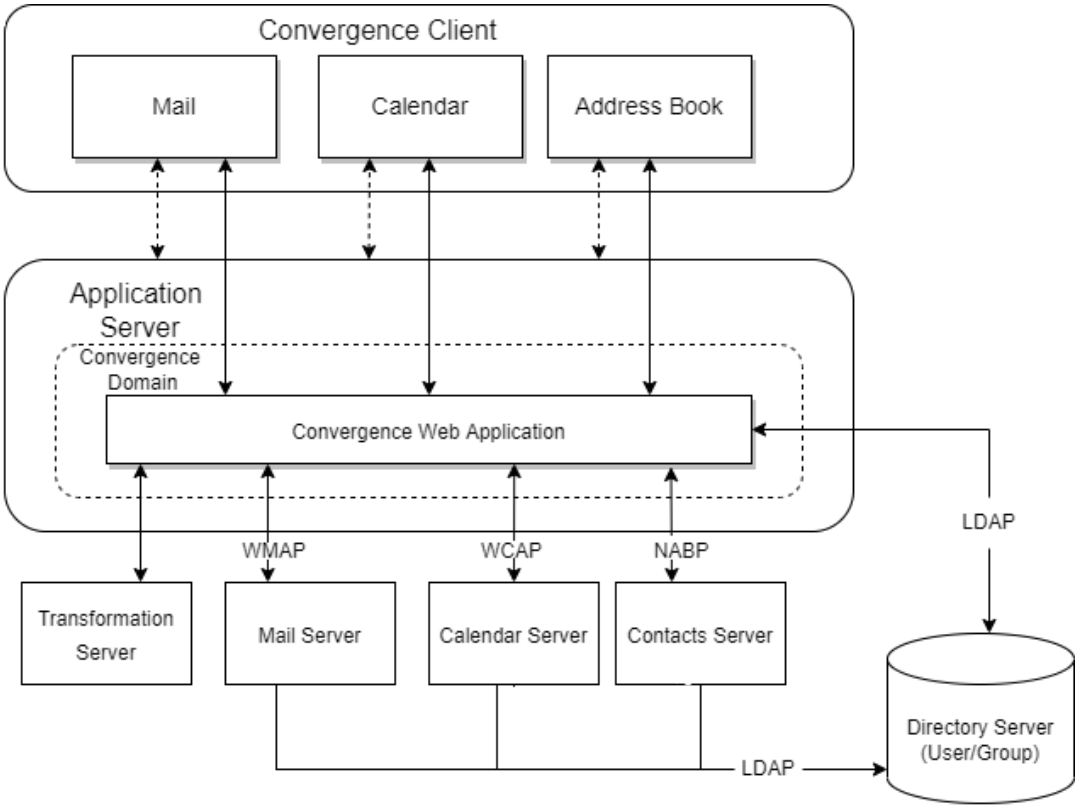
The Convergence address book service provides:

- Common address book across services
- Create contacts and groups of contacts
- Corporate address book
- Import or export contact information
- Send email or schedule events directly from the address book

Convergence Deployment Architecture

Figure 1-1 shows the Convergence components. The top layer shows the various Convergence services. The middle layer represents the Convergence server itself, deployed to the Oracle WebLogic server domain. The bottom layer shows the dependencies that the Convergence server has on other applications to deliver its services and features.

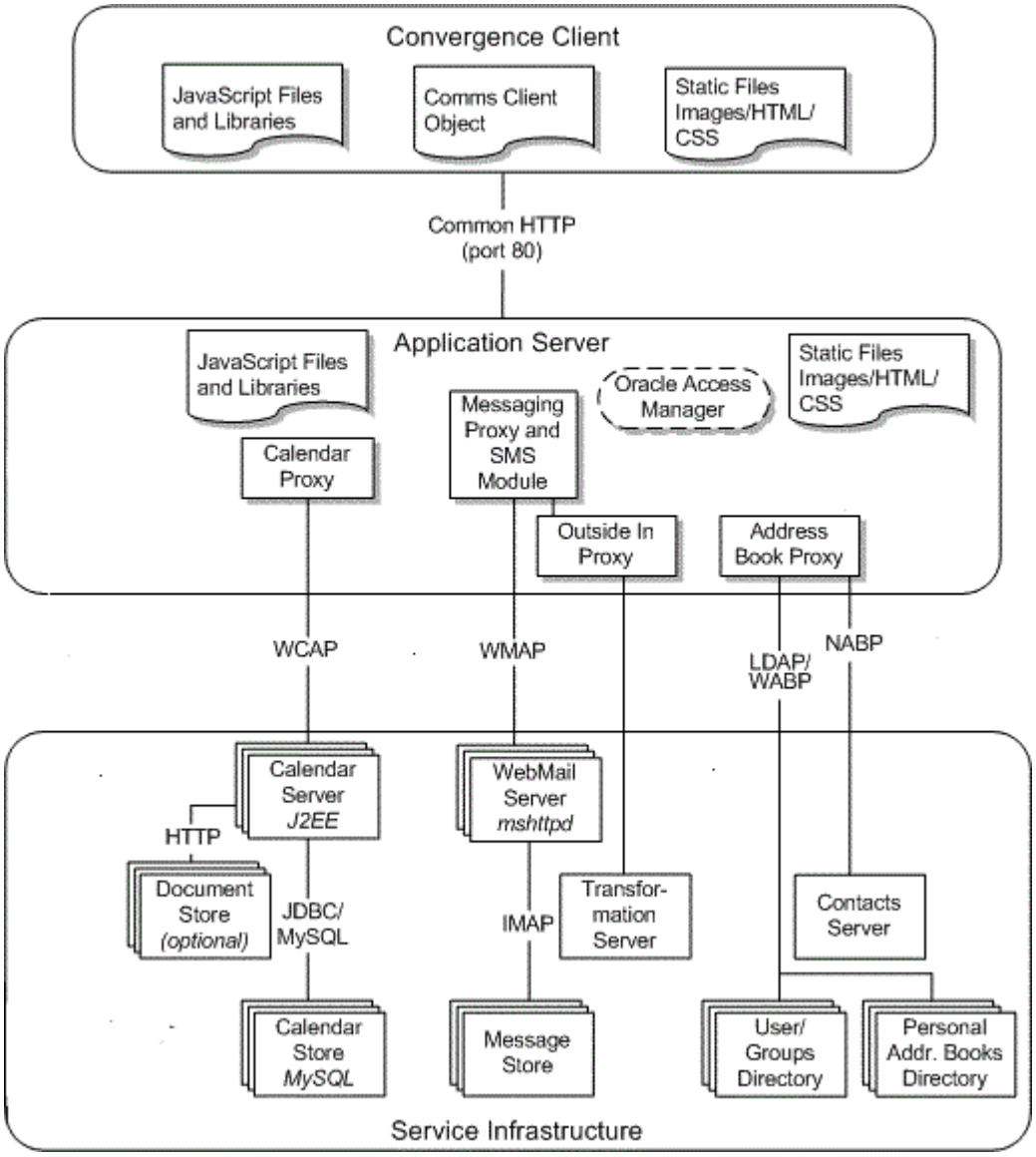
Figure 1-1 Convergence Components



Convergence consists of several service proxies. The service proxies communicate with their appropriate server using various protocols.

Figure 1-2 shows the logical architecture that depicts the logical building blocks of the components and the infrastructure services needed to support them. The logical architecture does not specify the hardware required to implement a deployment. However, it helps you visualize the interrelationship among components, provides a basis for analyzing use cases, and is the starting point for the deployment design.

Figure 1-2 Convergence High-Level Logical Architecture



You can add Convergence to an existing deployment or plan a new deployment that includes Convergence.

Convergence Client Components

The Convergence client runs in a browser. The client uses Dojo to provide the basic infrastructure for the client components. 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 client extension and customization.

Convergence Static Components

Convergence uses static content files such as HTML, CSS, and JavaScript. These static files are deployed to the application server **docroot** directory.

Convergence Domain Components

The Convergence server components are deployed to an application server domain. The server components reside in the application and interact with servers to deliver Convergence services (such as email, calendar, and address book services). The server provides the services that use the client to render data on the browser. The client API communicates with the services to fetch this data.

Convergence server components communicate with other servers and components to provide the following:

- Authentication and authorization
- Session management and Single Sign-On (SSO) access control
- Protocol service
- Configuration management (XML configuration files and command line interface)
- Proxy services for mail, calendar, and address book services from other communications servers
- Centralized and secure request management
- Logging and basic monitoring of activities

Directory Placeholders Used in This Guide

Table 1-1 lists the directory placeholders used in this guide:

Table 1-1 Convergence Directory Placeholders

Placeholder	Description
WLS_Home	The directory in which Oracle WebLogic Server software is installed. For example: **WLS_HOME**.
Convergence_Domain	The application server directory containing the configuration files for the domain in which Convergence is deployed. *Convergence_Domain* is created in *WLS_HOME*/*Oracle_Home*/ *user_projects*/**domains**. *Convergence_Domain* for Oracle WebLogic Server Deployment is: • *WLS_HOME*/*Oracle_Home*/*user_projects*/**domains/base_domain**
Convergence_Home	Specifies the installation location for the Convergence software. The default is **/opt/sun/comms/iwc**.
Data directory	The data directory is: /**var**/**opt**/**sun**/**comms**/**iwc**.
c11n_Home	The directory in which all Convergence customization files and directories are created for WebLogic Server. The *c11n_Home* directory for Oracle WebLogic Server is: • *data_directory*/**web-src/client/iwc_static/c11n**

2

Using the Convergence Administration Utility

This chapter provides an overview of how to use the Oracle Communications Convergence administration command-line utility to administer Oracle Communications Convergence.

About the Convergence Administration Utility

You can use the Convergence **iwcadmin** command-line utility to perform administrative tasks in Convergence. The following are some of the reasons you would want to use the command-line utility:

- 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 suit 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.

Administration Utility Options

The **iwcadmin** command 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 **iwcadmin** command exists in the *Convergence_Home***/sbin** directory.

You can use the **iwcadmin** command only on the local machine on which Convergence is installed.

You must restart the Oracle WebLogic server if you make any configuration changes using the **iwcadmin** command.

Command-Line Utility Syntax

Use the **iwcadmin** command to display its usage and syntax:

```
iwcadmin -h
```

The following example shows the usage and syntax of the **iwcadmin** command:

```
USAGE: iwcadmin [-p port] [-s] [-o param_name [-v param_value]] [-l
[group_name]] [-f config_params_file] [-V]
    -u    --admin           userID of user authorized to make iwcadmin
updates. Optional parameter. If -u is not specified, userID (default: admin)
                            is pulled from the iwcadmin.properties file.
```

```
    -p    --port            Administration port of the server.
    -s    --secure          Use a secure connection (HTTPS).
    -o    --option          The configuration parameter name to read or write.
    -v    --value           The value to be set. Must be used with the -o
option and must be specified immediately after the -o option.
    -l    --list            List all the configuration parameters and their
values.
    -f    --file            The file from which to read configuration
property/value pairs.
    -V    --version         Display the version information of the product.
    -h    --help            Display this message.
```

- To read the value of a property:

  ```
  iwcadmin [-p port] [-s] -o option_name
  ```

- To write the value of a property:

  ```
  iwcadmin [-p port] [-s] -o option_name -v option_value
  ```

- To update multiple properties:

  ```
  iwcadmin [-p port] [-s] -f path/filename
  ```

- To read the value of all configuration properties:

  ```
  iwcadmin [-p port] [-s] -l
  ```

- To get information about configuration properties:

  ```
  iwcadmin [-p port] [-s] -o config_parameter_name -h
  ```

- To get information about configuration properties for a specific module:

  ```
  iwcadmin [-p port] [-s] -l group_name
  ```

  This option is useful when you want to see the values of the configuration parameters for a specific group

  For 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
  ```

  Where *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.

For example:

```
iwcadmin -l -h lists all the configuration parameters and their values. It optionally
takes the group name as an argument and lists the parameters that belong to the given
group.
Available groups: base, ugldap, auth, mail, log, cal, caldav, nab,  ab, client, admin,
sso, user, ens, notify, oin.
```

- To get the current version of the software:

```
iwcadmin -V
```

> **Note:**
>
> If you use **tcsh** and enter an **iwcadmin** parameter enclosed in curly braces {}, you must escape the braces by preceding each brace with a backslash (\).
>
> For example:
>
> ```
> \{ ... \}
> ```

Managing Security of Passwords

When using the **iwcadmin** command, you cannot include the `-W password_file` parameter unless the password file is encrypted. For this reason, the `-W` parameter is omitted from all examples in this guide.

Use the following command to retrieve an encrypt password:

```
iwcadmin -o admin.adminpwd
```

If you exclude the `-W password_file` parameter from your commands, the command-line utility asks you to provide your password.

Command-line Options

Table 2-1 lists all the command-line syntax options.

Table 2-1 Options for Configuration Utility for Convergence

Option	Long name	Description
-p	--port	Administration port on which the server listens.
-s	--secure	Optional. Ensures a secure connection.
-o	--option	Configuration property name to read or write. If you do not specify the `-v` option, the utility performs a read operation. If this option is specified in the same command with the `-f` option, the `-f` option is ignored. The `-o` option takes precedence.
-v	--value	Value to be set. Use with the `-o` option and must be specified immediately after the `-o` option.
-f	--file	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 **=**), and a line return between options.
-V	--version	Version information of the product.
-l	--list	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.
-h	--help	Help to use this utility.

You can 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] [-s] -o config_params_name -h
```

The `-h` 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 Administration Utility in Batch Mode

To update multiple attributes or configuration parameters in your deployment, invoke the **iwcadmin** command in batch mode. The **-f** parameter 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.

   ```
   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
```

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 **iwcadmin** command with the **-f** option and provide the path to the file:

```
iwcadmin -f /tmp/logLevelSetting
```

3
Convergence Administrative Tasks

This chapter describes several administrative tasks for Oracle Communications Convergence.

Authentication

This section describes administrative tasks related to authentication.

See *Convergence Security Guide* for more information on certificate-based authentication.

Setting Up Account for End User

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

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

The procedures for setting up email address login which uses the directory server **mail** attribute are the following:

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

Constructing a Filter for Email Address Login

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

The **mail** attribute identifies the primary email address for a user, calendar group, or calendar resource. This is the email address retrieved and displayed by lookup applications.

Table 3-1 lists the variables used in constructing the filter.

Table 3-1 Mail Attribute Filter Variables

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 directory server attributes, specifically **inetDomainSearchFilter**, see the discussion about directory server object classes and attributes in your Oracle Communications Messaging Server and Oracle Communications Calendar Server documentation.

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 Properties 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))"
```

Enabling Email Address Login for Back-End Servers

You can use the **iwcadmin** command to set up email address login into back-end servers.

Enabling Email Address Login for Messaging Server

To set up email address login for mail server, set the **mail.uidreplayformat** parameter.

```
iwcadmin -o mail.uidreplayformat -v "%o"
```

Enabling Email Address Login for Calendar Server

To set up email address login for calendar server, set the **caldav.uidreplayformat** parameter.

```
iwcadmin -o caldav.uidreplayformat -v "%o"
```

Enabling Email Address Login for Contacts Server Address Book

To set up email address login for contacts server address book, set the **nab.uidreplayformat** parameter.

```
iwcadmin -o nab.uidreplayformat -v "%o"
```

Resetting Convergence User Password

Users can reset their password using the **Forgot Password** feature. By default, this feature is disabled.

To allow users to reset their password, enable **Forgot Password** by using the **iwcadmin** command:

```
./iwcadmin -o base.enableforgotpassword -v true
```

When this option is enabled, users can reset their password by clicking the **Forgot Password** link provided in the Convergence login page.

The password reset is protected by two factor authentication. Users must provide either their email address or phone number. After the email address is verified, users will be allowed to select two factor authentication. A One-Time Password (OTP) will be sent to their registered mobile number or the configured secondary email address, depending on the option selected. On verification of the OTP, users can change the password.

To enable two factor authentication by SMS, use the **iwcadmin** command:

```
./iwcadmin -o base.sms.enable -v true
```

To enable two factor authentication by a secondary email address, use the`iwcadmin` command:

```
./iwcadmin -o base.mail.enable -v true
```

The password reset session is valid for 4 minutes. The administrator can change the password reset session timeout using the following command:

```
./iwcadmin -o base.sessiontimeout -v <value>
```

The one-time password is valid for 3 minutes by default. The administrator can change the duration of OTP validity using the below command:

```
./iwcadmin -o base.sms.timeout -v <value> for SMS
./iwcadmin -o base.mail.timeout -v <value> for Email
```

This feature also supports the following new options:

- base.enableforgotpassword
- base.sessiontimeout
- base.sms.enable
- base.sms.channel
- base.sms.defaultLDAPAttribute
- base.sms.timeout
- base.mail.enable
- base.mail.timeout.

For more information about these options, see **iwcadmin** help or Table 10-1.

> **Note:**
>
> To send OTP via SMS, Convergence requires the Messaging Server as it implements an SMPP client (the MTA SMS channel) that communicates with the remote Short Message Service Center (SMSC).
>
> For more information, see One-Way SMS in *Messaging Server System Administrator's Guide* to setup One-way SMS.
>
> To send the OTP to a secondary email address, enable the secondary email address feature in Convergence by using the command below. This allows users to add a secondary email address using Preferences in Convergence. You can do this with the following command:
>
> ```
> ./iwcadmin -o client.enablesecondaryemail -v true
> ```

The same channel name needs to be configured in Convergence for the `base.sms.channel` parameter.

By default, users' mobile numbers are stored in the **mobile** ldap attribute to be used to send OTP via SMS. However, the administrator can change the default mobile number ldap attribute to the one used to store the mobile number with the following command:

```
./iwcadmin -o base.sms.defaultLDAPAttribute -v <mobile>
```

To configure the SMS channel, use the following command:

```
./iwcadmin -o base.sms.channel -v sms
```

The OTP message's default subject and body will be in English. To send a message in a different language, customize the **application.properties** file under **config** folder. Ensure the message does not exceed 160 characters for SMS mode of two-factor authentication. For locales with non-ASCII characters, limit to 20 to 30 characters as each character may take 2 to 3 bytes of storage.

Configuring Multi-factor Authentication using Oracle Mobile Authenticator

Multi-factor authentication (MFA), also known as two-factor authentication (2FA) is a security process that requires users to provide two or more separate forms of identification before granting access to the application. It aims to enhance security by adding an additional layer of authentication beyond the user name and password.

The multi-factor authentication feature is available in Convergence from 3.0.3.4.0. By default, this feature is disabled. When this feature is enabled, the user enters their user name, password and then the OTP generated by Mobile Authenticator to log in to Convergence.

> **Note:**
>
> This feature should not be enabled when SSO is enabled in Convergence.

Prerequisites:

- Directory Server Setup 6.4.0.29.0 or above, as this feature requires LDAP **objectClass iwcAddonService** and LDAP attributes **iwcAddonAllowedServices, iwcAddonCredentials** in LDAP schema definition.
- Download the Mobile Authenticator application from an application store.

By default MFA is disabled in Convergence deployment. The following are the configuration steps for OMA:

Configuring MFA at deployment level:

- Ensure the following are set to true:

  ```
  ./iwcadmin -o base.enablemultifactauth -v true
  ./iwcadmin -o base.oma -v true
  ```

- Restart the Application Server.

Configuring MFA at LDAP domain level:

> **Note:**
>
> The administrator should manually provision **ldapAttribute** and **ObjectClass** to enable MFA for a domain:
>
> | LDAP Attribute | LDAP ObjectClass |
> |---|---|
> | iwcAddonAllowedServices | iwcAddonService |

To Enable MFA at domain level:

- Add **objectClass iwcAddonService** to the domain entry.
- Add **iwcAddonAllowedServices** attribute to the domain entry.
- Set **iwcAddonAllowedServices** attribute with value `mfa=true` in the domain entry.

For example, Schema 2:

To add ObjectClass:

```
dn:o=example.com,o=isp
changetype: modify
add: objectclass
objectclass:iwcAddonService
```

To Add Attribute:

```
dn:o=example.com,o=isp
changetype: modify
add: iwcAddonAllowedServices
iwcAddonAllowedServices:mfa=active
```

Schema 1:

To add ObjectClass:

```
dn: dc=example,dc=com, o=internet
changetype: modify
add: objectclass
objectclass:iwcAddonService
```

To Add Attribute:

```
dn: dc=example,dc=com, o=internet
changetype: modify
```

```
add: iwcAddonAllowedServices
iwcAddonAllowedServices: mfa=active
```

```
ldapmodify -D "cn=Directory Manager" -w pwd -h host -p port -f
<ldif_content>.ldif
```

- Restart Application Server.

To disable MFA at domain level:

- Set `mfa=inactive` in **iwcAddonAllowedServices** ldapAttribute.
- Restart Application Server.

Configuring MFA at User level in LDAP:

- Setting **iwcAddonAllowedServices** ldapAttribute as `mfa=active` at domain level will enable MFA for all users in that domain.
- At user level mfa can be set to active/inactive by setting `iwcAddonAllowedServices:mfa=active/inactive`.

When MFA is enabled,

- iwcAddonService ObjectClass is added when user logs in to Convergence
- ldapAttribute iwcAddonCredentials is added when user registers for OMA.

LDAP Attribute	LDAP ObjectClass
iwcAddonCredentials	iwcAddonService
iwcAddonAllowedServices	iwcAddonService

When MFA is enabled for a domain, all users in that domain can login to Convergence only after verification of OTP generated by the Mobile Authenticator.

When a user from a MFA enabled domain logs into Convergence for the first time, the user has to register using the "Register for Mobile Authenticator" link after log in. The user can register in Mobile Authenticator by scanning the QR code or by manually adding the key.

Mobile Authenticator app can be downloaded from an application store. This feature is verified with Oracle Mobile Authenticator app.

Once MFA registration is successfully done, the user can log in to Convergence only after verification of OTP generated by the Mobile Authenticator. The multi-factor authentication session will be valid for 4 minutes and the OTP will be valid for 30 seconds by default.

In case of any issue with OMA, contact your system administrator to reset the old key before re-registering for OMA. Then the user needs to re-register again in Convergence using "Register for Mobile Authenticator" link.

Resetting the old key in case of OMA issues

- Search for **iwcAddonCredentials** attribute for the user.
- Delete this attribute which has `mfa={"key":"SampleKey"}`:

```
 ldapsearch -D "cn=Directory Manager" -w pwd -h hostname -p port -b
"uid=testuser,ou=People,o=example.com,o=isp" iwcAddonCredentials
```

- Take note of the **dn** and the **iwcAddonCredentials**" attribute which has "mfa={key:"....."}". For example, `mfa={"key":"ZYQV3%%%LLY3G###JAYISNZKZQS5Z"}`.

```
ldapmodify -D "cn=Directory Manager" -w password -h localhost -p 1389 -f
modify.ldif
```

- Add the below lines in the **modify.ldif** , change the **dn** as required:

```
dn: uid=testuser,ou=People,o=example.com,o=isp
changetype: modify
delete: iwcAddonCredentials
iwcAddonCredentials: mfa={"key":"SampleKey"}
```

- Replace the SampleKey with actual key which was listed in the **ldapsearch**.

> **Note:**
>
> Any change in **base.oma.timeout** and **base.oma.issuer** needs all the registered users to re-register by scanning the QR code in Mobile authenticator to make sure the correct OTP and issuer information is used for verification.

For more information on MFA related configuration parameters to change OMA issuer and OMA time out, see Table 10-1.

Configuring Directory Server Authentication in Convergence

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

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

Configuring Convergence for Multiple Directory Servers

You can configure Convergence to use a separate directory server for user authentication and another for user/group information.

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

To enable your site to use a separate directory 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 UG LDAP and directory server authentication must be the same.
- **auth.ldap.dcroot** - DC (Domain Component) or user tree root node in the directory server. This should be the same value as in the UG LDAP.

- **auth.ldap.host** - Host name of the authentication directory server.
- **auth.ldap.enablessl** - Set this parameter to **true** or **false** to enable or disable SSL.
- **auth.ldap.port** - Port number on which the directory server listens. If the directory 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 directory server pool is initialized.
- **auth.ldap.maxpool** - Maximum number of connections that you want to have when the directory server pool is initialized.
- **auth.ldap.timeout** - Set this to the maximum number seconds that the directory server should wait for returning search results before ending a search.
- **auth.ldap.binddn** - The Bind DN of the user. The directory 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 Administration Utility in Batch Mode".

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

```
iwcadmin -o auth.ldap.ugfilter -v user_group_filter
```

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.

Configuring LDAP Over SSL

If you use the same directory server, both for authentication and storing user preferences, you must set the **ugldap.enablessl** and **ugldap.port** configuration parameters by using the **iwcadmin** command.

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

If your deployment uses a directory server other than the User/Group LDAP for authentication, you must set the following parameters by using the **iwcadmin** command:

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

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.

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

- Address Book (ADDRESS_BOOK)
- Administration (ADMIN)
- Authentication (AUTH)
- Configuration (CONFIG)

- Default (DEFAULT)
- Event Notification System (ENS)
- Notify (NOTIFY)
- Protocol (PROTOCOL)
- Calendar Proxy (PROXY_CAL)
- Mail Proxy (PROXY_MAIL)
- Network Address Book Proxy (PROXY_NAB)
- Outside In Proxy (PROXY_OIN)
- SIEVE filters (SIEVE)

For each component, you can set a log level. The existing log levels are described in "About Log Levels". 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 = DEBUG
log.ADMIN.level = DEBUG
log.AUTH.level = DEBUG
log.CONFIG.level = DEBUG
log.DEFAULT.level = DEBUG
log.ENS.level = DEBUG
log.NOTIFY.level = DEBUG
log.PROTOCOL.level = DEBUG
log.PROXY_CAL.level = DEBUG
log.PROXY_MAIL.level = DEBUG
log.PROXY_NAB.level = DEBUG
log.PROXY_OIN.level = DEBUG
log.SIEVE.level = DEBUG
```

Enabling 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 **iwcadmin** command.

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

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

About 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

Setting and Unsetting the Appender Reference for the Components of Convergence

You can set or unset the appender reference for the components of Convergence. Appender reference is used so that the logging properties can be set for an individual component. If the component does not require the logging properties at component level, you can unset the appender reference by setting its value to a blank.

To set the appender reference for the component, type the following command:

```
iwcadmin -o log.component_name.appendername -v appender_name
```

where *component_name* is the name of component of Convergence.

where *appender_name* is the name of the appender.

For example, the following command sets the appender reference ADDRESS_BOOK_APPENDER for the ADDRESS_BOOK.

```
iwcadmin -o log.ADDRESS_BOOK.appendername -v ADDRESS_BOOK_APPENDER
```

For example, the following command sets the appender reference GENERIC for the PROXY_CAL.

```
iwcadmin -o log.PROXY_CAL.appendername -v GENERIC
```

To unset the appender reference for the component, type the following command:

```
iwcadmin -o log.component_name.appendername -v
```

where component_name is the name of component of Convergence.

For example, the following command unsets the appender reference for the ADDRESS_BOOK.

```
iwcadmin -o log.ADDRESS_BOOK.appendername -v
```

> **Note:**
>
> You can also set the same appender reference for more than one component of the Convergence.
>
> For example, the following command sets the appender reference GENERIC for the PROXY_CAL, PROXY_MAIL, and SIEVE components.
>
> ```
> iwcadmin -o log.PROXY_CAL.appendername -v GENERIC
> iwcadmin -o log.PROXY_MAIL.appendername -v GENERIC
> iwcadmin -o log.SIEVE.appendername -v GENERIC
> ```

Specifying the Logging properties for an individual Component

You can specify the following logging properties for an individual component after the appender reference is set for the component:

- log.appender.*appender_name*.type

- log.appender.*appender_name*.location
- log.appender.*appender_name*.sizetriggerval
- log.appender.*appender_name*.maxbackupindex
- log.appender.*appender_name*.pattern

  where appender_name is the name of appender.

This example shows how to set the logging properties for the ADDRESS_BOOK after the appender reference ADDRESS_BOOK_APPENDER is set for the component:

```
iwcadmin -o log.appender.[ADDRESS_BOOK_APPENDER].type -v FILE
iwcadmin -o log.appender.[ADDRESS_BOOK_APPENDER].location -v /opt/sun/comms/iwc/logs/
ADDRESS_BOOK_LOGS.log
iwcadmin -o log.appender.[ADDRESS_BOOK_APPENDER].sizetriggerval -v 2048
iwcadmin -o log.appender.[ADDRESS_BOOK_APPENDER].maxbackupindex -v 5
iwcadmin -o log.appender.[ADDRESS_BOOK_APPENDER].pattern -v '%c: %p from %C  Thread %t
at %d%m %n'
```

> **Note:**
>
> When an appender reference is not associated with the component, all logs for that component will default to global logging properties (specified by log.location, log.adminloglocation, log.pattern etc).

For more information about the logging properties, see Table 10-5.

Specify the 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 **iwcadmin** command are sent to the administration log location.

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

```
iwcadmin -o log.location -v /data/logs/file.log
```

where *file* is the name you choose for the log file.

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

```
iwcadmin -o log.adminloglocation -v /data/logs/file.log
```

About Log Rotation Policies

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 -o log.sizetriggerval -v 102400
```

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

```
iwcadmin -o log.timetriggerval -v "'.'yyyy-MM"
```

For more information about frequency patterns for time based log rotation, see the apache web site:

http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/DailyRollingFileAppender.html

Logging User IP Address and Session Tracking Information

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 -o log.pattern -v '%c: %p from %C  Thread %t ipaddress=%X{ipaddress}
sessionid=%X{sessionid} at %d - %m %n'
iwcadmin -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 Oracle WebLogic Server hosting Convergence resides behind a front-end reverse proxy or a load balancer (web server), the IP address of the front-end is captured, not the IP address of the browser. To overcome this situation, ensure that the **WebLogic Plugin Enabled** option is selected in the **Web Applications** tab for the domain name where Convergence is deployed (*DomainName* > **Configuration > Web Applications**).
>
> If you use a reverse proxy in front of Convergence, you should configure that reverse proxy to put the original client IP address into an HTTP Header that must be called **proxy-ip**.
>
> If you have selected the **WebLogic Plugin Enabled** option, 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 cannot log into Convergence.
>
> See the Oracle WebLogic Server documentation for more information.

Sample Convergence Logging Session

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 Oracle WebLogic server is shutdown. All sessions are then invalidated.

Adding Username to the Log Pattern

To include the username in the log pattern, modify the log pattern to incorporate the username attribute. This ensures the username is captured in every log entry.

Use the following commands to include the username in the log pattern:

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

After adding the above commands, restart the Oracle WebLogic Managed Server.

About SSL in Convergence

This section explains how to configure Convergence with SSL.

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

Configuring 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 Oracle WebLogic server level and also set the **base.sslport** configuration parameters using the **iwcadmin** command.

For **base.sslport** properties, refer to "Convergence Properties Reference ".

```
iwcadmin -o base.sslport -v ssl_port
```

Configuring Authentication Only SSL in Convergence

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 Oracle WebLogic server SSL port value, and the **base.enableauthonlyssl** value using the **iwcadmin** command. For example:

```
iwcadmin -o base.sslport -v ssl_port
iwcadmin -o base.enableauthonlyssl -v true
```

Enabling SSL for Back-End Servers

Use the **iwcadmin** command to enable SSL between Convergence and back-end servers.

Enabling SSL for Messaging 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
```

Where *mail_port* is the SSL port open on the Messaging server.

Enabling SSL for Calendar Server

To enable SSL for Calendar Server 7 and Calendar Server 8, set the **caldav.enablessl** and **caldav.port** configuration properties.

```
iwcadmin -o caldav.enablessl -v true
iwcadmin -o caldav.port -v caldav_port
```

Where *caldav_port* is the SSL port open on the Calendar Server.

Enabling SSL for Convergence Address Book

The address book service provided by Convergence is a part of Convergence. To enable SSL for the address book service, enable SSL for Convergence.

Enabling SSL for Contacts Server Address Book

To enable SSL for Contacts Server, set the **nab.enablessl** and **nab.port** configuration properties.

```
iwcadmin -o nab.enablessl -v true
iwcadmin -o nab.port -v nab_port
```

Where *nab_port* is the SSL port open on the Contacts Server.

Enabling SSL for the Directory Server

To enable SSL between Convergence and the directory server, set the **ugldap.enablessl** and **ugldap.port** configuration properties.

```
iwcadmin -o ugldap.enablessl -v true
iwcadmin -o ugldap.port -v ldap_port
```

Where *ldap_port* is the SSL port open on the directory server.

Redirecting Convergence HTTP Sessions to HTTPS

Oracle recommends setting up automatic HTTPS redirection on the Convergence web container. See the container documentation for the preferred approach for setting up HTTPS redirection.

Enabling HTTP Strict Transport Security

You can enable HTTP strict transport security (HSTS) to protect the Convergence server from dynamic content accessed in Convergence (for example, in an email). HSTS requires at least one successful HTTPS request, otherwise the HSTS header is ignored.

By default, HSTS is not enforced.

Use the **iwcadmin** command to set **base.hstsmaxage**:

```
iwcadmin -o base.hstsmaxage -v duration
```

where *duration* represents the number of seconds that a host is remembered as a known HSTS host. A value of **0** disables HSTS. Any value greater than **0** enforces HSTS.

Configuring the Convergence Display Name

You can configure the Convergence Display Name to map to directory server *displayName*.

Table 3-2 lists the configuration parameters for mapping the directory server display name to the Convergence display name.

Table 3-2 Configuration Parameters for Mapping the Directory Server displayName

Parameter	Description
general.screenname	Defines the *screen name* directory server attribute, also referred to as *displayname*. Located in the **useroption-mappings.properties** 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 directory server *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 directory server *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
   ```

Configuring the Corporate Address Book to Perform *displayName* Search

To configure the corporate address book for search by directory server *displayName*, modify the following parameters in the **config/templates/ab/corp-dir/xlate-inetorgperson.xml** file:

1. Search *displayName* and *cn* where *displayName* has a different directory server 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 directory server attribute from *cn*. In this scenario, no modification is required.
3. Search *displayName* only where *displayName* has the same directory server attribute *cn*. In this scenario, no modification is required.

Configuring Convergence to Hide Global Time Zone Selection from Options

To configure Convergence to hide global time zone selection from options (Date & Time), you must set the **client.hideglobaltimezoneselection** configuration parameter to **true**.

To set the parameter to **true**, type the following command.

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

The default value is false.

Configuring Convergence to Prevent Host Header Attack

Host header specifies the host name for an incoming HTTP client request. The web server uses this value of the host header to dispatch the request to the specified website or web application. Since, the HTTP host header is controlled by the user, the user may enter incorrect or malicious information causing a host header attack. To prevent the attack, web servers can configure a virtual host to which the redirection happens in case of a host header attack.

Convergence uses different approaches to prevent host header attack in a single domain and multi-domain environment.

Preventing Host Header Attack in a Single Domain

When the Convergence deployment is in a single domain, you can set the server name in the Oracle WebLogic server settings to prevent the Convergence server from host header attack. However, this approach is only possible when the Convergence deployment is in a single domain.

To set a Server Name in Oracle WebLogic Server:

1. Log in to the Oracle WebLogic Server Administration Console.

2. Select **HTTP** from the **Protocols** menu (**Environment/Servers/ManagedServer/Protocols/HTTP**).

   HTTP is assumed to be in use for Convergence.

3. Enter server name in the **Frontend Host** box.
4. Enter server port in the **Frontend HTTP Port** box.
5. Click **Save**.
6. Restart Oracle WebLogic Server and the Managed Server.

   For more information on mitigating host header attacks on Oracle WebLogic Server, see: https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=255242706168486&id=2356316.1&_afrWindowMode=0&_adf.ctrl-state=ht6sq8y55_4.

Preventing Host Header Attack in Multiple Domains

When multiple domains are configured in the Convergence deployment, you can configure default host and whitelisted hosts to prevent the Covergence server from host header attack. To configure default host and whitelisted hosts, you can set the **base.defaulthost** and the **base. whitelistedhosts** values using the iwcadmin command. For example:

```
iwcadmin -o base.defaulthost -v "abcd.abc.com"
iwcadmin -o base.whitelistedhosts -v "*.abc.com,*.xyz.com"
```

When the **base.defaulthost** and the **base. whitelistedhosts** parameters are set, the following occurs:

- If the domain is a part of whitelisted domains, the user gets redirected to the corresponding domain page.
- If the domain is not a part of whitelisted domains, the user gets redirected to the value configured as **base.defaulthost**.

See "Convergence Properties Reference " for information on **base.defaulthost** and **base. whitelistedhosts**.

When there is a specific login page set for a domain, this domain should be included in the whitelisted hosts, for the redirection to happen as expected.

About Single Sign-On

You can enhance Convergence security by configuring single sign-on (SSO).

Oracle recommends that you deliver SSO functionality using Oracle Access Manager.

You can also configure Convergence for Trusted Circle SSO or write a custom SSO module.

Configuring Convergence for SSO with Oracle Access Manager

You can integrate Convergence with Oracle Access Manager to deliver SSO capabilities.

Setting Up Oracle Access Manager

Install and configure Oracle Access Manager according to its documentation. Refer to *Oracle Fusion Middleware Installation Guide for Oracle Identify Management* for detailed installation and configuration information as you complete the following tasks:

1. Install Oracle Database. During the installation, specify the following:
   - For **Installation Option**, select **Create and Configure a Database**.
   - For **System Class**, select **Desktop**.
   - Ensure the database has write permissions to the Oracle Base folder.
   - For **Character Set**, select **UNICODE**.
2. Set the following environment variables:
   - export ORACLE_HOME=*database_home*

     where *database_home* is the database instance directory.
   - export PATH=**$ORACLE_HOME/bin:$PATH**
   - export ORACLE_SID=*database_SID*
3. Tune the following database parameters:
   - SQL>alter system set processes=500 scope=spfile;
   - SQL>alter system set open_cursors=1500 scope=spfile;
   - SQL>alter system set session_cached_cursors=500 scope=spfile;
   - SQL>alter system set session_max_open_files=50 scope=spfile;
   - SQL>alter system set aq_tm_processes=1 scope=spfile;
   - SQL>alter system set job_queue_processes=10 scope=spfile;
4. Create the schemas for Oracle Access Manager on the database using the Oracle Repository Creation Utility.
5. Install and configure Oracle WebLogic Server.
6. Install Oracle Access Manager and deploy it to the WebLogic server.
7. Using the Oracle Access Manager console, configure an identity store for the Unified Communications Suite directory server. Specify the following values:
   - For **Store Type**, select the directory server used.
   - For **Location**, enter your directory server location.
   - For **Bind DN**, enter **cn=directory manager**.
   - Specify the directory server user search base. For example, enter **o=***my_domain***.com,o=isp**.
   - For **Group Name Attribute**, enter **cn**.
   - Specify the directory server group search base. For example, enter **o=***my_domain***.com,o=isp**.
8. Using the Oracle Access Manager console, configure an authentication module for the new identity store.
9. Using the Oracle Access Manager console, change the authentication scheme to use the new authentication module.
10. Install and configure Oracle Web Tier and Oracle HTTP Server. Ensure the following:
    - Modify **mod_wl_ohs.conf**. Add or replace the following lines:

```
<IfModule weblogic_module>
  WebLogicHost OAM_Host
  WLLogFile /tmp/weblogicdebug
  Debug ON
```

```
  DynamicServerList Off
  WebLogicPort OAM_ADMIN_SERVER_PORT
</IfModule>
```

The **mod_wl_ohs.conf** file enables communication between Oracle Access Manager and Oracle HTTP Server.

- Create an Oracle wallet with a signed certificate from a certificate authority and a user certificate.
- Modify **httpd.conf**. Locate the section in the file similar to the example below. Modify the section to match the example below, replacing the sample values.

```
ProxyRequests Off
SSLProxyEngine On
SSLProxyWallet "Oracle_Wallet_Absolute_Path"
RequestHeader set Front-End-Https "On"
ProxyPass /iwc https://Host:Port/iwc
ProxyPass /iwc_static https://Host:Port/iwc_static
ProxyPassReverse /iwc https://Host:Port/iwc
ProxyPassReverse /iwc_static https://Host:Port/iwc_static
<Location "/iwc">
  Order allow,deny
  Allow from all
</Location>
<Location "/iwc_static">
  Order allow,deny
  Allow from all
</Location>
```

- Modify **ssl.conf**. Turn on **SSLEngine** and set **SSLWallet** to the user wallet location.

11. Configure the Convergence Oracle WebLogic server:
    - Enable SSL in Convergence. See "About SSL in Convergence" for more information.
    - Import the certificate authority certificate used in the Oracle wallet into the Oracle WebLogic server.
12. Install and configure a webgate for Oracle HTTP Server. Ensure the following:
    - Register the webgate on Oracle Access Manager using the administration console. Ensure the following:
      - For the base URL, enter **http://***HTTP_Host***:***port*, where *HTTP_Host* is the Oracle HTTP Server host name and *port* is the Oracle HTTP Server port number.
      - For the logout redirect URL, enter the URL to the location of the custom logout redirect script you will create later.
    - Copy the generated files and artifacts to the Oracle HTTP Server webgate instance location.
13. In the policy configuration for Oracle Access Manager, configure authentication and authorization policies to pass user email attributes in email header variables. Set up the policies with the following values on the **Responses** tab:
    - For **Name**, specify the Oracle Access Manager mail ID.
    - For **Type**, select **Header**.
    - For **Value**, enter **${user.attr.mail}**.

Enabling SSO with Oracle Access Manager

To configure Convergence for SSO with Oracle Access Manager:

1. Using the **iwcadmin** command, set the following properties:
   - Set **sso.oam.enable** to **true**
   - Set **sso.misc.OAMAuthHeader** to the Oracle Access Manager mail ID
   - Set **sso.misc.OAMLogoutUrl** to the URL of the custom logout redirect script
2. Ensure that the idle session time-out value in Convergence (**client.autologouttime**) is the same as in Oracle Access Manager. In Oracle Access Manager, the idle session time out is on the System Configuration page under Common Settings.
3. Create a custom HTML logout redirect script. Place the script inside the Oracle HTTP Server or the Convergence Oracle WebLogic server domain. Ensure the following:
   - The webgate for Oracle Access Manager logout redirect URL points to this script.
   - The Convergence sso.misc.OAMLogoutUrl parameter points to this script.
   - The logout script clears any cookies belonging to applications protected by Oracle Access Manager, including applications under other webgates.

   See "Sample Custom Logout Redirect Script" for a sample custom logout redirect script.

Sample Custom Logout Redirect Script

This section provides a sample custom HTML logout redirect script. This sample script uses `https://Convergence_Server:port/iwc/svc/iwcp/lougout_oam.iwc` as the new logout URL. The logout script can be run from any tab in the same browser session and does not require a token parameter.

You can copy the following sample and use it as a starting point for your own custom HTML logout redirect script.

```
<!DOCTYPE html>
<html>
<head>
<title>logout_oam_custom_script.html</title>
<script type="text/javascript">
//Replace "<OAM_SERVER_HOST:PORT>" by OAM server and its port.
Example:"example.my_oam_server.com:14100"
var timedout = false;
var timeoutDuration = 0; //should be set, if we want to make sure logout process is not
stuck at this page for long time. Unit is seconds
var protectedAppClearCookieURL = [];
var logoutAttemptedAppCount = 0;
function logout(){

    for (var i=0; i < protectedAppClearCookieURL.length ; ++i){
        var img = document.createElement("img");
        img.onload = imageLoadedHandler;
        img.onerror = imageErrorHandler;
        img.src = protectedAppClearCookieURL[i];
    }

    if(timeoutDuration){
        setTimeout(function(){
            timedout = true;
            errorOccurred = true;
            doRedirect();
        },timeoutDuration);
    }

}
```

```
function imageLoadedHandler() {
    logoutAttemptedAppCount++;

    if (logoutAttemptedAppCount >= protectedAppClearCookieURL.length) {
        doRedirect();
    }
}

function imageErrorHandler() {
    logoutAttemptedAppCount++;
    errorOccurred = true;

    if (logoutAttemptedAppCount >= protectedAppClearCookieURL.length){
        doRedirect();
    }
}

function doRedirect() {
    if(errorOccurred) {
        //Cuurently ignoring error..@TODO handle this
        //alert('LOGOUT_ERROR');
    }
    document.location.href =  "http://OAM_SERVER_HOST:Port/oam/server/logout";     //
default logout redirect URL handler
}

</script>
</head>
<body onload="logout()">
    <CENTER>
        <BR/>
            <IMG src="http://OAM_SERVER_HOST:Port/oam/pages/images/wait.gif" border="0"
ALT=""/>
        <BR/>
    </CENTER>
</body>
</html>
```

Configuring 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
```

Enabling SSO, by default enables single sign-off.

To manually enable single sign off, enter the following command:

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

> **Note:**
>
> Multi-Factor Authenticator feature should not be enabled when SSO is enabled in Convergence.

Writing a Custom SSO Module

To enhance security in Convergence, you can write your own custom modules for authentication or single sign-on. For more information, refer to the discussion about security considerations for developers in *Convergence Security Guide*.

Directory Server Services for Convergence

This section explains the different directory server services for Convergence.

Configuring Directory Server Failover

To configure Convergence for directory server failover, enter:

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

ldap1:port1 and **ldap2:port2** are the directory servers that are a part of the failover.

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

Configuration Management

This section explains the administrative tasks pertaining to configuration management.

Configuring 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 the Oracle WebLogic server.

The following log message appears indicates that the SSL configuration is 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 **iwcadmin.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 **iwcadmin** command.
2. Set the **truststorepath** parameter to the directory where you stored the trust store.
3. Set a password for truststorepasswd.

Changing Convergence Administrator Password

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

```
iwcadmin -o admin.adminpwd -v new_password
```

Deployment-Specific Customizable Client Options for Convergence

- Customizing the Login URL and Page for a Specific Domain
- Configuring Another Page for Changing Password
- Configuring Another Page for Changing Password for users of a specific domain
- Setting the Auto Logout Time

Customizing the Login URL and Page for a Specific Domain

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. 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, 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.

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

Configuring Another Page for Changing Password

To configure Convergence to use a different page for changing user password, set the **client.changepasswordpage** configuration property by typing the following command.

```
iwcadmin -o client.changepasswordpage -v <URL to the password management page>
```

When **client.changepasswordpage** is set, the **Change Password** tab in Convergence Global Options displays a link to the configured password management page. The default Change Password Page provided by Convergence can be retained by resetting the value of this configuration parameter.

```
iwcadmin -o client.changepasswordpage -v  ""
```

This will reset the default Change Password page provided by Convergence and will display the text boxes to enter Current Password and New password.

The following scenarios apply:

User's Password is About to Expire

Convergence handles password policies applied to user in Directory Server.

When a user login with the password that is about to expire, the "Change Password" and "Remind me Later" buttons are displayed in the Convergence banner.

- When **client.changepasswordpage** is not set, clicking "Change Password" button, redirects the user to the default Change Password Page provided by Convergence.
- When **client.changepasswordpage** is set, clicking "Change Password" button, redirects the user to the configured password management page to change the password.

User's Password is Expired

Convergence handles password policies applied to user in Directory Server.

- When **client.changepasswordpage** is not set and a user logins with the expired password, a warning message is displayed in the Convergence Login page.The user has to contact system administrator to change the password for this user.
- When **client.changepasswordpage** is set and a user logins with the expired password, a warning message is displayed in the Convergence Login page along with the "Change Password" button. The UserName, Password fields and "Sign In" buttons will be disabled on the Login page. Clicking "Change Password" button, redirects the user to the configured password management page to change the password.

User's Password is Reset by Administrator

Convergence handles password policies applied to user in Directory Server.

- When **client.changepasswordpage** is not set and a user logins with the new password provided by administrator, user can login to Convergence. Depending on the password policy rules, user will be forced to change the password using the Change Password dialog box that appears.
- When **client.changepasswordpage** is set and a user logins with the new password provided by administrator, a warning Message is displayed on the Convergence Login page along with the "Change Password" button. The UserName, Password fields and "Sign In" button will be disabled on the Login page. Clicking "Change Password" button, redirects user to the configured password management page to change the password.

Configuring Another Page for Changing Password for users of a specific domain

In a Convergence deployment with multiple domains, users can login to a domain by typing the URL and suffix the domain name to the user name.For example, **user1@siroe.com**.

To set a different Change Password page for a domain, set the **client.{domain-name}.changepasswordpage** configuration property by typing the following command.

```
iwcadmin -o client.{domain_name}.changepasswordpage -v <URL to the password management
page>
```

where, *domain_name* is the domain name.

When **client.{domain-name}.changepasswordpage** is set, the **Change Password** tab in Convergence Global Options displays a link to the configured password management page for the users of the specified domain.

The following scenarios apply:

User's Password is About to Expire

Convergence handles password policies applied to user from each domain in Directory Server.

When a user login with the password that is about to expire, the "Change Password" and "Remind me Later" buttons are displayed in the Convergence banner.

- When the **client.changepasswordpage** and the **client.{domain-name}.changepasswordpage** are not set, clicking "Change Password" button redirects the users from all the domains to the default Change Password Page provided by Convergence.
- When the **client.changepasswordpage** is set and the **client.{domain-name}.changepasswordpage** is not set, clicking "Change Password" button, redirects the users from all the domains to the configured password management page to change the password.
- When the **client.changepasswordpage** is set and the **client.{domain-name}.changepasswordpage** is set for *domain_name1*, clicking "Change Password" button:
  - Redirects the users from *domain_name1* to the password management page configured for the *domain_name1*.
  - Redirects the users from other domains to the configured password management page defined by the **client.changepasswordpage**.
- When the **client.changepasswordpage** is not set and the **client.{domain-name}.changepasswordpage** is set for *domain_name1*, clicking "Change Password" button:
  - Redirects the users from *domain_name1* to the password management page configured for the *domain_name1*.
  - Redirects the users from other domains to the default Change Password page provided by Convergence.

User's Password is Expired

Convergence handles password policies applied to user from each domain in Directory Server.

- When the **client.changepasswordpage**, the **client.{domain-name}.changepasswordpage** are not set and user logins with the expired password, a warning message is displayed in the Convergence Login page.The user has to contact system administrator to change the password for this user.
- When the **client.changepasswordpage** is set, the **client.{domain-name}.changepasswordpage** is not set, and a user logins with the expired password, a warning message is displayed in the Convergence Login page along with the "Change Password" button. The UserName, Password fields and "Sign In" button will be disabled on

the Login page. Clicking "Change Password" button, redirects the users from all the domains to the configured password management page to change the password.

- When the **client.changepasswordpage** is set, the **client.{domain-name}.changepasswordpage** is set for *domain_name1*, and a user logins with the expired password, a warning message is displayed in the Convergence Login page along with the "Change Password" button. Clicking "Change Password" button:
  - Redirects the users from *domain_name1* to the password management page configured for the *domain_name1*.
  - Redirects the users from other domains to the configured password management page defined by the **client.changepasswordpage**.
- When the **client.changepasswordpage** is not set and the **client.{domain-name}.changepasswordpage** is set for *domain_name1*, and a user logins with the expired password, a warning message is displayed in the Convergence Login page along with the "Change Password" button.
  - For the users from *domain_name1*, clicking "Change Password" button, redirects the user to the password management page configured for the *domain_name1*.
  - For the users from other domains, the "Change Password" button is not displayed and they have to contact system administrator to change the password.

User's Password is Reset by Administrator

Convergence handles password policies applied to users from each domain in Directory Server.

- When the **client.changepasswordpage**, the **client.{domain-name}.changepasswordpage** are not set and a user logins with the new password provided by administrator, the user can login to Convergence. Depending on the password policy rules, user from all the domains will be forced to change the password using the Change Password dialog box that appears.
- When **client.changepasswordpage** is set, **client.{domain-name}.changepasswordpage** is not set, and a user logins with the new password provided by administrator, a warning message is displayed on the Convergence Login page along with the "Change Password" button. The UserName, Password fields and "Sign In" button will be disabled on the Login page. Clicking "Change Password" button, redirects user to the configured password management page to change the password.
- When **client.{domain-name}.changepasswordpage** is set for *domain_name1*, **client.changepasswordpage** is set, and a user logins with the new password provided by administrator, a warning message is displayed in the Convergence Login page along with the "Change Password" button. The UserName, Password fields and "Sign In" button will be disabled on the Login page. Clicking "Change Password" button:
  - Redirects the users from *domain_name1*, to the password management page configured for the *domain_name1*.
  - Redirects the users from other domains to the configured password management page defined by **client.changepasswordpage.**
- When the **client.changepasswordpage** is not set, the **client.{domain-name}.changepasswordpage** is set for *domain_name1*, and a user logins with the new password provided by administrator.
  - For the users from *domain_name1*, a warning message is displayed in the Convergence Login page along with the "Change Password" button. The UserName, Password fields and "Sign In" button will be disabled on the Login page. Clicking

"Change Password" button, redirects the user to the password management page configured for the *domain_name1*.

- Users from other domains can login to Convergence. Depending on the password policy rules, the user will be forced to change the password using the Change Password dialog box that appears.

Setting the Auto Logout Time

You can configure Convergence to automatically log users out of the session after a specified number of minutes. By default, auto logout is set to 15 minutes. To configure auto logout, set the **client.autologouttime** property, as shown in the following example:

```
iwcadmin -o client.autologouttime -v logout_time
```

Where *logout_time* is an integer equal to or greater than zero. Set **client.autologouttime** to zero to disable auto logout, preventing Convergence from logging out users for inactivity.

Verifying 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. Enter the following command:

   ```
   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:**
   >
   > Where **/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. For example.

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

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

   ```
   admin123 ---> rE9ZIq6H0r49RgsQrKHXsw==
   ```

4. Compare the encrypted password (rE9ZIq6H0r49RgsQrKHXsw==) 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...
```

Creating a Directory Server User to Manage Convergence

A user must have a minimum set of privileges to manage directory server 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 **ldapmodify** command, create the user:

```
ldapmodify -h hostname -p port -D "cn=Directory Manager" -w pwd -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 ug_ldap_bindpassword
```

Configuring VLV 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.

- base DN
- filter
- sort order
- scope of the index

> **Note:**
>
> If you have multiple back-end Directory Servers that store user group information, you must create the indexes on all the instances. For more information, see Indexing Directory Data in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Applying the VLV Browsing Index Settings

Use the **ldapmodify** command to specify the Directory Server browsing search indexes. For 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 a scheduled change window. This is because the Directory Server needs to be restarted. For more information, see Generating Indexes.

Follow these steps to create vlv indexing in OUD. For more information, see Creating a New VLV Index in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

1. Change the directory to the Directory Server Instance location:

   ```
   cd /opt/oracle/Oracle/Middleware/asinst_1/bin
   ```

2. Use `dsconfig` to create a new VLV index as follows:

   ```
   dsconfig -h ldap_host -p 4444 -D "cn=directory manager" -j pwd-file -n \
     create-local-db-vlv-index \
     --element-name backend --index-name name --set sort-order:attributes \
   --set scope:scope --set base-dn:baseDN --set filter:filter
   ```

   where:

   - `index-name` specifies a unique index name, which cannot be altered after the VLV index is created.
   - `sort-order` specifies the names of the attributes by which the entries are sorted and their order of precedence, from highest to lowest.
   - `scope` specifies the LDAP scope of the query being indexed and can be one of `base-object`, `single-level`, `subordinate-subtree`, or `whole-subtree`.
   - `base-dn` specifies the base DN used in the search query being indexed.
   - `filter` specifies the LDAP filter used in the query being indexed and can be any valid LDAP filter.

   To know the value for the element name, use the command:

   ```
   ./dsconfig -h ldap_host -p 4444 -D "cn=Directory Manager" -j
   <pwd_file_location>  -X -n list-workflow-elements
   Workflow Element    : Type               : enabled
   --------------------:--------------------:--------
   adminRoot           : ldif-local-backend : true
   userRoot            : db-local-backend   : true
   virtualAcis         : db-local-backend   : true
   ```

```
we-ucs-comms-config : db-local-backend   : true
we-ucs-mlusers      : db-local-backend   : true
we-ucs-PiServerDb   : db-local-backend   : true
```

For example:

```
./dsconfig -D "cn=directory manager" -j
          <pwd_file_location> -n create-local-db-vlv-index --element-name
userRoot
            --index-name vlvtest --set sort-order:"cn"
          --set scope:whole-subtree --set base-dn:o=usergroup--set
      filter:"(&(mail=*)(cn=*))"
```

3. Check that the index was created by listing the existing VLV indexes:

```
$ dsconfig -h ldap_host -p 4444 -D "cn=directory manager" -j
        pwd-file -n \ list-local-db-vlv-indexes \ --element-name backend
```

4. Display the index properties to verify your changes:

```
$ dsconfig -h ldap_host -p 4444 -D "cn=directory manager" -j pwd-file -n \
get-local-db-vlv-index-prop \ --element-name backend --index-name name
```

5. Rebuild the index. You can either stop the server, rebuild the index, and restart the server:

```
stop-ds
rebuild-index --baseDN baseDN --index vlv.name
start-ds
```

Or, you can rebuild the index online by running the rebuild-index command as a task:

```
rebuild-index -h ldap_host -p 4444 -D "cn=Directory manager" -j pwd-file -
X \
--baseDN baseDN --index vlv.name
```

Handling 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 3-3 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_Domain***/jsp/samplefiles/MailServiceErrorJSON.jsp**.

Table 3-3 lists the requests that are redirected, the URL patterns, and appropriate error responses.

Table 3-3 Requests that are Redirected, URL Patterns, and Error Responses

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

4

Enabling Core Services for Convergence

You can integrate Oracle Communications Convergence with other Oracle Communications products to provide the following core services:

- Email and messaging, provided by Oracle Communications Messaging Server.
- Calendar, provided by Oracle Communications Calendar Server.
- Address book, provided by Convergence or Oracle Communications Contacts Server.

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)

Enabling Services for the Entire Convergence Installation

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 and calendar 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**. See *Convergence Installation and Configuration Guide* for more information.

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.

Use the Convergence **iwcadmin** command-line utility to set the following options to either **true** or **false**:

- **mail.enable**
- **caldav.enable** (for Calendar Server 7 and Calendar Server 8)
- **ab.enable** (for Convergence address book service) or **nab.enable** (for Contacts Server address book service)

> **Note:**
>
> In an address book co-existence scenario, set both **ab.enable** (Convergence) **nab.enable** (Contacts Server).

Enabling Services for an Individual User or Domain

To enable or disable a service for a user or domain, you must set the appropriate directory server attributes for that service in the user entry or domain entry in the directory server.

Managing Service Access Through the Directory Server

Managing services through the directory server affects user access to Convergence and to the software products that deliver the Convergence services. This is a very different conceptual territory than controlling the services available through Convergence, the client. When you disable directory server service attributes, user access to the software that provides service is also disabled. All clients are disabled for those users, not only Convergence.

To manage access to services in the directory server:

1. Install and configure the Oracle Communications software that delivers services in Convergence: Messaging Server, Calendar Server, and Contacts Server (optional).
2. Manage the services available to users and domains in the directory server. When you change a user's access to a service in the directory server, you affect that user's access to Messaging Server or Calendar Server, no matter which clients that user may use to access these services. Similarly, when you change domain-level services in the directory server, you affect the access to services for all users in the domain.
3. Manage 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" for more information.

See "Enabling Services for an Individual User or Domain" for more information.

Enabling and Disabling Services with Directory Server Provisioning

You can configure mail or calendar services by setting the appropriate directory server user and domain attributes. You can use directory server tools or provisioning scripts (if they have been developed at your site).

Directory Server 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
```

Directory Server Attributes for Calendar Service

To enable calendar service to 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
```

5

Mail Service Administration

This chapter describes how to administer the mail service in Oracle Communications Convergence.

See "Enabling Core Services for Convergence" for information about enabling services.

Managing Attachment Previewing

By default, Convergence can preview only JPG, GIF, and TXT email attachments. In a desktop environment, native applications must be installed to view email attachments such as Office documents, or browser plug-ins must be installed in the browser to enable Convergence to preview PDF attachments.

If Convergence is integrated with Oracle Outside In Transformation Server, Convergence is capable of previewing many different file types regardless of the web browser, including DOC and XLS type email attachments.

See *Convergence Installation and Configuration Guide* for information about installing Outside In Transformation Server and configuring it for Convergence.

About Outside In Transformation Server and the Outside In Proxy

Each time a user previews an attachment, Convergence attempts to open it in the browser. If Convergence is not able to open the attachment by default, it sends the attachment to Outside In Transformation Server. The transformation server transforms the attachment into HTML, which Convergence can render in the browser.

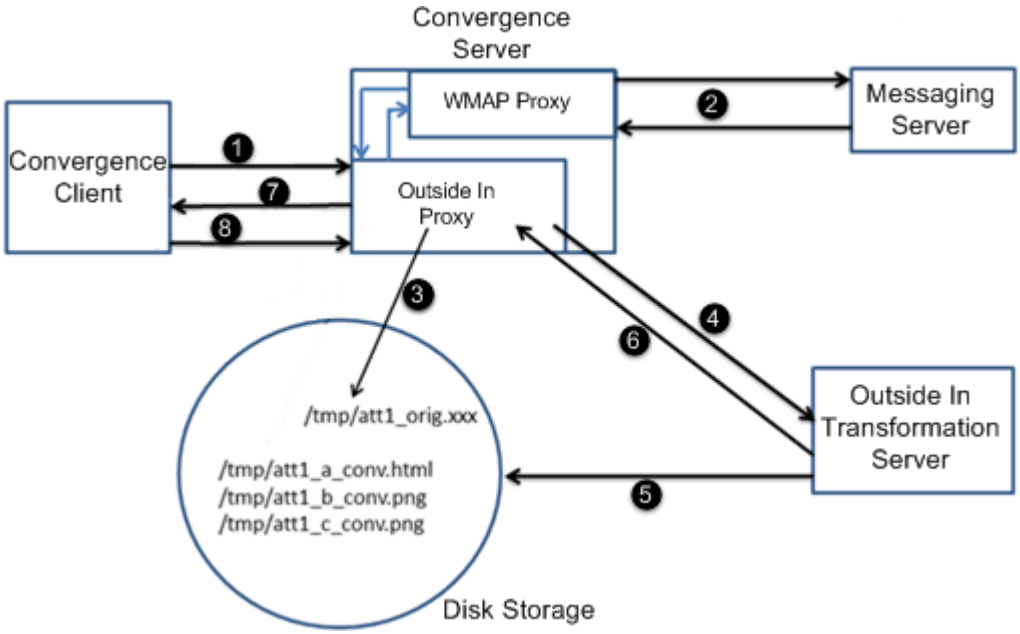
The transformation server can handle a large number of simultaneous requests by placing attachment requests in a queue.

The Outside In proxy creates a temporary directory for each user requesting to view attachments. For each transformation, the Outside In proxy creates a temporary subdirectory under the user directory. The Outside In proxy passes the input directory containing the transformed attachment and the output directory of the transformed attachment to the Transformation Server. The Outside In proxy deletes the subdirectory after a configurable time-out period has passed.

The Convergence server manages file management to the transformation server. Convergence uses a session cookie and a server-generated URL token for each attachment request. For security, Convergence masks the URL token.

Figure 5-1 shows the attachment preview workflow.

Figure 5-1 Convergence Attachment Request Workflow



The following list explains the attachment preview workflow from Figure 5-1.

1. The Convergence client sends the request to the Convergence server.

   If the request is for an attachment type that can be rendered natively in the browser, the request is sent to the WMAP proxy.

   If the request is for an attachment type that cannot be rendered natively in the browser, the request is first passed to the Outside In proxy, and then to the WAMP proxy.

2. The request is sent to the Messaging server. The Messaging server sends the attachment back to the Convergence server.

3. For attachment types that cannot be rendered natively in the browser, the Outside In proxy sends the response from the Messaging server to the disk storage.

4. For attachment types that cannot be rendered natively in the browser, the Outside In proxy communicates where it saved the attachment to the Outside In Transformation server, and also informs the transformation server where to save the attachment after it has been converted.

5. For attachment types that cannot be rendered natively in the browser, the transformation server converts the attachment into a format that can be natively rendered in the browser and saves it to the directory provided by the Outside In proxy.

6. For attachment types that cannot be rendered natively in the browser, the transformation server informs the Outside In proxy that it has completed transforming the file.

7. If the original request was for an attachment type that could be rendered native in the browser, the Convergence server sends the attachment to the browser.

   If the original request was for an attachment type that could not be rendered native in the browser, the Outside In proxy provides the browser with a redirection URL to the transformed attachment on the disk storage.

8. If the original request was for an attachment type that could not be rendered native in the browser, the Convergence client accesses the transformed attachment using the URL provided by the Outside In proxy and renders it in the browser.

Configuring File Directory Access

Convergence and Outside In Transformation Server have to be configured so that they can both read and write attachments in the storage disk. Convergence must have full permissions to the storage disk to read, write, and delete files.

The Convergence Server and the Outside In Transformation Server can run on the same machine or on different machines. Configure the transformation server as a network file system (NFS).

- If the transformation server is running on Solaris:
  - Share the **/export/tsdir/** directory.

    ```
    chmod 700 /export/tsdir
    ```

  - Edit **/etc/dfs/dfstab** and add the following line:

    ```
    share -F nfs -d [-o root=host_name] "tsdir" /export/tsdir
    ```

    Include the **-o** parameter when the Convergence server and the transformation server are running as local root, where *host_name* is the host name of the Convergence server. Omit the **-o** parameter when the Convergence server and the transformation server are running as the same user.

  - Create a soft link or mount to the NFS directory. For example:

    ```
    -s //net/host_name/export/tsdir /export/tsdir
    ```

- If the transformation server is running on Linux:
  - Share the **/export/tsdir/** directory:

    ```
    chmod 700 /export/tsdir
    ```

  - If the Convergence server and the transformation server are running as the same user, edit **/etc/exports** and add the following line:

    ```
    /export/tsdir
    ```

    If the Convergence server and the transformation server are running as local root, edit **/etc/exports** and add the following line:

    ```
    /export/tsdir host_name(rw,no_root_squash)
    ```

  - Create a soft link or mount to the NFS directory. For example:

    ```
    -s //net/host_name/export/tsdir /export/tsdir
    ```

The Outside In proxy generates a unique URL for each attachment and provides it to the Convergence client.

The following example shows the sample configuration settings for Outside In proxy in the Convergence **configuration.xml** file:

```
<OINService>
     <ServiceName v="SUN_OIN_SERVICE"/>
     <BackendServiceDetails>
          <Enable v="true"/>
          <HostName v="oin server name"/>
          <PortNumber v="60611"/>
```

```
    </BackendServiceDetails>
    <TsdirPath v="/export/tsdir"/>
    <AutoPruneInterval v="5"/>
</OINService>
```

You can use the **iwcadmin** command to configure the parameters for the Outside In proxy.

Managing Attachment Life Cycles

The Outside In proxy manages the life cycle of attachments, including temporary directories, file creation, deletion, and purging, and the number of directories and disk space per user.

By default, the Outside In proxy automatically deletes an attachment from the storage disk after five minutes.

Use the **iwcadmin** command to configure the duration after which attachments are deleted from the storage disk. For example, to configure the proxy to delete attachments from the disk after three minutes:

```
iwcadmin -o oin.autopruneinterval -v 3
```

Supporting Extended Character Locales

Oracle Outside In Transformation Server supports many typical font sets and some extended font sets. However, depending on the locales being used in your deployment, you may need to install and configure additional font sets to support the rendering of attachments.

By default, when the transformation server cannot render characters because the font is missing, it replaces the character with an asterisk. For example, if a user is using Convergence with the Japanese locale, but the transformation server does not have access to Japanese font sets, the transformation server will render attachments with asterisks.

Install all required fonts on the host machine where the transformation is installed and export the GDFONTPATH environment variable.

See the Oracle Outside In Technology documentation for more information.

Customizing Transformation Blacklist

The Outside In Transformation Server blacklist enumerates the types of files that are prevented from being sent to the transformation server, such as ZIP files or EXE files.

You can customize the blacklist to add or remove file types. See the discussion about customizing the attachment blacklist in for more information.

About HTML Filtering

You can configure Convergence to filter embedded HTML content from email messages, because such content could contain malicious code. By default, HTML filtering is enabled. When HTML filtering is enabled:

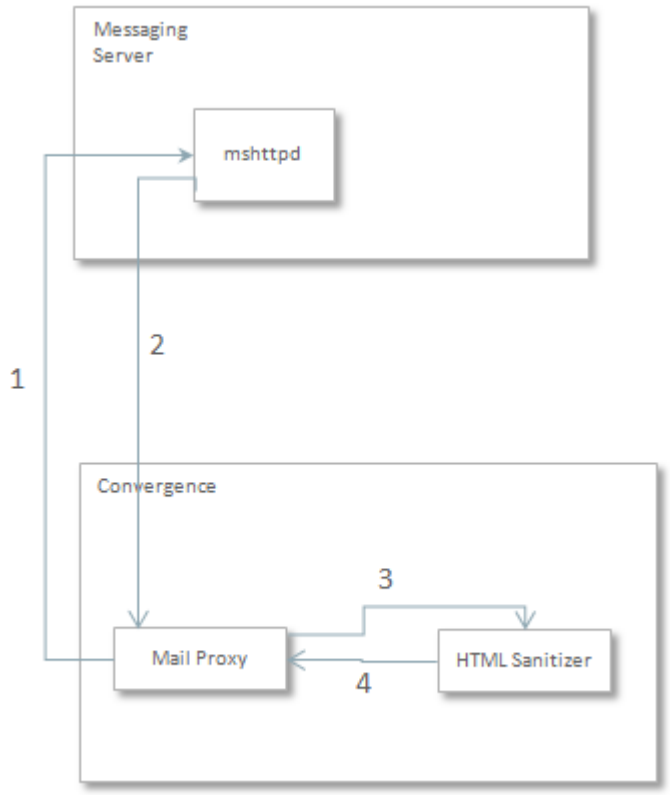
- Convergence removes specified elements, attributes, protocols, and CSS properties from incoming email messages before routing the messages to users.
- Convergence provides an option to allow the URLs in inline styles in email messages. This can be set by using the **mail.htmlsanitizer.allowurlsinstyle** parameter. This option should be enabled only when the URL referenced in the email message is from trusted source

and is secure. See "Convergence Properties Reference " for information on mail.htmlsanitizer.allowurlsinstyle.

Convergence includes a default whitelist, a blacklist, a CSS whitelist of HTML elements, attributes, protocols, and CSS properties. Whitelisted and CSS whitelisted entries are permitted in email messages. Blacklisted entries are removed from email messages. Elements, attributes, protocols, and CSS properties that do not appear on any of these whitelists are treated as blacklist entries.

Figure 5-2 shows the approach that is used for HTML filtering in Convergence.

Figure 5-2 HTML Filtering in Convergence



Configuring HTML filtering consists of the following tasks:

- Enabling and Disabling HTML Filtering
- Configuring HTML Filtering in Convergence

Enabling and Disabling HTML Filtering

You enable and disable HTML filtering using the **iwcadmin** command. By default, HTML filtering is enabled.

To enable or disable HTML filtering, enter:

```
iwcadmin -o mail.htmlsanitizer.enable -v {true|false}
```

when the **mail.htmlsanitizer.enable** parameter is set to **false**, HTML content is not displayed in the email message. Only the text or plain content is displayed in the Convergence email

message. To display the HTML content, set the **role.http.convergencefilterenabled** parameter to **true** in the Messaging Server. See the discussion about HTML Filtering in your Messaging Server documentation.

> **Note:**
>
> In Convergence 3.0.1 patch sets, the HTML filtering is disabled by default. If you are installing Convergence 3.0.1 patch sets, see Table 5-1 for the information on recommended configurations for HTML filtering in Convergence and Messaging Server.

Table 5-1 Recommended Configurations for HTML Filtering in Different Releases of Convergence and Messaging Server

Convergence	Messaging Server	Recommended Configuration in Convergence	Recommended Configuration in Messaging Server
3.0.3 X	8.1.X and later	mail.htmlsanitizer.enable = true	No additional configurations required
3.0.2 X	8.0.2.2 and later	mail.htmlsanitizer.enable = true	No additional configurations required
3.0.2 X	8.0.2.2 and later	mail.htmlsanitizer.enable = false	http.convergencefilterenabled = 1 http.enableblacklistfilter = 1
3.0.1.1.0 to 3.0.1.4.0	8.0.2 to 8.0.2.1	mail.htmlsanitizer.enable = true/false	http.convergencefilterenabled = 1 http.enableblacklistfilter = 1
3.0.1.1.0 to 3.0.1.4.0	Below 8.0.2	mail.htmlsanitizer.enable = true/false	No additional configurations available
Below 3.0.1.1.0	Below 8.0.2	No additional configurations available	No additional configurations available

> **Note:**
>
> Convergence releases before 3.0.1.1.0 release were completely dependent on the blacklist based filtering provided by Messaging Server for HTML filtering. Whitelist based filtering was introduced in Convergence 3.0.1.1.0 release. Oracle recommends Convergence for HTML filtering rather than Messaging Server.The blacklist filter (**http.enableblacklistfilter**) has been disabled from Messaging Server 8.0.2 release onwards and a new parameter, **http.convergencefilterenabled**, has been introduced for HTML filtering. Only when this parameter is set to 1, mshttpd will send HTML content in the message body and expects the content to be sanitized by Convergence.

Configuring HTML Filtering in Convergence

The default Convergence whitelist includes all known safe HTML elements, attributes, and protocols. The default Convergence blacklist includes all known potentially harmful HTML elements, attributes, and protocols. The default Convergence CSS whitelist includes all known safe CSS properties.

Blacklist takes precedence over whitelist; that is, if an element is present in both whitelist and blacklist, the element will be considered as blacklisted and the element will not be allowed in the email content.

You use the **iwcadmin** command to create an additional whitelist, blacklist, CSS whitelist with additional elements, attributes, protocols, or CSS properties.

It is not possible to modify the default whitelist, blacklist, or CSS whitelist. The contents of the default lists are deliberately excluded from this documentation, as such information could be used to target whitelisted values.

To configure the additional blacklist:

```
iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "filtering_value"
```

To configure the additional whitelist:

```
iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v "filtering_value"
```

To configure the additional CSS properties for whitelist:

```
iwcadmin -o mail.htmlsanitizer.additionalCSSwhitelist -v "filtering_value"
```

Where *filtering_value* is a comma-separated list of HTML elements, attributes, protocols, or CSS properties.

The following example shows a sample configuration using the additional blacklist:

- Do not allow *attribute1* and *attribute2* on all elements
- `iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "attribute1, attribute2"`
- Do not allow *attribute1* on *element1* only.

  `iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "attribute1@element1"`
- Do not allow *element1* and *element2*.

  `iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "@element1,@element2"`
- Do not allow *element1*. Do not allow *attribute1* on any element. Do not allow *attribute2* on *element2*.

  `iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "@element1,attribute1, attribute2@element2"`
- Do not allow *attribute1*, *attribute2* and *attribute3* on *element1*.

  `iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "attribute1@element1,attribute2@element1, attribute3@element1"`
- Do not allow protocol1. Colon(:) at end indicates it is a protocol.

  `iwcadmin -o mail.htmlsanitizer.additionalblacklist -v "protocol1:"`

For example:

```
iwcadmin -o mail.htmlsanitizer.additionalblacklist  -v "@source,srcdoc@iframe,ftp:"
```

With this settings, HTML element *source*, *srcdoc* attribute of HTML element *iframe*, and *ftp* protocol will not be allowed in the mail content.

The following example shows a sample configuration using the additional whitelist:

- Allow *attribute1* and *attribute2* on all elements
- `iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v "attribute1, attribute2"`

- Allow *attribute1* on *element1* only.

  ```
  iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v "attribute1@element1"
  ```

- Allow *element1* and *element2*.

  ```
  iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v "@element1,@element2"
  ```

- Allow *element1*. Allow *attribute1* on any element. Allow *attribute2* on *element2*.

  ```
  iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v "@element1,attribute1,
  attribute2@element2"
  ```

- Allow *attribute1*, *attribute2* and *attribute3* on *element1*.

  ```
  iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v
  "attribute1@element1,attribute2@element1, attribute3@element1"
  ```

- Allow protocol1. Colon(:) at end indicates it is a protocol.

  ```
  iwcadmin -o mail.htmlsanitizer.additionalwhitelist -v "protocol1:"
  ```

For example:

```
iwcadmin -o mail.htmlsanitizer.additionalwhitelist  -v "testattr2@div, abc:"
```

With this settings, *testattr2* (custom attribute) of HTML element *div*, and protocol *abc* (custom protocol) will be allowed in the mail content.

> **Note:**
>
> For additionalwhitelist and additionalblacklist, if an attribute is specified without an associated element, then that attribute will not be allowed on any element.

The following example shows a sample configuration while configuring the additional CSS properties for whitelist:

```
iwcadmin -o mail.htmlsanitizer.additionalCSSwhitelist -v "item_1,item_2"
```

where *item* is a CSS property like visibility and z-index.

> **Note:**
>
> Only few additional CSS properties can be added to the whitelist. You can check the logs to identify the unsupported CSS property and remove it from the whitelist.

Convergence allows the URLs in inline styles in email messages. This can be set by using the **mail.htmlsanitizer.allowurlsinstyle** parameter. Enabling this option is vulnerable to XSS. This option should be enabled only when the URL referenced in the email message is from trusted source and is secure.

In this example, the **image.png** displays in the email message when **mail.htmlsanitizer.allowurlsinstyle** is set to true:

Restricting Attachment Types for End-Users

You can configure the type of files that can be attached to an email in Convergence 3.0.3.4.0. Depending on the configuration , the end user will not be able to attach any restricted file types, such as .dll, .exe, .py and will also not be able to save it on draft. If the user tries to upload a restricted attachment, an error message will be displayed in the Convergence UI.

There are two configuration options which can be configured using **iwcadmin** command:

- client.enableAttachmentRestriction: This parameter can be set to true/false to enable or disable this feature. By default, this feature is disabled.
- client.restrictedExtensionTypes: This parameter can be used to set the attachment types that have to be restricted.

The following are the steps to enable attachment restrictions:

1. Set `client.enableMailAttachmentRestriction` to true using the **IWCAdmin** CLI:

   ```
   ./iwcadmin -o client.enableAttachmentRestriction -v true.
   ```

2. Check the value of `client.restrictedExtensionTypes` to verify the attachment types to be restricted are part of the list.
   If its not part of the existing list, update the parameter to include the attachment type.
3. Edit `<data-directory>/WEB-INF/web.xml` and uncomment the **MailAttachmentFilter** related entries, servlet filter and filter-mapping.
4. Navigate to the installed directory and redeploy convergence in the Application server:

   ```
   $ cd /opt/sun/comms/iwc/sbin
   $ ./config-weblogic deploy /tmp/wlspass
   ```

   where **/tmp/wlspass** file contains the Weblogic admin password.
5. Restart the application server.

Restricting Number of Emails that can be sent to Recipients in a Defined Time Period

Convergence offers a way to limit the number of emails end users can send through Convergence during a given time period (3.0.3.4.0 onwards). The recipient list can include email aliases, in which case will be treated as a single recipient. For example, Convergence can restrict the number of mails sent by a single user to 20 recipients during a time period of 5 minutes. To enable this, follow these steps:

1. Edit **<data-directory>/WEB-INF/web.xml** file and and uncomment the **RateLimitFilter** entries, servlet filter and filter-mapping.
2. Go to installed directory and re-deploy Convergence in the application server:

   ```
   $ cd /opt/sun/comms/iwc/sbin
   $ ./config-weblogic deploy /tmp/wlspass
   ```

   - Where **/tmp/wlspass** file contains the Weblogic admin password.

Enabling Anti-Spam

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 to Combat Spam

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.

  ```
  iwcadmin -o mail.spam.enableaction  -v true
  ```

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

  ```
  iwcadmin -o mail.spam.folder -v SpamFolder
  ```

You must restart the Oracle WebLogic server after making the configuration changes.

When you set the parameters, the following spam related functionality is enabled 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 to Combat Spam

A more effective way to counter spam messages is to deploy a spam filer 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 the Messaging Server documentation.

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.

Disabling Rich Text Formatting

You can disable rich text formatting in Convergence. When rich text formatting is disabled, email messages are sent in plain text.

To disable rich text formatting, set the **client.enablertfcompose** configuration property to **false**. By default, this parameter is set to **true**. For example:

```
iwcadmin -o client.enablertfcompose -v false
```

Enabling Sound Alerts

Users can configure their Convergence to play a sound alert when they receive a new email message.

For enabling sound alerts, the following configuration change has to be done in Oracle Weblogic server:

1. Create a file titled **mimemappings.properties** under the <*Convergence_Domain*>/**config** folder and add **mp3=audio/mpeg**.

   OR

   Modify the <*Convergence_Domain*>/**servers/ManagedServer/tmp/_WL_user/<Convergence>/<value>/war/WEB-INF/web.xml** to add the following:

   ```
    <mime-mapping>
   <extension>mp3</extension>
   <mime-type>audio/mpeg</mime-type>
   </mime-mapping>
   ```

2. Restart Weblogic Managed Server.

6
Address Book Service Administration

This chapter describes how to administer the address book service in Oracle Communications Convergence provided by Convergence Server.

See "Enabling Core Services for Convergence" for information about enabling services.

The address book service can be also provided by Oracle Communications Contacts Server. See *Contacts Server System Administrator's Guide* for information about administering Contacts Server.

See *Convergence Installation and Configuration Guide* for information about configuring Convergence with Contacts Server.

Configuring Horizontal Scalability for the 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 are stored. The psRoot attribute is in the form `ldap://ldap_host:ldap_port/DN`. The value of psRoot attribute determines the DB type and DB location.

For 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 host name 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 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 **iwcadmin** command-line interface by setting the **ab.useuserpsroot** to **false**. If set to false, Convergence uses the Default Server value that is set in the Convergence configuration.

Set **ab.useuserpsroot** 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 example shows 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 default server, you must set the **ab.pstore.defaultserver** configuration parameter to the personal store identifier:

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

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

Configuring Address Book to Use Different Directory Server from the User Group 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 host name 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 bind dn 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:

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

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

If the configured directory server needs to act as the personal store's default server, then set the **ab.pstore.defaultserver** configuration parameter. For example:

```
iwcadmin -o ab.pstore.defaultserver -v psidentifier1
```

Configuring 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:

```
iwcadmin -o ab.corpdir.[identifier].ldaphost -v host.siroe.com
iwcadmin -o ab.corpdir.[identifier].ldapport -v 400
iwcadmin -o ab.corpdir.[identifier].ldapbinddn -v "cn=Directory Manager"
iwcadmin -o ab.corpdir.[identifier].ldapbindcred -v xyzxyz
```

Where *identifier* identifies the corporate directory configuration for **host.siroe.com**. For a single corporate directory configuration, you must use **default** as the identifier.

See "Setting Up Multiple Corporate Directories " for information about configuring and enabling multiple corporate directories.

Enabling Address Autocomplete for the Corporate Directory

To enable autocomplete 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.

Setting Up 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:

- **ab.{*identifier*}.psrootpattern**
- **ab.{*identifier*}.pstore.defaultserver**
- **ab.{*identifier*}.pstore.[domain].ldaphost**
- **ab.{*identifier*}.pstore.[*domain*].ldapport**
- **ab.{*identifier*}.pstore.[*domain*].ldapbinddn**
- **ab.{*identifier*}.pstore.[*domain*].ldapbindcred**

The following example shows the configuration parameter settings:

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

Where *domain.com* is the domain (within curly braces).

All the configuration data for the domain **domain.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 **domain.com**, type the following command:

```
iwcadmin -o ab.{domain.com}.pstore.lookthrulimit -v 2000.
```

To set up domain-based configuration for Corporate Directory:

1. Set the following configuration parameters:
   - **ab.{*identifier*}.corpdir.[*domain*].urlmatch**
   - **ab.{*identifier*}.corpdir.[*domain*].searchattr**
   - **ab.{*identifier*}.corpdir.[*domain*].lookthrulimit**
   - **ab.{*identifier*}.corpdir.[*domain*].ldaphost**
   - **ab.{*identifier*}.corpdir.[*domain*].ldapport**
   - **ab.{*identifier*}.corpdir.[*domain*].ldapbinddn**
   - **ab.{*identifier*}.corpdir.[*domain*].ldapbindcred**

   For example:

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

   Where *domain.com* specifies the domain. All the configuration data for the domain **domain.com** is grouped in to one logical set identified by using identifier **corpdomainid1**.

   > **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.

2. Copy **dictionary-*locale*.xml** (for example: **dictionary-en.xml**) from *Convergence_Home*/**config/templates/ab/domain/defaultps** to *Convergence_Home*/**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.

Disabling 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 "Setting Up Domain-Based Configuration for Address Book".
2. Disable the Corporate Directory for the specific domain:

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

3. Restart the Oracle WebLogic server.

> **Note:**
>
> You can ignore errors or exceptions in the log files.

Changing the Default Corporate Directory Search Filter in Address Book

To change the default corporate directory search filter, set the **ab.corpdir.[*identifier*].searchfilter** configuration parameter with the search criteria you want to base your corporate directory searches on.

The following example shows 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=GROUPOFUNIQUENAMES)(objectClass=GROUPOFURLS) \\
(objectClass=ICSCALENDARRESOURCE)(objectClass=INETORGPERSON)))(objectClass=*))'
```

Where **[filter]** is replaced with the search generated by the **ab.corpdir.[*identifier*].searchattr** configuration option.

The 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=GROUPOFUNIQUENAMES)
(objectClass=GROUPOFURLS)
(objectClass=ICSCALENDARRESOURCE)(objectClass=INETORGPERSON)))(objectClass=*))"
attrs="objectClass createTimestamp cn uid description mail multiLineDescription
modifyTimestamp"
```

Configuring Virtual List View for Convergence Corporate Directory

Follow these steps to configure Convergence to make use of virtual list view (VLV):

1. Configure Directory Server with VLV. For more information on creating and managing browsing indexes in Directory Server:

- See Configuring VLV Browsing Indexes for Directory Server.
- See Configuring VLV Indexes in *Oracle Fusion Middleware Administrator's Guide for Oracle Unified Directory*.

> **Note:**
>
> The following steps are applicable only if the Convergence Deployment is using the Convergence Address Book. When Contact Server is used as Address book service, the settings have to be changed in Contact Server. When Contact Server is configured in VLV mode, then all searches (for example, people, group, resources) use VLV.

2. Set the VLV filter and scope in the corporate directory.

```
iwcadmin -o ab.corpdir.[default].vlvfilter -v  "(&(&(objectclass=inetorgperson)
(mail=*)(cn=*)(!(psIncludeInGAB=false)))(objectClass=*))"
iwcadmin -o ab.corpdir.[default].vlvscope -v 2
iwcadmin -o ab.corpdir.[default].vlvsearchbase -v "o=example.com,o=usergroup"
iwcadmin -o ab.corpdir.[default].vlvsortby -v "entry/displayname"
```

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

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

About Supported vCard Standards

Convergence supports the following vCard standards:

- vCard 2.1
- vCard 3.0

Convergence supports the following encoding formats for importing and exporting vCard:

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

Changing the Locale Character Set for Importing or Exporting vCard Entries

Convergence supports the following locales by default:

- 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.

Table 6-1 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.

Table 6-1 Supported Default vCard Locales

Locale	Encoding	Import Parameter	Export Parameter
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.

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.

Enabling Contact Export and Import with Photo in vCard

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:

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

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

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

Hiding Administrator Accounts in the Default Domain Corporate Directory

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. For example:

```
iwcadmin -o ab.corpdir.[default].searchfilter  -v
'(&([filter])(!(psIncludeInGAB=false)))'
```

About Personal Address Book Contacts Deleted by the End User

If a contact has been deleted by the end user, Convergence determines what do to 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 appears in Convergence 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.

Enhancing Corporate Directory Search Using VLV Indexing

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.

Creating the VLV Index in the Directory Server

To enable VLV indexes in the directory server, you must set the following parameters:

- *base DN*
- *filter*
- *sort order*
- *scope of the index*

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. For more information, see Indexing Directory Data and Managing Directory Data in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

Generating Indexes

Generate the indexes for the settings to take effect. Perform the following steps during a scheduled change window to restart Directory Server.

Follow these steps to create VLV indexing in OUD. For more information, see Creating a New VLV Index in *Oracle Fusion Middleware Administering Oracle Unified Directory*.

1. Change the directory to the Directory Server Instance location. For example,

   ```
   cd /opt/oracle/Oracle/Middleware/asinst_1/bin
   ```

2. Use `dsconfig` to create a new VLV index:

   ```
   dsconfig -h ldap_host -p ldap_adminport -D "cn=directory manager" -j pwd-
   file -n \
     create-local-db-vlv-index \
     --element-name backend --index-name name --set sort-order:attributes \
   --set scope:scope --set base-dn:baseDN --set filter:filter
   ```

   where:

   - `index-name` specifies a unique index name, which cannot be altered after the VLV index is created.
   - `sort-order` specifies the names of the attributes by which the entries are sorted and their order of precedence, from highest to lowest.
   - `scope` specifies the LDAP scope of the query being indexed and can be one of base-object, single-level, subordinate-subtree, or whole-subtree.
   - `base-dn` specifies the base DN used in the search query being indexed.
   - `filter` specifies the LDAP filter used in the query being indexed and can be any valid LDAP filter.

Note:

To know the value for element name, use the command:

```
./dsconfig -h ldap_host -p ldap_adminport -D "cn=Directory
Manager" -j pwd-file -X -n list-workflow-elements
```

For example,

```
./dsconfig -h ldap_host -p 4444 -D "cn=Directory Manager" -j
<pwd_file_location>  -X -n list-workflow-elements
Workflow Element    : Type               : enabled
--------------------:--------------------:--------
adminRoot           : ldif-local-backend : true
userRoot            : db-local-backend   : true
virtualAcis         : db-local-backend   : true
we-ucs-comms-config : db-local-backend   : true
we-ucs-mlusers      : db-local-backend   : true
we-ucs-PiServerDb   : db-local-backend   : true


./dsconfig -D "cn=directory manager" -j <pwd_file_location> -n
create-local-db-vlv-index --element-name userRoot
 --index-name vlvtest --set sort-order:"cn" --set scope:whole-
subtree --set base-dn:o=usergroup
--set filter:"(&(mail=*)(cn=*))"
```

3. Check the index was created by listing the existing VLV indexes:

```
dsconfig -h ldap_host -p ldap_adminport -D "cn=directory manager" -j pwd-
file -n \
  list-local-db-vlv-indexes \
  --element-name backend
```

For example,

```
./dsconfig -h ldap_hostname -p 4444 -D "cn=Directory Manager" -j /tmp/
ds_pass -X -n list-local-db-vlv-indexes --element-name userRoot
Local DB VLV Index : Type    : base-dn : scope         :
filter            : sort-order
------------------:---------:---------:--------------:------------------
:-----------
vlvtest            : generic : o=dav   : whole-subtree : (&(mail=*)
(cn=*)) : cn
```

4. . Display the index properties to verify your changes:

```
dsconfig -h ldap_host -p ldap_adminport -D "cn=directory manager" -j pwd-
file -n \
  get-local-db-vlv-index-prop \
  --element-name backend --index-name name
```

For example,

```
./dsconfig -h ldap_host  -p 4444 -D "cn=directory manager" -j /tmp/ds_pass
-n get-local-db-vlv-index-prop --element-name userRoot  --index-name
vlvtest
Property   : Value(s)
base-dn    : o=dav
filter     : (&(mail=*)(cn=*))
name       : vlvtest
scope      : whole-subtree
sort-order : cn
```

5. Rebuild the index. You can either stop the server, rebuild the index, and restart the server:

```
stop-ds
$ rebuild-index --baseDN baseDN --index vlv.name
start-ds
```

Or, rebuild the index online by running the **rebuild-index** command as a task:

```
rebuild-index -h localhost -p 4444 -D "cn=Directory manager" -j pwd-file -
X \
  --baseDN baseDN --index vlv.name
```

The following is a sample VLV search using ldapsearch command:

```
./ldapsearch -p 1389 -D "cn=Directory Manager" -w  ldap_password -b
o=usergroup --searchScope sub --sortOrder cn --virtualListView "0:0:0:0"
"(objectclass=*)"
```

Configuring Convergence

> **Note:**
>
> The following steps are applicable only if the Convergence Deployment is using the Convergence Address Book. When Contact Server is used as Address book service, the VLV settings should be changed in the Contact Server.

You need to configure Convergence to use the indexes after generating the indexes for Directory Server. Using the **iwcadmin** command, set the following Convergence parameters:

- **ab.corpdir.[default].vlvfilter**
- **ab.corpdir.[default].vlvscope**
- **ab.corpdir.[default].vlvpaging**
- **ab.corpdir.[default].vlvsortby**
- **ab.corpdir.[default].vlvsearchbase**
- **ab.corpdir.[default].vlvsortby**

For example:

```
iwcadmin -u admin_user_id -o ab.corpdir.[default].vlvfilter -v "(&(mail=*)(cn=*))"
iwcadmin -o ab.corpdir.[default].vlvscope -v 2
iwcadmin -o ab.corpdir.[default].vlvpaging -v true
iwcadmin -o ab.corpdir.[default].vlvsortby -v "entry/displayname,person/
surname,email,person/givenname"
iwcadmin -o ab.corpdir.[default].vlvsearchbase -v "o=isp"
```

The value for **ab.corpdir.[default].vlvfilter** 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.

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.[domain].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.

> **Note:**
>
> Convergence can be configured to enable address book service using both Convergence (WABP) and Contacts (NAB) servers and it is called co-existence mode. In this mode of configuration some users may be using WABP and others might have been migrated to NAB. You need to set the **nab.nabuserattr** parameter to an LDAP attribute used in the user entry to indicate that the user has been migrated to NAB. The default value of this attribute is **nabStore** (defined as part of **nabUser** ObjectClass). If this attribute is not present in user LDAP entry then it indicates that you are a WABP user and not a NAB user.
>
> ```
> iwcadmin -o nab.nabuserattr -v user_attribute
> ```
>
> See "Convergence Properties Reference " for information on **nab.nabuserattr**.

Verifying the VLV Settings

To verify 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

Convergence only supports *cn*.

2. Log in to Convergence and type a search command in the corporate directory to check corresponding log files. Two cases with corresponding log files 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
```

Performing a VLV search using ldapsearch command (with syntax explained)

```
$ ./ldapsearch -p 1389 -D "cn=Directory Manager" -w  <password> -b
o=usergroup --searchScope sub --sortOrder cn
--virtualListView "0:0:0:0" "(objectclass=*)"--virtualListView
'beforeCount:afterCount:offset:contentCount'
```

where:

- **offset** specifies the index of the target entry.
- **contentCount** specifies the estimated total number of results (or zero if it is not known), or `beforeCount:afterCount:assertionValue` (where the entry should be the first entry whose primary sort value is greater than or equal to the provided **assertionValue**). In either case, **beforeCount** is the number of entries to return before the target value and **afterCount** is the number of entries to return after the target value.

```
./ldapsearch -h ldap_host -p ldap_port -D "cn=directory manager" -j /tmp/
ds_pass -b o=example.com,o=usergroup -S cn -G "0:1:cal"
'(&(&(objectclass=inetorgperson)(mail=*)(cn=*)(!(psIncludeInGAB=false)))
(objectClass=*))' debugsearchindex
dn: cn=debugsearch
debugsearchindex: vlv=[INDEX:vlv.vlv_in_sun_com_cn][COUNT:4] final=[COUNT:2]

# VLV Target Offset:  4
# VLV Content Count:  1740
```

```
#./ldapsearch -p 1389 -D "cn=Directory Manager" -j /tmp/ds_pass  -b
o=usergroup --searchScope sub --sortOrder cn --virtualListView "0:0:0:0"
"(objectclass=*)"
dn: cn=andromeda,ou=People,o=example.com,o=usergroup
davUniqueId: dd9ca981-a45611e1-8093d2ed-c263972e
mail: andromeda@example.com
cn: andromeda
objectClass: icsCalendarResource
objectClass: daventity
objectClass: top
objectClass: inetResource
uid: andromeda
icsCalendar: andromeda@example.com,o=example.com,o=usergroup
```

```
# VLV Target Offset:  1
# VLV Content Count:  2094
```

The example below uses the Virtual List View Control options to specify the following:

- **Before = 0** specifies that 0 entries before the target should be displayed.
- **After = 2** specifies that 2 entries after the target should be displayed.
- **Index=1** specifies that the offset of the target entry within the result set should be returned.
- **Count=0** specifies that target entry at the index position should be returned, which is the first entry.

Thus, the server returns the first entry plus two entries after the target sorted in ascending order by the **givenName** attribute.

```
./ldapsearch -p 1389 -D "cn=Directory Manager" -j /tmp/ds_pass -b o=usergroup
--searchScope sub --sortOrder cn --virtualListView "0:2:1:0"
"(objectclass=*)" cn
dn: cn=andromeda,ou=People,o=example.com,o=usergroup
cn: andromeda

dn: uid=anilsri,ou=People,o=example.com,o=usergroup
cn: anilsri

dn: cn=applgroup,ou=Groups,o=example.com,o=usergroup
cn: dav-interest
cn: applgroup

# VLV Target Offset:  1
# VLV Content Count:  2094
```

When Convergence uses Contact Server as Address book

1. Make the Contact Server log level to FINEST.

   ```
   /opt/sun/comms/nabserver/sbin/davadmin config modify -o
   log.dav.errors.loglevel  -v FINEST
   /opt/sun/comms/nabserver/sbin/davadmin config modify -u admin -o
   store.corpdir.defaultcorpdirectoryurl -v "ldap://ugldap/??sub?(&(mail=*)
   (cn=*))?vlv"
   /opt/sun/comms/nabserver/sbin/davadmin config modify -u admin -o
   store.corpdir.enablecorpdir -v true
   ```

2. Restart the Contact Server.
   You can verify the VLV indexing by searching for an entry in the corporate address book from IWC. The following logs are verified in Contact Server error log file while searching the user in corporate address book.

Logs from commands.0 file

```
FINER   [2023-02-27T14:19:13.141+0000]
<...AclChecker.checkAllPrivilegesRecur> no more privileges to process - grant
FINE    [2023-02-27T14:19:13.141+0000]
<...CorpDirectoryManager.searchSubNodes> VLV Lookup - Total Matching 1,373
Index Position 0
```

```
FINE    [2023-02-27T14:19:13.142+0000] <...BaseOperation.postprocess> -----
Search end. Processing time=0.323 secs.
NbEvaluatedNodes=101,NbMatchingNodes=100
```

Logs from errors.0 file

```
FINER   [2023-02-28T09:41:30.708+0000] <...AclChecker.checkAllPrivileges>
Checking [READ] against /davserver/rest/directory/default/
uid%3Dcaltest1084%2Cou%3DPeople%2Co%3Dsun.com%2Co%3Ddav for subject
u:c4df2182-422a11dd-8002d2ed-c263972er2@sun.com:otherownercal$estroom5@sun.com
FINER   [2023-02-28T09:41:30.708+0000]
<...AclChecker.checkAllPrivilegesRecur> Acl for /davserver/rest/directory/
default/uid%3Dcaltest1084%2Cou%3DPeople%2Co%3Dsun.com%2Co%3Ddav:
V1;g^p:authenticated^r
FINER   [2023-02-28T09:41:30.708+0000]
<...AclChecker.checkAllPrivilegesRecur> Privilege READ granted by
g^p:authenticated^r
FINER   [2023-02-28T09:41:30.708+0000]
<...AclChecker.checkAllPrivilegesRecur> no more privileges to process - grant
FINER   [2023-02-28T09:41:30.709+0000] <...AclChecker.checkAllPrivileges>
Checking [READ] against /davserver/rest/directory/default/
uid%3Dcaltest1085%2Cou%3DPeople%2Co%3Dsun.com%2Co%3Ddav for subject
u:c4df2182-422a11dd-8002d2ed-c263972er2@sun.com:otherownercal$estroom5@sun.com
FINER   [2023-02-28T09:41:30.709+0000]
<...AclChecker.checkAllPrivilegesRecur> Acl for /davserver/rest/directory/
default/uid%3Dcaltest1085%2Cou%3DPeople%2Co%3Dsun.com%2Co%3Ddav:
V1;g^p:authenticated^r
FINER   [2023-02-28T09:41:30.709+0000]
<...AclChecker.checkAllPrivilegesRecur> Privilege READ granted by
g^p:authenticated^r
FINER   [2023-02-28T09:41:30.709+0000]
<...AclChecker.checkAllPrivilegesRecur> no more privileges to process - grant
FINER   [2023-02-28T09:41:30.709+0000] <...AclChecker.checkAllPrivileges>
Checking [READ] against /davserver/rest/directory/default/
uid%3Dcaltest1086%2Cou%3DPeople%2Co%3Dsun.com%2Co%3Ddav for subject
u:c4df2182-422a11dd-8002d2ed-c263972er2@sun.com:otherownercal$estroom5@sun.com
FINER   [2023-02-28T09:41:30.709+0000]
<...AclChecker.checkAllPrivilegesRecur> Acl for /davserver/rest/directory/
default/uid%3Dcaltest1086%2Cou%3DPeople%2Co%3Dsun.com%2Co%3Ddav:
V1;g^p:authenticated^r
FINER   [2023-02-28T09:41:30.709+0000]
<...AclChecker.checkAllPrivilegesRecur> Privilege READ granted by
g^p:authenticated^r
FINER   [2023-02-28T09:41:30.709+0000]
<...AclChecker.checkAllPrivilegesRecur> no more privileges to process - grant
FINE    [2023-02-28T09:41:30.710+0000]
<...CorpDirectoryManager.searchSubNodes> VLV Lookup - Total Matching 1,433
Index Position 0
FINE    [2023-02-28T09:41:30.711+0000] <...BaseOperation.postprocess> -----
Search end. Processing time=0.18 secs.
NbEvaluatedNodes=101,NbMatchingNodes=100
FINE    [2023-02-28T09:41:30.711+0000] <...DavServerServlet.service> [RES]
[200]    Command execution time: 0.184 secs
FINE    [2023-02-28T09:45:53.998+0000] <...LDAPSingleHostPool.getConnection>
got connection from getConnection() for pool Pool number:0. Host=cHostname
```

Logs when Convergence is using the default Convergence Address Book

```
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.wabp.cmd.SearchEntryHandler
Thread [ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,303 - Processing command: search_entry.wabp
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.wabp.cmd.SearchEntryHandler
Thread [ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,305 - Searching with: bookid:
e146978b7be21300 filter: entry/displayname=caluser* sortby: +entry/displayname
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.wabp.cmd.SearchEntryHandler
Thread [ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,305 - Searching with entries per page: 100
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.coresrv.CorePersonalStore
Thread [ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,305 - psearchBook:
bookEntryID=e146978b7be21300, filter=entry/displayname=caluser*,
sortBy=+entry/displayname, entryType=[abperson],entriesPerPage=100
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.coresrv.DBHandler  Thread
[ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,305 - Match found: ldap://corpdirectory
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.ldapplug.iLdapDb  Thread
[ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,306 - Performing VLV search:true
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.coresrv.CorePersonalStore
Thread [ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,306 - psearchBook: new searchID=1
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.coresrv.CorePersonalStore
Thread [ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,364 - getResult: searchID=1firstentry=1
ADDRESS_BOOK: DEBUG from com.sun.comms.client.ab.ldapplug.iLdapSearch  Thread
[ACTIVE] ExecuteThread: '12' for queue: 'weblogic.kernel.Default (self-
tuning)' at 2023-02-28 05:49:42,365 - LDAPSearchConstraints {LDAPConstraints
{time limit 0, referrals true, hop limit 5, bind_proc null, rebind_proc
com.sun.comms.shared.ldap.LDAPRebindImpl@5f9e800c, server controls {SortCtrl:
isCritical=true {SortKey: key=cn reverse=false}} {VirtListCtrl:
isCritical=true beforeCount=0 afterCount=99 listIndex=-1 listSize=0}} size
limit 3000, server time limit 0, aliases 0, batch size 1, max backlog 100,
referralErrors 0}
```

7
Calendar Service Administration

This chapter describes how to administer the calendar service in Oracle Communications Convergence.

See "Enabling Core Services for Convergence" for information about enabling services.

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 Calendar service.

     ```
     iwcadmin -o caldav.enable -v true
     ```

   - **caldav.host** - Set this parameter to the host name on which the CalDAV server is installed.

     ```
     iwcadmin -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 Oracle WebLogic server Configuration Details panel during the Calendar Server Initial Configuration.

     ```
     iwcadmin -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 or later Initial Configuration.

     ```
     iwcadmin -o caldav.proxyadminid -v proxy_admin_id
     ```

   - **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 Initial Configuration.

     ```
     iwcadmin -o caldav.proxyadminpwd -v proxy_admin_pwd
     ```

   - **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 is deployed and should be suffixed with /wcap. For example, if the URI path where Calendar Server is deployed is /caldav, then this parameter should be set to /caldav/wcap.

     ```
     iwcadmin -o caldav.serviceuri -v service_uri
     ```

> **Note:**
>
> Make sure that the CALDAV users have the LDAP attribute **davUniqueId** defined as part of **davEntity** object class.
>
> For more information on **davUniqueId** LDAP attribute, see the discussion about *Provisioning Calendar Server Users* in your Calendar Server documentation for more information.

2. Restart the Oracle WebLogic server.

Enabling SMS Calendar Notifications in Convergence

You can configure Convergence to send you SMS notifications of your calendar events.

When a user sets up calendar event reminder SMS notifications in the Convergence UI, Calendar Server generates the notifications as specially formatted messages with SMS addresses as recipients; they are then submitted to Messaging Server for processing. Within Messaging Server, the SMS channel processes the notification messages. The messages are submitted to an SMSC provider (through an SMPP protocol) to be delivered as SMS messages to SMS addresses.

SMS addresses, which are added by end users to the Convergence UI, should be of the form **+***subscriber_number*@**sms.***your_domain*, where subscriber_number is usually a phone number where a user expects to receive SMS notifications. The format of each subscriber_number is specific to the SMSC provider. For example, some providers might require an international format with the country code. The portion @**sms.***your_domain* represents a site-specific domain name and is the same name that is used in the Messaging Server's SMS channel configuration.

To enable SMS calendar notifications in Convergence:

1. Set up and configure an SMS channel in Messaging Server. See *Messaging Server System Administrator's Guide* for more information.
2. Enable SMS notifications for calendar events in Convergence server:

```
iwcadmin -o user.cal.enablesmsnotify -v true
```

Convergence users can now enable SMS calendar notifications in Convergence in the Convergence **Options** tab.

Hiding or Showing the SMS Option in the Notifications Tab in Calendar Options and in the Reminder Dialog Box

Convergence enables you to hide or show the SMS option in the **Notifications** tab in Calendar Options and in the **Reminder** dialog box. To do so, set the **client.enablesmsnotification** configuration property to **false** or **true**. By default, this parameter is set to **true**. For example:

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

If the parameter is set to **false**, the SMS notification option will be hidden in the **Notifications** tab in Calendar Options and in the **Reminder** dialog box.

Reserving Calendar Resources

To reserve resources for a calendar event, place yourself on the **New Event** Page for an event you are creating or editing and do one of the following:

- In the **Reservations** field, enter the name or email address of one or more resources. The resource's email address is displayed in a list as you type, select the address from the list.
- Next to the **Reservations** field, click the address book icon, the **Add Resources** dialog box is displayed. This dialog box lists all the resources created in the corporate directory. See "Creating a Calendar Resource in Corporate Directory" for more information.

  You can list or search the resources based on the resource type, that is, Rooms or Equipment. By default, **Rooms** option is selected as a resource type. The **Add Resources** dialog box displays the following details about the resource:

  - **Type**
  - **Display Name**
  - **Email Address**
  - **Address**
  - **Phone Number**
  - **Capacity**

> **Note:**
>
> Convergence provides an option to list or search the resources based on the resource type in three pane layout for Contacts Server users.
>
> In two pane layout, the **Add Resources** dialog box lists **Display Name** and **Email Address** only.

Creating a Calendar Resource in Corporate Directory

You can create calendar resources in corporate directory by specifying the required attributes in the LDIF file. You must set the following LDAP attributes in the LDIF file for creating the resource by specifying the resource type:

- inetResourceType
- floor
- building
- ucapsCountryCode
- inetResourceCapacity
- telephoneNumber

> **Note:**
>
> All these attributes are part of **inetResource** object class.

The following is a code sample of the **ldif** file:

```
DN: cn= CalResourcesOne ,ou=People,o=calResourceone@aplsorgone.com,o=isp
objectClass: top
objectClass: inetresource
objectClass: icscalendarresource
objectClass: daventity
cn: Meeting
description: Conference Room
davUniqueId: bfeaea46-38bd-48ff-bb72-9d58da573527
icsStatus: active
inetResourceStatus: active
mail: calResourceone@aplsorgone.com
inetResourceType: Room
floor: 3rd
building: Kalyani Magnum
l: Bangalore
ucapsCountryCode: IN
inetResourceCapacity: 10
telephoneNumber: 4445555666
```

Viewing Event Invitation and Task Details in Anonymous Calendar in Convergence

To view event invitation and task details in anonymous calendar in Convergence, the **davcore.acl.calendaranonymousall** and **davcore.acl.schedulinganonymousall** parameters should be set to **true** as follows:

```
davcore.acl.calendaranonymousall=true
davcore.acl.schedulinganonymousall=true
```

In Calendar Server 8.0.0.1.x, the default value for the above parameters was changed to **false**. When Convergence is used with Calendar Server 8.0.0.1.x and above, set these parameters to **true** and restart the Oracle WebLogic server in which Calendar Server is deployed.

In addition to this, the following command can be used to correct the behavior for existing calendar user accounts:

```
CalendarServer_home/sadmin/davadmin account repair -a account -l
```

Where, *CalendarServer_home* specifies the installation location for the Calendar Server software and *account* specifies the user's account. For example,

```
/opt/sun/comms/davserver/sbin/davadmin  account repair -a user -l
```

For more information on the **davadmin** command usage, see your Calendar Server documentation.

See the discussion about Administering Calendar Server Access in your Oracle Communications Calendar Server documentation for more information on the parameters.

See the instructions for viewing anonymous calendar in Convergence in Convergence Online Help.

8
Contacts Server Administration

This chapter describes how to administer the Contacts Server Address Book service in Oracle Communications Convergence.

See "Enabling Core Services for Convergence" for information about enabling services.

Enabling Contacts Server Service

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

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

1. Enable the following Contacts Server related parameters in Convergence:
   - **nab.enable** - Set this parameter to **true** to enable the Contacts Server service.

     ```
     iwcadmin -o nab.enable -v true
     ```
   - **nab.host** - Set this parameter to the host name on which the Contacts Server is installed.

     ```
     iwcadmin -o nab.host -v siroe.com
     ```
   - **nab.port** - Set this parameter to the web component port number on which Contacts Server is deployed. This should be same as the port number specified for **Server Instance HTTP Port** in the Application Server (WebLogic Managed Server) Configuration Details panel during the Contacts Server Initial Configuration.

     ```
     iwcadmin -o nab.port -v port_number
     ```
   - **nab.proxyadminid** - Set this parameter to the proxy admin id on which Contacts Server is deployed. This should be same as the Administrator User Id specified during Contacts Server Initial Configuration.

     ```
     iwcadmin -o nab.proxyadminid -v proxy_admin_id
     ```
   - **nab.proxyadminpwd** - Set this parameter to the proxy admin password on which Contacts Server is deployed. This should be same as the Administrator password specified during Contacts Server Initial Configuration.

     ```
     iwcadmin -o nab.proxyadminpwd -v proxy_admin_pwd
     ```
   - **nab.serviceuri** - Set this parameter to the serviceuri on which Contacts Server is deployed. This should be same as the URI Path where the Contacts Server is deployed.

     ```
     iwcadmin -o nab.serviceuri -v service_uri
     ```

> **Note:**
>
> Make sure that the Contacts Server users have the LDAP attribute **davUniqueId** defined as part of **davEntity** object class.
>
> For more information on **davUniqueId** LDAP attribute, see the discussion about *Provisioning Contacts Server Users* in your Contacts Server documentation for more information.

2. Restart Oracle WebLogic server.

9

Configuring Convergence to Use Proxy Authentication

This chapter 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 user name and password of the privileged user requesting the authentication is sent with the user name of the user requesting the authentication.

The parameters include:

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

The protocol request must pass these parameters for performing authentication.

Configuring Convergence for Proxy Authentication

For proxy authentication to work, the privileged user (the Proxy Admin user) must be provisioned for the domain. A user is considered a proxy administration user if the LDAP entry has **isMemberOf** operational attribute, whose value is set to the DN of **Service Administrators**. The administration 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 administration user are provisioned when the administrators for Oracle Communications Messaging Server (**admin**) and Oracle Communications Calendar Server (**calmaster**) are configured. This 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:

```
iwcadmin -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&password=password_privileged_user&proxyauth=username&fm
t-out=text/json
```

Where the values for:

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

10

Convergence Properties Reference

This chapter lists all the configuration parameters that are available in Oracle Communications Convergence. Each parameter is described with its name and a description of its purpose. Use the **iwcadmin** command-line utility to update the configuration properties for your deployment. See "Using the Convergence Administration Utility" for more information.

Global Convergence Configuration Properties

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.

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 parameter_name
```

In the following configuration properties tables, the command-line option name found in the left column is the parameter you use after *-o* option in the **iwcadmin** command. 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.

The following tables list the Convergence Server global configuration properties:

- Table 10-1 Deployment-Level Global Configuration Properties
- Table 10-2 LDAP User and Group Configuration Properties
- Table 10-3 Authentication Configuration Properties
- Table 10-4 Mail Service Configuration Properties
- Table 10-5 Logging Configuration Properties
- Table 10-6 Calendar Service Configuration Properties for Calendar Server 7 and Calendar Server 8
- Table 10-7 Address Book Service Configuration Properties for Contacts Server
- Table 10-8 Address Book Service Configuration Properties for Convergence WABP
- Table 10-9 Deployment or Domain Specific Configuration Properties
- Table 10-10 Administration Service Configuration Properties
- Table 10-11 Single Sign-On Configuration Properties

- Table 10-12 User Preferences Configuration Properties
- Table 10-13 Event Notification System Configuration Properties
- Table 10-14 Address Book Service JMQ Notification Configuration Properties
- Table 10-15 Outside In Proxy Configuration Properties

Table 10-1 Deployment-Level Global Configuration Properties

Option Name	Description
base.defaultdomain	Default domain to use for user resolution • Allowed Pattern/Values: [A-Za-z0-9\-]+(\.[A-Za-z0-9\-]+)+ • Data Type: String
base.loginseparator	Character to be used as login separator (between user ID and domain). It should match any one of the character defined in service.loginseparator of mail and calendar back end service • Allowed Pattern/Values: a character • Data Type: String • Default value: @
base.defaultlocale	Default locale to be used • Default value: en_us • 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. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
base.enablehosteddomain	Whether hosted domains is enabled • Data Type: Boolean • Allowed Pattern/Values: true or false • Default value: true
base.port	Port number at which the application listens • Default value: 8080 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
base.sslport	SSL Port number at which the application listens • Default value: 8181 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
base.enableauthonlyssl	SSL can be used only for authentication and the subsequent access via non-ssl • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
base.ipaccessurl	The access URL for this application. The URL must use IP address instead of host name. • 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	IP address along with the token is used for authorization if set to true • Allowed Pattern/Values: true or false • Default value: false • Data Type: Boolean

Table 10-1 (Cont.) Deployment-Level Global Configuration Properties

Option Name	Description
base.ignoreurldomain	Prevents the use of the URL domain. • Default value: false • Data Type: Boolean • Allowed Pattern/Value: true or false
base.authcookiepath	Cookie path for authorization cookie. • Default value: / • Data Type: String
base.enablealwayssl	Whether calls to HTTP protocol are redirected to HTTPS protocol. • Default value: true • Data Type: Boolean • Allowed Pattern/Value: true or false
base.hstsmaxage	The number of seconds, after receiving a request with STS header, that the host is considered as a Known HSTS Host. A value of 0 indicates that HSTS is not enforced. • Default value: 0 • Allowed Pattern/Values: 0 or higher integer • Data Type: Integer
base.defaulthost	Default host name configured to redirect, in case, the requested host in the URL is invalid. The URL specifies the location where the Convergence is deployed on an Application Server. (example: http://localhost:8080/) • Default value: null • Allowed Pattern/Values: [A-Za-z0-9\\-]+(\\.[A-Za-z0-9\\-]+)* • Data Type: String
base.whitelistedhosts	Comma-separated list of allowed hosted domains • Default value: null • Allowed Pattern/Values: *.*domain*.com where, *domain* is the name of domain. (example: *.abc.com,*.xyz.com) • Data Type: String
base.googlemapapikey	The Google map API key is used to access the Google maps service in the Convergence address book. The Google map API key is restricted to Javascript API, Geocoding API, and Directions API. See the Google Maps Platform documentation for more information: https://developers.google.com/places/web-service/get-api-key. • Data type: String • Default value: null
base.enableforgotpassword	By setting this property to true, user will be allowed to reset the forgot password. • Data Type: boolean • Allowed Pattern: true or false • Default Value: false
base.sessiontimeout	Enables session timeout for reset password in seconds. • Data Type: Integer • Allowed Pattern: Greater than or equal to 0 • Default Value: 240
base.sms.enable	Enables resetting password using multifactor authentication using SMS. • Data Type: boolean • Allowed Pattern: true or false • Default Value: true

Table 10-1 (Cont.) Deployment-Level Global Configuration Properties

Option Name	Description
base.sms.channel	Messaging server SMS channel name. • Data Type: String • Allowed Pattern: sms • Default Value: sms
base.sms.defaultLDAPAttribute	Default LDAP Attribute to be used to send SMS. • Data Type: String • Allowed Pattern: mobile or telephoneNumber • Default Value: mobile
base.sms.timeout	Enables specifying OTP expiry time in seconds. • Data Type: Integer • Allowed Pattern: Greater than or equal to 0 • Default Value: 180
base.mail.enable	Enables resetting password using multifactor authentication using Email. • Data Type: boolean • Allowed Pattern: true or false • Default Value: false
base.mail.timeout	Enables specifying OTP expiry time in seconds. • Data Type: Integer • Allowed Pattern: Greater than or equal to 0 • Default Value: 180
base.enablemultifactauth	By setting this property to true, multi factor authentication will be enabled for the user during login.One of the authentication mechanism like mobile authentication needs to be enabled.Multi factor authentication is enabled for all domains listed under ActivatedDomains list. • Data Type: boolean • Allowed Pattern: true or false • Default Value: false
base.oma.enable	Enables multifactor authentication using mobile authenticator. • Data Type: Boolean • Allowed Pattern: True or False • Default Value: True
base.oma.issuer	Issuer of time based one time password. If not set, the domain name is considered as the issuer. • Data Type: String
base.oma.timeout	Specifies OTP expiry time in seconds. • Data Type: Integer • Allowed Pattern: Greater than or equal to 0 • Default Value: 30

Table 10-2 LDAP User and Group Configuration Properties

Option Name	Description
ugldap.schemaversion	Schema level used by the deployment • Default value: 1 • Allowed Pattern/Values: 1 or 2 • Data Type: Integer

Table 10-2 (Cont.) LDAP User and Group Configuration Properties

Option Name	Description
ugldap.dcroot	Domain component root suffix • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String
ugldap.basedn	Base DN to start the user search from • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String
ugldap.ugfilter	User/group filter to apply while user lookup • Default value: (uid=%U%V) • Data Type: String
ugldap.domainfilter	Domain filter to apply while domain lookup • Default value: (&(objectClass=sunManagedOrganization)(|(sunPreferredDomain=%V)(associatedDomain=%V))) • Data Type: String
ugldap.srchopattrs	Comma-separated list of retrievable LDAP operational attributes • Default value: *,isMemberOf • Data Type: String
ugldap.host	Host name of the LDAP service • 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	Port number at which LDAP service listens • Default value: 389 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
ugldap.enablessl	Whether LDAP is SSL enabled • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
ugldap.enabledsslprotocols	A list of the SSL protocols that will be used to decide which protocol to use while connecting to LDAP server over SSL connection. The first in the list will be considered first and so forth. If none of the listed protocol is supported by the back end server the connection to back end server will be rejected. • Default value: TLSv1.2,TLSv1.1,TLSv1 • Data Type: string • Allowed Pattern/Values: A comma separated list of SSL protocols. Ex: TLSv1.2,TLSv1.1. Please refer Java Secure Socket Extension (JSSE) Reference Guide for the list of protocols that can be used in enabled protocols.
ugldap.minpool	Minimum number of connections in LDAP Pool • Default value: 1 • Allowed Pattern/Values: Greater than 0 and less than the max pool • Data Type: Integer

Table 10-2 (Cont.) LDAP User and Group Configuration Properties

Option Name	Description
ugldap.maxpool	Maximum number of connections in LDAP Pool • Default value: 30 • Allowed Pattern/Values: Greater than 0 and greater than the min pool • Data Type: Integer
ugldap.timeout	LDAP operation time out in seconds • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ugldap.refreshinterval	Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ugldap.monitoringinterval	Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down • Default value: 60 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ugldap.binddn	The admin DN used for creating LDAP connection pool • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String
ugldap.bindpwd	The admin DN password • Default Value: Not Applicable • Data Type: String

Table 10-3 Authentication Configuration Properties

Option Name	Description
auth.cert.enable	Enables and disables X509 Certificate-based authentication. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
auth.cert.enablefallback	Enables and disables fallback to form-based login. This option should be set in conjunction with auth.cert.enable. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
auth.ldap.enable	This creates default configuration parameters required to enable LDAP authentication mechanism. Specific parameters can further be modified/created using parameter-specific CLI option. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false

Table 10-3 (Cont.) Authentication Configuration Properties

Option Name	Description
auth.ldap.loginimpl	An implementation of LoginModule interface (JAAS technology in Java). This property refers to a pluggable custom authentication module • Default value: Not applicable • Data Type: String
auth.ldap.callbackhandler	An implementation of HttpCallbackHandler class, which extends CallBackHandler (JAAS technology in Java). This property refers to a pluggable custom authentication module • Default value: com.sun.comms.client.security.auth.AppCallbackHandler • Data Type: String
auth.ldap.enableproxyauth	Use this option to enable Proxy Authentication of the user. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
auth.ldap.schemaversion	The value of this should be same as ugldap. • Default value: 2 • Allowed Pattern/Values: 1 or 2 • Data Type: Integer
auth.ldap.dcroot	The value of this should be same as ugldap.dcroot • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String
auth.ldap.basedn	The value of this should be same as ugldap.basedn • Default value: Not Applicable • Allowed Pattern/Values: (.=.([,;+].))? • Data Type: String
auth.ldap.ugfilter	The value of this should be same as ugldap.ugfilter • Default value: (uid=%U%V) • Data Type: String
auth.ldap.domainfilter	The value of this should be same as ugldap.domainfilter • Default value: (&(objectClass=sunManagedOrganization)(|(sunPreferredDomain=%V)(associatedDomain=%V))) • Data Type: String
auth.ldap.host	Host name of the auth LDAP service • 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	Port number at which auth LDAP service listens • Default value: 389 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
auth.ldap.enablessl	Whether auth LDAP is SSL enabled • Default value: true • Allowed Pattern/Values: true or false • Data Type: Boolean

Table 10-3 (Cont.) Authentication Configuration Properties

Option Name	Description
auth.ldap.enabledsslprotocols	A list of SSL protocols that will be used to decide which protocol to use while connecting to LDAP server over SSL connection. The first in the list will be considered first and so forth. If none of the listed protocol is supported by back end server the connection to back end server will be rejected. • Default value: TLSv1.2,TLSv1.1,TLSv1 • Allowed Pattern/Values: A comma separated list of SSL protocols. Ex: TLSv1.2,TLSv1.1. Please refer Java Secure Socket Extension (JSSE) Reference Guide for the list of protocols that can be used in enabled protocols. • Data Type: String
auth.ldap.minpool	Minimum number of connections in LDAP Pool • Default value: 1 • Allowed Pattern/Values: Greater than 0 and less than max pool • Data Type: Integer
auth.ldap.maxpool	Maximum number of connections in LDAP Pool • Default value: 30 • Allowed Pattern/Values: Greater than 0 and greater than min pool • Data Type: Integer
auth.ldap.timeout	LDAP operation time out in seconds • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
auth.ldap.refreshinterval	Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
auth.ldap.monitoringinterval	Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down • Default value: 60 • Allowed Pattern/Values: Greater than or equal 1 • Data Type: Integer
auth.ldap.binddn	The admin DN used for creating LDAP connection pool • Default value: Not applicable • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String
auth.ldap.bindpwd	The admin DN password • Default value: Not Applicable • Data Type: String
auth.custom.servicename	Name of service for custom authentication module • Default value: Not Applicable • Data Type: String
auth.custom.loginimpl	An implementation of LoginModule interface (JAAS technology in Java). This property refers to a pluggable custom authentication module • Default value: Not Applicable • Data Type: String

Table 10-3 (Cont.) Authentication Configuration Properties

Option Name	Description
auth.custom.callbackhandler	An implementation of HttpCallbackHandler class, which extends CallBackHandler (JAAS technology in Java). This property refers to a pluggable custom authentication module • Default value: Not Applicable • Data Type: String
auth.misc	Placeholder for custom auth provider configuration • Allowed Pattern/Values: user-defined-attribute • Data Type: String
auth.adminuserlogin.enable	Whether proxy admins are allowed to login through web client • Default value: true • Data Type: Boolean

Table 10-4 Mail Service Configuration Properties

Option Name	Description
mail.enable	Whether mail service is enabled or not • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
mail.host	Host name of the back-end mail service • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-]+(\.[A-Za-z0-9\-]+)* • Data Type: String
mail.port	Port number at which back-end mail service listens • Default value: 8990 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
mail.enablessl	Whether mail service is SSL enabled • Default value: true • Allowed Pattern/Values: true or false • Data Type: Boolean
mail.enabledsslprotocols	A list of the SSL protocols that will be used to decide which protocol to use while connecting to Messaging Server over SSL connection. The first in the list will be considered first and so forth. If none of the listed protocol is supported by the back end server the connection to back end server will be rejected. • Default value: TLSv1.2,TLSv1.1,TLSv1 • Allowed Pattern/Values: A comma separated list of SSL protocols. Ex: TLSv1.2,TLSv1.1. Please refer Java Secure Socket Extension (JSSE) Reference Guide for the list of protocols that can be used in enabled protocols. • Data Type: String
mail.requesttimeout	Time out value in seconds to use if Mail server does not respond within this time. Zero means never time out • Default value: 180 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0

Table 10-4 (Cont.) Mail Service Configuration Properties

Option Name	Description
mail.cookiename	Cookie name used by mail service as session identifier • Default value: webmailsid • Data Type: String
mail.proxyadminid	Back-end 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 • Default value: Not Applicable • Data Type: String
mail.proxyadminpwd	Back-end mail service's proxy admin password. Used for proxy-auth to mail service • Default value: Not Applicable • Data Type: String
mail.uwcsievecompatible	Specifies whether the sieve should be compatible with Communications Express • Default value: true • Allowed Pattern/Values: true or false • Data Type: Boolean
mail.uidreplayformat	The replayformat option takes an argument of string that says how to construct the user ID for replay to the back end server. • Default value: %U@%V • Valid macros: %U = uid of the user ("hari"), %V = domain of the user ("somedomain.com"), %o = Actual value that was entered while log in, %s = uid@domain ("hari@somedomain.com") • Data Type: String
mail.spam.folder	Spam folder used to move messages marked as spam by the user • Default value: spam • Data Type: String
mail.spam.enableaction	Specifies whether Spam Action (ability to mark/unmark messages as spam) should be enabled • Default value: false • Allowed Pattern/Values: true or false • Data Type: Boolean
mail.pop.refreshinterval	Time interval (in sec) for the client to check the external mail server for new messages • Default value: 600 • Allowed Pattern/Values: 0-3600 seconds • Data Type: Integer
mail.pop.requesttimeout	Time interval (in sec) to wait for the response for POP requests. Zero means never timeout. • Default: 600 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0.

Table 10-4 (Cont.) Mail Service Configuration Properties

Option Name	Description
mail.enablemsgpreview	Turns on/off the mail preview pane • Default: true • Data Type: Boolean • Allowed Pattern/Values: true or false 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.
mail.maxpool	Maximum number of connections per route in a pool; this setting can be used when setting up a connection manager. • Default: 100 • Data Type: Integer
mail.pooltimeout	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. • Default: 240 • Data Type: Integer
mail.externalaccount.enable	Whether to enable external account or not. • Default value: true • Allowed Pattern/Values: true or false • Data Type: Boolean
mail.restrictanyone	Mirror option of store.privatesharedfolders.restrictanyone on Oracle Communications Messaging Server • Default value: false • Allowed Pattern/Values: true or false • Data Type: Boolean
mail.htmlsanitizer.enable	Whether HTML sanitizer is enabled or not. • Default value: true • Allowed Pattern/Values: true or false • Data Type: Boolean
mail.htmlsanitizer.additionalwhitelist	Comma separated list of HTML elements and attributes which should be allowed in mail content. Convergence already has an internal whitelist which cannot be changed. This additional whitelist is in addition to the internal whitelist. If an attribute is specified without an associated element, then that attribute will not be allowed for all elements. • Default value: Not applicable • Allowed Pattern/Values: *item1*[, *item2* ...]. Where *item* can be <protocol>:|<attribute>|<attribute>@<element> • Data Type: string Examples: • attribute1, attribute2 - Allow attribute1 and attribute2 on all elements • attribute1@element1 - Allow attribute1 on element1 only • @element1, @element2 - Allow element1 and element2 with no attributes • protocol1: - Allow protocol1. Colon(:) at end indicates it is a protocol

Table 10-4 (Cont.) Mail Service Configuration Properties

Option Name	Description
mail.htmlsanitizer.additionalblacklist	Comma separated list of HTML elements and attributes which should be disallowed in mail content. Convergence already has an internal blacklist which cannot be changed. This additional blacklist is in addition to the internal blacklist. If an attribute is specified without an associated element, then that attribute will not be allowed on any element. • Default value: Not applicable • Allowed Pattern/Values: *item1*[, *item2* ...]. Where *item* can be <protocol>:|<attribute>|<attribute>@<element> • Data Type: string Examples: • attribute1, attribute2 - Do not allow attribute1 and attribute2 on all elements • attribute1@element1 - Do not allow attribute1 on element1 only • @element1, @element2 - Do not allow element1 and element2 • protocol1: - Do not allow protocol1. Colon(:) at end indicates it is a protocol
mail.htmlsanitizer.additionalcsswhitelist	Comma separated list of CSS properties for inline style, which should be allowed in mail content. Convergence already has a default CSS property list, only few additional CSS properties can be added to the whitelist. If an additional CSS property is not supported by HTML sanitizer, an exception will be thrown. • Default value: Not applicable • Allowed Pattern/Values: *item1*[, *item2* ...]. Where *item* can be CSS property like visibility and z-index • Data Type: string
mail.htmlsanitizer.allowurlsinstyle	Whether to allow URLs in inline styles or not. Enabling this option is vulnerable to XSS. This option can be set if the URLs referenced in mail content is from trusted source and is secure. • Default value: false • Allowed Pattern/Values: true or false] • Data Type: Boolean Example:
mail.htmlsanitizer.sanitizesignature	Whether to enable HTML sanitization for email signature. • Default value: true • Data Type: boolean • Allowed Pattern: true or false

Table 10-5 Logging Configuration Properties

Option Name	Description
log.enableusertrace	Specifies whether user IP address and session ID should be included in the logs. Log pattern must include %X{ipaddress} and %X{sessionid}. • Allowed Pattern/Values: true or false • Default value: true • Data Type: Boolean

Table 10-5 (Cont.) Logging Configuration Properties

Option Name	Description
log.locationtype	Definition for specifying Log Location Type. Currently supported location type: FILE, CONSOLE (aka STDOUT). • Default value: CONSOLE • Allowed Pattern/Values: FILE or CONSOLE • Data Type: String
log.location	The Location value is the location of Log file (and hence is applicable only for FILE type) • Default value: /data/logs/iwc.log • Data Type: String
log.adminloglocationtype	Log location type for admin log file • Default value: FILE • Allowed Pattern/Values: FILE or CONSOLE • Data Type: String
log.adminloglocation	The location of admin log file (and hence is applicable only for FILE type) • Default value: /data/logs/iwc_admin.log • Data Type: String
log.sizetriggerval	Set the maximum size in KB, that the log file is allowed to reach before being rolled over to backup files • Default value: 2048 • Allowed Pattern/Values: Greater than 0 KB • Data Type: Integer
log.timetriggerval	The rolling schedule is specified by this pattern. Set the Date pattern at which the log file will be rolled over to backup files • 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	This option determines how many backup files are kept before the oldest is erased. This option takes a positive integer. If set to zero, there will be no backup files and the log file will be truncated when it reaches the size trigger value. The max backup index option is considered only if size trigger is set and is ignored for time trigger. • Default value: 1 • Data Type: Integer
log.pattern	The log record pattern used by the loggers • 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 print function in C. For detailed patterns, refer to Pattern Layout documentation in Apache Log4j project • Data Type: String
log.DEFAULT.level	Level of Logging • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String

Table 10-5 (Cont.) Logging Configuration Properties

Option Name	Description
log.CONFIG.level	Level of Logging for Config module • Default value: WARN • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.AUTH.level	Level of Logging for Auth module • Default value: DEBUG • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.PROXY_MAIL.level	Level of Logging for Proxy Mail module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.ADDRESS_BOOK.level	Level of Logging for Address Book module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.PROXY_CAL.level	Level of Logging for Proxy Cal module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.PROXY_NAB.level	Level of Logging for Contacts Server proxy module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.PROTOCOL.level	Level of Logging for Protocol module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.SIEVE.level	Level of Logging for Sieve module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.NOTIFY.level	Level of logging for notification module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.ADMIN.level	Level of Logging for Admin module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.ENS.level	Level of logging for ENS module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String

Table 10-5 (Cont.) Logging Configuration Properties

Option Name	Description
log.PROXY_OIN.level	Level of Logging for Proxy OIN module • Default value: INFO • Allowed Pattern/Values: OFF | ERROR | WARN | INFO | DEBUG • Data Type: String
log.ADDRESS_BOOK.appendername	Appender name for ADDRESS_BOOK component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.ADMIN.appendername	Appender name for ADMIN component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.AUTH.appendername	Appender name for ADMIN component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.CONFIG.appendername	Appender name for CONFIG component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.DEFAULT.appendername	Appender name for DEFAULT component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.ENS.appendername	Appender name for ENS component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.NOTIFY.appendername	Appender name for NOTIFY component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.PROTOCOL.appendername	Appender name for PROTOCOL component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.PROXY_CAL.appendername	Appender name for PROXY CAL component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.PROXY_CONF.appendername	Appender name for PROXY CONF component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String

Table 10-5 (Cont.) Logging Configuration Properties

Option Name	Description
log.PROXY_MAIL.appendername	Appender name for PROXY MAIL component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.PROXY_NAB.appendername	Appender name for PROXY NAB component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.PROXY_OIN.appendername	Appender name for PROXY OIN component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.SIEVE.appendername	Appender name for SIEVE component • Default value: Not Applicable • Allowed Pattern/Values: • Data Type: String
log.appender.[*appender_name*].type where *appender_name* is the name of appender.	Definition for specifying Log Location Type. Currently supported location type: FILE, CONSOLE (aka STDOUT). • Default value: CONSOLE • Allowed Pattern/Values: FILE or CONSOLE • Data Type: String
log.appender.[*appender_name*].maxbackupindex where *appender_name* is the name of appender.	This option determines how many backup files are kept before the oldest is erased. This option takes a positive integer. If set to zero, there will be no backup files and the log file will be truncated when it reaches the size trigger value. The max backup index option is considered only if size trigger is set and is ignored for time trigger. • Default value: 1 • Data Type: Integer
log.appender.[*appender_name*].sizetriggerval where *appender_name* is the name of appender.	Set the maximum size in KB, that the log file is allowed to reach before being rolled over to backup files. • Default value: 2048 • Allowed Pattern/Values: Greater than 0 KB • Data Type: Integer
log.appender.[*appender_name*].pattern where *appender_name* is the name of appender.	The log record pattern used by the loggers. • 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 print function in C. For detailed patterns, refer to Pattern Layout documentation in Apache Log4j project. • Data Type: String

Table 10-6 Calendar Service Configuration Properties for Calendar Server 7 and Calendar Server 8

Option Name	Description
caldav.enable	Whether CalDAV Calendar service is enabled or not • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false

Table 10-6 (Cont.) Calendar Service Configuration Properties for Calendar Server 7 and Calendar Server 8

Option Name	Description
caldav.host	Host name of the back end CalDAV service • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\-]+(\.[A-Za-z0-9\-]+)* • Data Type: String
caldav.port	Port number at which back end CalDAV service listens • Default value: 8080 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
caldav.enablessl	Whether SSL should be used against back end CalDAV service • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
caldav.enabledsslprotocols	A list of the SSL protocols that will be used to decide which protocol to use while connecting to CalDAV Server over SSL connection. The first in the list will be considered first and so forth. If none of the listed protocol is supported by the back end server the connection to back end server will be rejected. • Default value: TLSv1.2,TLSv1.1,TLSv1 • Allowed Pattern/Values: A comma separated list of SSL protocols. Ex: TLSv1.2,TLSv1.1. Please refer Java Secure Socket Extension (JSSE) Reference Guide for the list of protocols that can be used in enabled protocols. • Data Type: String
caldav.requesttimeout	Time out value in seconds to use if CalDAV server does not respond within this time. Zero means never time out • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 180 • Data Type: Integer
caldav.serviceuri	Context URI at which the WCAP interface in CalDAV service is accessible • Default value: /wcap • Data Type: String
caldav.proxyadminid	Back end 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 • Default value: Not Applicable • Data Type: String
caldav.proxyadminpwd	Back end CalDAV service's proxy admin password. Used for proxy-auth to calendar service • Default value: Not Applicable • Data Type: String
caldav.davuserattr	Attribute name in the user's LDAP entry indicating the user is a CalDAV user in a co-existence deployment • Default value: davstore • Data Type: String
caldav.groupobjectclass	Object class names of groups to be filtered while searching for Corp-Dir groups. The filter matches with any one of the configured object class names to retrieve the results • Default value: null • Data Type: String

Table 10-6 (Cont.) Calendar Service Configuration Properties for Calendar Server 7 and Calendar Server 8

Option Name	Description
caldav.autoprovision	Whether CalDAV auto-provision in the back end CalDAV Server is enabled or not. • Allowed Pattern/Values: true or false • Default value: false • Data Type: Boolean
caldav.davuserobjectclass	Name of the LDAP object class which should be present for valid CalDAV users if auto-provisioning is disabled • Allowed Pattern/Values: Name of the LDAP object class • Default value: icsCalendarUser • Data Type: String
caldav.uidreplayformat	The replayformat option takes an argument of string that says how to construct the user ID for replay to the back end server. • Default value: %U@%V • Valid macros: %U = uid of the user ("hari"), %V = domain of the user ("somedomain.com"), %o = Actual value that was entered while log in, %s = uid@domain ("hari@somedomain.com") • Data Type: String
caldav.wcapversion	WCAP Version of the CalDAV Service • Default value: 7.0 • Data Type: String
caldav.maxpool	Maximum number of connections per route in a pool; this setting can be used when setting up a connection manager. • Default: 100 • Allowed Pattern/Values: Greater than 0. • Data Type: Integer
caldav.pooltimeout	Defines the time out (seconds) used when retrieving a connection from the pool. • Default: 240 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer

Table 10-7 Address Book Service Configuration Properties for Contacts Server

Option Name	Description
nab.enable	Whether the address book service provided by Contacts Server is enabled • Data Type: Boolean • Allowed Pattern/Values: true or false • Default value: false
nab.host	Host name of the back-end address book service provided by Contacts Server • Allowed Pattern/Values: [A-Za-z0-9\-]+(\.[A-Za-z0-9\-]+)* • Data Type: String
nab.port	Port number at which back-end address book service provided by Contacts Server service listens • Default value: 8080 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer

Table 10-7 (Cont.) Address Book Service Configuration Properties for Contacts Server

Option Name	Description
nab.enablessl	Whether SSL is enabled to Contacts Server • Default value: true • Allowed Pattern/Values: true or false • Data Type: Boolean
nab.enabledsslprotocols	A list of the SSL protocols that will be used to decide which protocol to use while connecting to NAB Server over SSL connection. The first in the list will be considered first and so forth. If none of the listed protocol is supported by the back end server the connection to back end server will be rejected. • Default value: TLSv1.2,TLSv1.1,TLSv1 • Allowed Pattern/Values: A comma separated list of SSL protocols. Ex: TLSv1.2,TLSv1.1. Please refer Java Secure Socket Extension (JSSE) Reference Guide for the list of protocols that can be used in enabled protocols. • Data Type: String
nab.requesttimeout	Time out value in seconds to use if address book service provided by Contacts Server does not respond within this time. Zero means never time out • Default value: 180 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
nab.proxyadminid	Contacts Server proxy admin UID. Used for proxy-auth to address book service. This should be of form: uid@domain if hosted domains setup is used • Data Type: String
nab.proxyadminpwd	Contacts Server proxy admin password. Used for proxy-auth to address book service • Data Type: String
nab.nabuserattr	Attribute name in the user's LDAP entry indicating whether the address book service is provided by Contacts Server or Convergence in a co-existence deployment • Default value: nabStore • Data Type: String
nab.uidreplayformat	The replayformat option takes an argument of string that says how to construct the user ID for replay to the back end server. • Default value: %U@%V • Valid macros: %U = uid of the user ("hari"), %V = domain of the user ("somedomain.com"), %o = Actual value that was entered while log in, %s = uid@domain ("hari@somedomain.com") • Data Type: String
nab.maxpool	Maximum number of connections per-route • Default value: 100 • Allowed Pattern/Values: Greater than 0. • Data Type: Integer
nab.pooltimeout	Defines the time out (seconds) used when retrieving a connection from the pool. • Default value: 240 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
nab.serviceuri	Context URI at which the address book service provided by Contacts Server is accessible • Data Type: String

Table 10-8 Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.enable	Enable or disable WABP service • Default value: false • Allowed Pattern/Values: true or false • Data Type: Boolean
ab.purgetype	Enables WABP purge, which permanently deletes entries marked for deletion. If **ab.purgetype** is **auto** then purging happens automatically upon login. If **ab.purgetype** is **manual** then purging can be done by invoking the **purge_entries.wabp** command. • Default value: auto • Allowed Pattern/Values: manual | auto • Data Type: String • Access Type: RESTRICTED
ab.expireperiod	WABP Purge, period (in days) after which the entries get deleted permanently. This is applicable only when **enableautopurge** is set to true • Default value: 30 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.purgeinterval	When **ab.purgetype** is set to **auto**, this parameter specifies the interval (in days) between purges of the database. • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.maxpostlength	Defines the maximum content-length of a POST command. -1 means no limit. • Default value: -1 • Allowed Pattern/Values: -1, 0 or greater than 0 • Data Type: Integer
ab.mycontacttag	Tag name for my contact • Default value: My Contact • Data Type: String
ab.myfavoritestag	Tag name for my favorites • Default value: My Favorites • Data Type: String
ab.maxphotosize	Maximum allowed photo size in bytes • Default value: 102400 • Allowed Pattern/Values: Greater than 0 • Data Type: Integer
ab.maxphotowidth	Limit on dimension (width in pixels) of images being served • Default value: 2000 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ab.maxphotoheight	Limit on dimension (height in pixels) of images being served • Default value: 2000 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.exportphoto	If this is enabled it exports contacts with photo data in vCard 3.0 format • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.importphoto	If this is enabled it imports contacts with photo data in vCard 3.0 format • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.import.vcard.misc	Specify encoding to be used during import corresponding to each locale • Default value: UTF-8 • Data Type: String
ab.export.vcard.misc	Specify encoding to be used during export corresponding to each locale • Default value: UTF-8 • Data Type: String
ab.maxpagedsearch	Max number of simultaneous paged search for an instance of PersonalStore • Default value: 10 • Allowed Pattern/Values: Greater than 1 • Data Type: Integer
ab.retries	Number of retries to fetch default address book when a new user logs in • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.psrootpattern	Defines a default psRoot pattern for users that do not 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") • Default value: ldap:///piPStoreOwner=%U,o=%D,o=PiServerDb • Allowed Pattern/Values: Starts with ldap:// • Data Type: String
ab.ldapdelay	Amount of delay in number of milliseconds to be introduced to compensate delays due to LDAP updates • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.storecachecount	Enable cache entry count • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.storeentrieslimit	Total number of entries allowed in the user's address book. • Default value: 1000 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.storequotawarn	Indicate whether quota warning can be issued or not. A positive integer greater than zero indicates a warning else no warning. • Allowed Pattern/Values: Greater than or equal to 0 • Default value: 100 • Data Type: Integer
ab.useuserpsroot	Whether the per User psRoot should be used or not • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.pstore.[*identifier*].ldappoolmin	Minimum connections to the LDAP server • Default value: 1 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.pstore.[*identifier*].ldappoolmax	Maximum connections to the LDAP server • Default value: 4 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.pstore.[*identifier*].ldappooltimeout	Max time (in seconds) to wait for a connection to be freed up • Default value: 10 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.pstore.[*identifier*].ldappoolrefreshinterval	Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.pstore.[*identifier*].ldappoolmonitoringinterval	Monitoring interval in seconds for LDAP pool, when the LDAP server is down • Default value: 60 • Allowed Pattern/Values: Greater than or equal to 1 • Data Type: Integer
ab.pstore.[*identifier*].ldaphost	Host name of the LDAP service • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\\-]+(\.[A-Za-z0-9\-]+)* • Data Type: String
ab.pstore.[*identifier*].ldapport	Port number at which LDAP service listens • Default value: 389 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
ab.pstore.[*identifier*].ldapbinddn	The admin DN used for creating LDAP connection pool. This pool will be used for PStore lookup • Default value: Not Applicable • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.pstore.[*identifier*].ldapbindcred	The admin DN's password, used for creating LDAP connection pool. This pool will be used for PStore lookup. • Default value: Not Applicable • Data Type: String
ab.pstore.[*identifier*].enableldapssl	Enable LDAP SSL • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.pstore.urlmatch	Specifies the type of URL this instance of the plug-in is responsible for. This value should be unique and is case sensitive. • Default value: ldap:// • Allowed Pattern/Values: Starts with ldap:// • Data Type: String
ab.pstore.randompaging	Specifies if the plug-in 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. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.pstore.logintype	This can be: anon (anonymous), restricted (login as user who has rights to view/write DB), or proxy (login as user that can 'masquerade') • Default value: restricted • Allowed Pattern/Values: anon, restricted, or proxy • Data Type: String
ab.pstore.defaultserver	Default server (identifier) used for construction psRoot • Default value: null • Data Type: String
ab.pstore.displayname	Display Name for Personal book • Default value: Personal Address Book • Data Type: String
ab.pstore.description	Description for Personal book • Default value: This is your personal Address Book • Data Type: String
ab.pstore.getalldbattr	This defines if all the database attributes should be passed in the LDAP search true or false. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.pstore.lookthrulimit	This is the max number of entries to read in any one search. Should be set to max in directory or largest AB possible. • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.pstore.deleteperm	Mark the contact/group as deleted instead of permanently deleting it by setting following parameter as false • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.pstore.allowdupentry	Parameter which, if set to true, allows personal address book entries/ groups to have the same name • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.pstore.admingroupdn	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 • Default value: null • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String
ab.pstore.collationrule	Locale on whose basis collation rule should be applied for Personal Address Book • Default value: en-US • Data Type: String
ab.pstore.collationsearchfield	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. • Default value: null • Data Type: String
ab.corpdir.[*identifier*].ldappoolmin	Minimum connections to the LDAP server • Default value: 1 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[*identifier*].ldappoolmax	Maximum connections to the LDAP server • Default value: 4 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[*identifier*].ldappooltimeout	Max time (in seconds) to wait for a connection to be freed up • Default value: 10 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[*identifier*].ldappoolrefreshinterval	Time interval (in minutes) after which, connections in LDAP pool will be re-created. 0 means no refresh is required • Default value: 0 • Data Type: Integer • Allowed Pattern/Values: Greater than or equal to 0
ab.corpdir.[*identifier*].ldappoolmonitoringinterval	Monitoring interval (in seconds) for LDAP pool, when the LDAP server is down • Default value: 60 • Data Type: Integer • Allowed Pattern/Values: Greater than 0

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.corpdir.[*identifier*].ldaphost	Host name of the LDAP service • Default value: Not Applicable • Allowed Pattern/Values: [A-Za-z0-9\\-]+(\.[A-Za-z0-9\-]+)* • Data Type: String
ab.corpdir.[*identifier*].ldapport	Port number at which LDAP service listens • Default value: 389 • Data Type: Integer • Allowed Pattern/Values: 0 to 65535
ab.corpdir.[*identifier*].ldapbinddn	The admin DN used for creating LDAP connection pool. This pool will be used for corpdir lookup • Default value: Not Applicable • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String
ab.corpdir.[*identifier*].ldapbindcred	The admin DN password, used for creating LDAP connection pool. This pool will be used for corpdir lookup. • Default value: Not Applicable • Data Type: String
ab.corpdir.[*identifier*].enableldapssl	Enable LDAP SSL • Default value: false • Allowed Pattern/Value: true or false • Data Type: Boolean
ab.corpdir.[*identifier*].enable	Whether corporate directory is enabled or not • Default value: true • Allowed Pattern/Value: true or false • Data Type: Boolean
ab.corpdir.[*identifier*].urlmatch	Specifies the type of URL this instance of the plug-in is responsible for. This value should be unique and is case sensitive. • Default value: ldap:// • Allowed Pattern/Values: Starts with ldap:// • Data Type: String
ab.corpdir.[*identifier*].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* • Default value: 0 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
ab.corpdir.[*identifier*].randompaging	Specifies if the plug-in 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. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.corpdir.[*identifier*].vlvpaging	Use VLV if DB has a VLV set for the default search type • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.corpdir.[*identifier*].logintype	This can be: anon (anonymous), restricted (login as user who has rights to view/write DB), or proxy (login as user that can 'masquerade') • Default value: restricted • Allowed Pattern/Values: anon, restricted, or proxy • Data Type: String If you are performing an anonymous search (specifically, **ab.corpdir.[*identifier*].logintype = anon**), you need to set the following additional parameters: **ab.corpdir.[*identifier*].ldaphost =** *ldap_host* and **ab.corpdir.[*identifier*].ldapport =** *ldap_port*.
ab.corpdir.[*identifier*].searchfilter	Search filter for corporate directory searches. Syntax: *(&(&(*[filter])*(|(objectClass=GROUPOFUNIQUENAMES)(objectClass=GROUPOFURLS)(objectClass=ICSCALENDARRESOURCE)(objectClass=INETORGPERSON)))(objectClass=*)))*, Where [filter] will be replaced with search criteria. Ex: If search criteria is cn=* then [filter] will be replaced with cn=* • Default value: null • Allowed Pattern/Values: Refer RFC 2254 • Data Type: String
ab.corpdir.[*identifier*].vlvfilter	VLV Search filter for corporate directory searches. • Default value: null • Allowed Pattern/Values: Refer RFC 2254 • Data Type: String
ab.corpdir.[*identifier*].vlvsearchbase	VLV search base dn from where the corporate directory vlv searches are performed. • Default value: null • Allowed Pattern/Values: (.*=.*([,;\+].*)*)? • Data Type: String
ab.corpdir.[*identifier*].vlvsortby	VLV sort by fields for performing corporate directory searches. Multiple fields must be comma separated. For example, entry/displayname,person/surname. • 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
ab.corpdir.[*identifier*].vlvscope	VLV Search scope used for corporate directory searches. • Default value: 2 • Allowed Pattern/Values: 0|1|2 • Data Type: Integer
ab.corpdir.[*identifier*].defaultserver	Default server (identifier) used for construction psRoot • Default value: null • Data Type: String
ab.corpdir.[*identifier*].displayname	Display Name for corp dir • Default Value: Corporate Directory • Data Type: String
ab.corpdir.[*identifier*].description	Description for corporate directory • Default Value: This is your Corporate Directory • Data Type: String

Table 10-8 (Cont.) Address Book Service Configuration Properties for Convergence WABP

Option Name	Description
ab.corpdir.[*identifier*].searchattr	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. • Default value: entry/displayname • Data Type: String Convergence can be configured to search corporate directory on required fields. For example, when the search string is "someone" and if you want to search this string only in the uid, set *ab.corpdir.[identifier].searchattr* to *@uid*. 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: 1. uid @uid 2. displayname entry/displayname 3. givenname person/givenname 4. surname person/surname. To refer uid, use @uid. The symbol @ must be used because the uid is attribute of an element.
ab.corpdir.[*identifier*].groupoc	Comma separated list of object classes to identify group entries. • Default Value: (objectclass=groupOfUniqueNames) • Data Type: String
ab.corpdir.[*identifier*].resourceoc	Comma separated list of object classes to identify resource entries. • Default value: (objectclass=ICSCALENDARRESOURCE) • Data Type: String
ab.corpdir.[*identifier*].getalldbattr	This defines if all the database attributes should be passed in the LDAP search. Valid values are true or false. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
ab.corpdir.[*identifier*].lookthrulimit	This is the max number of entries to read in any one search. Should be set to max in directory or largest AB possible. • Default value: 0 • Allowed Pattern/Values: 0 or greater • Data Type: Integer
ab.corpdir.[*identifier*].collationrule	Locale on whose basis collation rule should be applied for Corporate Directory • Default Value: en-US • Data Type: String
ab.corpdir.[*identifier*].collationsearchfield	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. • Default Value: null • Data Type: String

Table 10-9 Deployment or Domain Specific Configuration Properties

Option Name	Description
client.updateunreadcount	Whether to update unread count for all folders when 'Get Mail' is clicked. Default is false. • 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 • Default value: 300 • Allowed Pattern/Values: 0-3600 seconds • 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 • Default value: 60 • Allowed Pattern/Values: 0-600 seconds • Data Type: Integer
client.corpabentriesperpage	Default number of entries per page used for corporate directory search. • 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 • Default value: en-US • Data Type: String
client.helpurl	Configure help URL for the application. For example help link out side application context: http://example.com/en/industries/communications To facilitate locale specific help URL, follow the below pattern. Please check the external help with locale specific support before configuring the help. For example: http://example.com/${locale}/industries/communications/ OR http://example.com/industries/communications?locale=${locale} ${locale} will be replaced with user preferred locale. • Default value: .../<iwc_static_context>/layout/help/... • Data Type: String
client.antispamurl	Site specified service endpoint, which can permit each site to train their anti-spam service to recognize the message as spam in the future • Default value: /antispam • Data Type: String
client.autologouttime	Time out period (in min) to auto log off users (by client) after a predefined period of inactivity • Default value: 15 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
client.smarttznames	Site wide defined set of time zones • Default value: "" • Data Type: String
client.enablecustomization	Turn on or off customization service • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false

Table 10-9 (Cont.) Deployment or Domain Specific Configuration Properties

Option Name	Description
client.enablertfcompose	Turn on/off RTF editing for entire deployment. If it set to false then user's preference to enable or disable RTF editing will be ignored by convergence client. The default value is true. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
client.screennameeditable	Turn on/off editing user's display name through mail's local identity option. • Allowed Pattern/Values: true or false • Default value: false • Default value: false • Data Type: Boolean
client.uploadfilemethod	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 • Default Value: html5 • Data Type: String • Allowed Pattern/Values: iframe (hide progress indicator) or html5 (display progress indicator)
client.enablecorpabautocomplete	Turn on/off Auto completion of addresses from Corporate Address Book. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
client.enablesecondaryemail	Enables or disables secondary email functionality. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
client.enablemap	Enables or disables map. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
client.enabledtheme	To enable all available themes use 'all', the default value is also all. To enable a subset of the supported themes provide the theme names in a comma separated list. Supported theme names are: [all | theme_blue | theme_orange | theme_dark_blue | theme_light_blue | theme_grey | theme_yellow | theme_green | theme_teal | theme_pink | theme_butterfly|theme_teal_ocean | theme_pink_hearts | theme_blue_cheery | theme_starry | Altair] The default user interface theme option should be one of the enabled themes. • Default value: all • Data Type: String
client.enablecallusingskype	Enables or disables call using skype. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false

Table 10-9 (Cont.) Deployment or Domain Specific Configuration Properties

Option Name	Description
client.hideglobaltimezoneselection	Whether to show or hide timezone selection in global options. • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
client.allowbuddyfromhosteddomain	Allows user to add from all the hosted domains. This option hides adding buddy from Personal Address Book and through Email Address when set to false. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
client.misc	This facilitates adding custom client preference. For example, misc.{custom-attribute}> • Allowed Pattern/Values: user-defined-attribute • Data Type: String
client.groupsearchuniqueid	Group search unique id field facilitates adding client specific custom field for unique Id. Multiple fields must be comma separated. Ex: uid,cn • Default value: uid • Data Type: string
client.groupsearchuniqueentry	Group search unique entry is XPath of group search unique id attributes. Ex: XPath for uid is entry/@entryID, cn is entry/displayname. Multiple fields must be comma separated. The order of the group search unique entry attribute should match exactly the order of group search unique id attributes. • Default value: entry/@entryID • Data Type: string
client.mainpage	Location of the static html main page • Default value: /iwc_static/layout/main.html • Data Type: String
client.loginpage	Location of the static html login page • Default value: /iwc_static/layout/login.html • Data Type: String
client.anoncalviewpage	Location of the static html Anonymous calendar view page • Default value: /iwc_static/layout/calendar.html • Data Type: String
client.changepasswordpage	The URL for changing the user's password after it expires • Data Type: String
client.enablesmsnotification	Hide or show the SMS option in the **Notifications** tab in Calendar Options and in the **Reminder** dialog box. • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
client.enableforcelogout	Whether to enable force logout or not when the primary services like mail and calendar are disabled. • Default value: false • Data Type: boolean • Allowed Pattern: true or false

Table 10-9 (Cont.) Deployment or Domain Specific Configuration Properties

Option Name	Description
client.enableAttachmentRestriction	Enables or disables attachment of certain file types in emails. • Default Value: false • Data Type: boolean • Allowed Pattern: true or false
client.restrictedExtensionTypes	List of file extensions blocked as attachments in emails • Default Value: .ade,.adp,.apk,.appx,.appxbundle,.bat,.cab,.chm,.cmd,.com,.cpl,.diagcab,.diagcfg,.diagpack,.dll,.dmg,.ex,.ex_,.exe,.hta,.img,.ins,.iso,.isp,.jar,.jnlp,.js,.jse,.lib,.lnk,.mde,.msc,.msi,.msix,.msixbundle,.msp,.mst,.nsh,.pif,.ps1,.scr,.sct,.shb,.sys,.vb,.vbe,.vbs,.vhd,.vxd,.wsc,.wsf,.wsh,.xll • Data Type: String • Allowed Pattern: comma separated list of extensions eg: .abc,.def

Table 10-10 Administration Service Configuration Properties

Option Name	Description
admin.enablessl	Whether SSL is enabled for admin service • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
admin.enabledsslprotocols	A list of the SSL protocols that will be used to decide which protocol to use while connecting to admin service over SSL connection. The first in the list will be considered first and so forth. If none of the listed protocol is supported by the admin service the connection to admin service will be rejected. • Default value: TLSv1.2,TLSv1.1,TLSv1 • Data Type: String • Allowed Pattern/Values: A comma separated list of SSL protocols. Ex: TLSv1.2,TLSv1.1. Please refer Java Secure Socket Extension (JSSE) Reference Guide for the list of protocols that can be used in enabled protocols.
admin.enablemonitoring	Whether monitoring is enabled • 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 • Default value: Not Applicable • Data Type: String
admin.keystorepwd	Keystore password for SSL enabled admin server • Default value: Not Applicable • Data Type: String

Table 10-11 Single-Sign-On Configuration Properties

Option Name	Description
sso.oam.enable	This creates default configuration parameters required to enable OAM SSO mechanism. Specific parameters can further be modified/created using parameter-specific CLI option. This flag differs from sso.enable • Allowed Pattern/Values: true
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 • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false • Access Type: RESTRICTED
sso.servicename	This specifies the enabled SSO service name • Data Type: String
sso.enable	This specifies whether SSO service is enabled or not • Default value: false • Allowed Pattern/Values: true or false • Data Type: Boolean
sso.enablesignoff	Whether single sign off service is enabled or not • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
sso.ssoserviceimpl	SSO implementation provider name • Default value: Not Applicable • Data Type: String
sso.notifyserviceimpl	Notification service implementation • Default value: null • Data Type: String
sso.enablerefreshsso	Whether SSO token refresh is enabled or not • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
sso.refreshinterval	After what percentage of convergence session time out interval, SSO token should be refreshed • Default value: 80 • Data Type: Integer
sso.misc	Placeholder for custom SSO provider configuration • Allowed Pattern/Values: user-defined-attribute • Data Type: String
sso.adminuid	Admin userid for SSO provider • Default value: Not Applicable • Data Type: String
sso.adminpwd	Admin password for SSO provider • Default value: Not Applicable • Data Type: String
sso.loginpage	Location of the login page to which the user is redirected to. • Default value: null • Data Type: String

Table 10-12 User Preferences Configuration Properties

Option Name	Description
user.common.defaultapp	The default application to display to user upon login • Default value: mail • Allowed Pattern/Values: Name of the service. For example, mail, calendar. • Data Type: String
user.common.theme	Specifies the name of default user interface theme used • Default value: theme_blue • Data Type: String
user.common.defaultmailhandler	Specifies the default mail handler for all mail links • Default value: uc • Data Type: String
user.common.dateformat	Specifies date display and input format • 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	Delimiter is the character that separates date, month and year in the date • Default value: / • Allowed Pattern/Values: This can be any of -, / or . • Data Type: String
user.common.timeformat	Specifies the time display format • Default value: 12 • Allowed Pattern/Values: This can be any of 12 or 24 • Data Type: Integer
user.common.timezone	Specifies the time zone used to normalize all time/date information in the client • Default value: America/Los_Angeles • Data Type: String
user.common.enablesmartTZ	Allows the end user to enable or disable the smart Time zone feature for the client • Default value: true • Data Type: Boolean • Allowed Pattern/Value: true or false
user.common.layoutPreference	Allows the end user to choose their preferred layout type (ecko/classic) • Default value: ecko • Data Type: String
user.ab.name	Specifies the name of address book • Default value: Personal Address Book • Data Type: String
user.ab.description	Specifies the description of address book • Default value: This is the personal address book • Data Type: String

Table 10-12 (Cont.) User Preferences Configuration Properties

Option Name	Description
user.ab.entriesperpage	Specifies the number of entries to be displayed per page • Allowed Pattern/Values: Greater than or equal to 1 • Default value: 100 • Data Type: Integer
user.cal.defaultview	Calendar view to be presented at log in • Default value: dayview • Allowed Pattern/Values: This can be any of dayview, weekview, monthview, next7view, agendaview • Data Type: String
user.cal.defaultcategory	Specifies the default category for a event or a task • Default value: Business • Allowed Pattern/Values: Default Category for an event or a task. Ex: Appointment, Breakfast, Business • Data Type: String
user.cal.daystart	Start time hour for displaying calendar information • Default value: 9 • Allowed Pattern/Values: Value of the hour in 24 hr format (0 - 23 hrs) • Data Type: Integer
user.cal.dayend	End time hour for displaying calendar information • Default value: 18 • Allowed Pattern/Values: Value of the hour in 24 hr format (0 - 23 hrs) • Data Type: Integer
user.cal.weekfirstday	First day of the week to be displayed on user's calendar • Default value: 1 • Allowed Pattern/Values: Valid values are 1 through 7. 1 - Sunday, 2 - Monday. etc. • Data Type: Integer
user.cal.weekenddays	Specifies the weekend days • Default value: 1,7 • Allowed Pattern/Values: Valid values are 1 through 7. 1 - Sunday, 2 - Monday. etc • Data Type: String
user.cal.reminderinterval	Amount of time before the event that an alarm should be sent • Default value: -PT0H30M • Data Type: String
user.cal.enablenotify	Enables/disables email notifications being sent for the event reminder • Default value: 0 • Allowed Pattern/Values: 0 - disable, 1 - enable • Data Type: Integer

Table 10-12 (Cont.) User Preferences Configuration Properties

Option Name	Description
user.cal.enablesmsnotify	Enables/disables sms notifications being sent for the event reminder • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
user.cal.enableinvitenotify	Enables/disables email notifications being sent when the calendar receives an invitation • Default value: false – Data Type: Boolean – Allowed Pattern/Values: true or false
user.cal.eventfilter	Specifies the type of events to be displayed • Default value: null • Data Type: String
user.mail.deleteonlogout	Specifies if mails marked as deleted has to be removed when user logs out of application • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
user.mail.autospellcheck	Specifies if auto spell check is enabled • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
user.mail.blockimages	Specifies if images in the incoming mail should be shown or blocked • Default value: false • Data Type: Boolean • Allowed Pattern/Values: true or false
user.mail.mailsperpage	Specifies the number of mails to display per page • Default value: 20 • Data Type: Integer
user.mail.sortorder	Specifies the sorting order • Default value: R • Data Type: String
user.mail.sortbycol	Specifies which column to be used to sort the mails • Default value: 6 • Data Type: Integer
user.mail.enablertfcompose	Specifies if compose window should use RTF • Default value: true • Data Type: Boolean • Allowed Pattern/Values: true or false
user.mail.displaycol	Specifies which columns to display in mail view • Default value: 2,1,4,3,5,6,0,7 • Data Type: String
Allowed Pattern/Values: true or false	Change my status to idle when I am inactive for this many minutes • Default value: 10 • Data Type: Integer

Table 10-13 Event Notification System Configuration Properties

Option Name	Description
ens.service.enable	Enable or disable event notification system • Default value: false • Allowed Pattern/Values: true or false • Data Type: Boolean
ens.[*Service_Name*].enable	Enable or disable notification service associated with this service name • Allowed Pattern/Values: true or false • Data Type: Boolean
ens.[*Service_Name*].servicename	The name used to identify this service in ENS. Setting this to blank deletes this service. • Data Type: String
ens.[*Service_Name*].datasource	The name used to identify data source for this service. • Data Type: String
ens.[*Service_Name*].threadpoolsize	The number of threads to be created to process incoming messages • Default value: 10 • Data Type: Integer

Table 10-14 Address Book Service JMQ Notification Configuration Properties

Option Name	Description
notify.service.enable	Enable or disable notification service • 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. • 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. • Data Type: String
notify.mq.[%serviceName%].enable	Enable or disable notification service associated with this service name • 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 • Allowed Pattern/Values: TOPIC or QUEUE • Data Type: String

Table 10-15 Outside In Proxy Configuration Properties

Option Name	Description
oin.enable	Whether OIN service is enabled or not • Default value: false • Allowed Pattern/Values: true or false • Data Type: Boolean
oin.host	Host name of the back-end OIN service • Allowed Pattern/Values: [A-Za-z0-9\-]+(\.[A-Za-z0-9\-]+)* • Data Type: String
oin.port	Port number at which back-end OIN service listens • Default value: 60572 • Allowed Pattern/Values: 0 to 65535 • Data Type: Integer
oin.requesttimeout	Time out value in seconds to use if OIN server does not respond within this time. Zero means never time out • Default value: 180 • Allowed Pattern/Values: Greater than or equal to 0 • Data Type: Integer
oin.tsdirpath	Directory path for the OIN Transformation Server. Default path is /export/tsdir. Administrator needs to ensure this directory is setup with proper permissions for Convergence and Transformation Server to access. • Default value: /export/tsdir/ • Data Type: String
oin.autopruneinterval	Time interval (in minutes) to delete the transformed files in the TsdirPath • Allowed Pattern/Values: Greater than 0 • Default value: 5 • Data Type: Integer

11

Monitoring Convergence

This chapter describes how to collect data and monitor Oracle Communications Convergence activity.

Overview of Monitoring Convergence

Monitoring is the process of gathering, exposing, and computing run-time data to assess the performance of your Convergence deployment.

You use all the following tools to monitor Convergence:

- You use a Java management extensions (JMX) client, such as Jconsole, to gather and view JMX metrics.

  For more information about Jconsole, see the Jconsole documentation at:

  https://docs.oracle.com/javase/8/docs/technotes/guides/jmx/index.html

- You use the **iwcmetrics** command-line utility to gather and view non-JMX metrics.

> **Note:**
>
> The **iwcmetrics** command cannot collect JMX-based metrics, and the JMX client cannot collect non-JMX metrics. You must use all methods to fully and properly monitor Convergence.

Before you can monitor Convergence, you must:

- Enable monitoring in Convergence

  See "Enabling Convergence Monitoring" for more information.

- Set up JMX-based server monitoring

  See "Configuring Convergence for JMX Monitoring" for more information.

See "Using Jconsole for Convergence Monitoring" for information about using Jconsole to monitor Convergence. See "About Convergence JMX Metrics" for information about the metrics collected by the JMX client.

See "Using the iwcmetrics Command for Convergence Monitoring" for information about using the **iwcmetrics** command to monitor Convergence. See "About Convergence Non-JMX Metrics" for information about the metrics collected by the **iwcmetrics** command.

Enabling Convergence Monitoring

Use the **iwcadmin** command-line utility to enable Convergence monitoring and data collection. Set the **admin.enablemonitoring** parameter to **true** and restart the Oracle WebLogic server:

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

Configuring Convergence for JMX Monitoring

To use a JMX-compliant GUI tool, such as Jconsole, you must configure JMX-based server monitoring, the JVM, and the JAAS. For more information on JMX and JAAS settings and configuration files, see the JMX documentation at:

https://docs.oracle.com/javase/8/docs/technotes/guides/jmx/index.html.

Using Jconsole for Convergence Monitoring

Jconsole is a JMX client which you can use to collect and view Convergence JMX metrics. See "About Convergence JMX Metrics" for more information about the metrics you can collect and view with Jconsole.

> **Note:**
>
> The default RMI listener has been changed to *localhost* in Convergence 3.0.3.2.0. Set `rmi.uselocalhost=false` in <*Convergence_Home*>/**config/adminservice.properties** to access JConsole when accessed from different hosts.

```
cat adminservice.properties
!Registry and Connector port configuration for JMX
rmi.registryport=50005
rmi.connectorport=50005
rmi.uselocalhost= false
```

To use Jconsole for Convergence monitoring:

1. Start Jconsole with 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 enter

   service:jmx:rmi://*hostname*:*port*/**jndi/rmi://***hostname*:*port*/**jmxrmi.**

> **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. For 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 user name 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.

See "About Convergence JMX Metrics" for a list of the metrics available.

About Convergence JMX Metrics

A JMX client can collect and view the following Convergence metrics:

- Authentication 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
- 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
  - Number of failed attempts

- User and Group LDAP
  - Directory server Host name from which the connections are being served
  - Number of free connections in the pool
  - Number of used connections in the pool
- Server
  - Active server duration

> **Note:**
>
> The JMX client cannot collect non-JMX metrics. See "Overview of Monitoring Convergence" for information about collecting non-JMX metrics.

Using the iwcmetrics Command for Convergence Monitoring

The **iwcmetrics** command-line utility is a script in the *Convergence_Home*/**sbin** directory which you can use to collect and view Convergence non-JMX metrics. See "About Convergence Non-JMX Metrics" for information about Convergence non-JMX metrics.

The following example shows the syntax of the **iwcmetrics** command:

```
iwcmetrics -U Convergence_URL -u user_name [-W password_file] -m Metric1,Metric2,MetricN
```

Table 11-1 describes the valid parameters for the **iwcmetrics** command.

Table 11-1 Parameters for iwcmetrics Command

Parameter	Description
-U	Specifies the complete Convergence URL: http(s)://*hostname.domain*:*port*/*URI*. For example: `https://Convergence.MyDomain.com:8181/iwc`
-u	Specifies the user name. The **iwcmetrics** command can only collect metrics for the services which the user is privileged to use. To collect metrics for all services, specify a user name that has access to all Convergence services.
-W	Specifies the location of the encrypted password file. If you omit the `-W` parameter, the command-line utility asks you to provide your password. For this reason, the `-W` parameter is omitted from all examples in this guide.
-m	Specifies the metrics to collect. This parameter can specify a single metric, a comma-separated list of metrics, or one or more entire groups of metrics. Metrics are grouped together by service. The `-m` parameter supports the following groups: iwc (Convergence), mail (email), caldav (calendar), and nab (Contacts Server address book). For example: `iwcmetrics -U Convergence_URL -u user_name -m metric1,metric2,group1,group2` Omit the `-m` parameter to collect all metrics. For example: `iwcmetrics -U Convergence_URL -u user_name` See "About Convergence Non-JMX Metrics" for more information about Convergence non-JMX metrics and the groups to which they belong.
-l	Lists all available metrics. You do not need to specify a user name or the Convergence URL. For example: `iwcmetrics -l`

Table 11-1 (Cont.) Parameters for iwcmetrics Command

Parameter	Description
-h	Displays information and help for the **iwcmetrics** command. You do not need to specify a user name or the Convergence URL. For example: `iwcmetrics -h`

The following list gives examples of using the **iwcmetrics** command:

- To display a list of all available metrics:

  ```
  iwcmetrics -l
  ```

- To display the help for the **iwcmetrics** command:

  ```
  iwcmetrics -h
  ```

- To collect all metrics:

  ```
  iwcmetrics -U Convergence_URL -u user_name
  ```

- To collect all metrics pertaining to the mail and address book services:

  ```
  iwcmetrics -U Convergence_URL -u user_name -m mail,nab
  ```

- To collect two metrics from different groups:

  ```
  iwcmetrics -U Convergence_URL -u user_name -m im.responsetime,caldav.status
  ```

About Convergence Non-JMX Metrics

Table 11-2 lists the Convergence metrics that can be collected and viewed using the **iwcmetrics** command.

Table 11-2 Parameters for iwcmetrics Command

Parameter Name	Description
iwc.loginresponsetime	A measure of the time taken (in milliseconds) to log into Convergence. This metric is part of the iwc group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m iwc.loginresponsetime`
mail.status	Indicates the status of Oracle Communications Messaging Server. A value of **0** indicates that it is working. This metric is part of the mail group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m mail.status`
mail.responsetime	A measure of the response time (in milliseconds) between Convergence and Messaging Server. This metric is part of the mail group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m mail.responsetime`
nab.status	Indicates the status of Oracle Communications Contacts Server. A value of **0** indicates that it is working. This metric is part of the nab group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m nab.status`

Table 11-2 (Cont.) Parameters for iwcmetrics Command

Parameter Name	Description
nab.responsetime	A measure of the response time (in milliseconds) between Convergence and Contacts Server. This metric is part of the nab group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m nab.responsetime`
caldav.status	Indicates the status of Oracle Communications Calendar Server. A value of **0** indicates that it is working. This metric is part of the caldav group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m caldav.status`
caldav.responsetime	A measure of the response time (in milliseconds) between Convergence and Calendar Server. This metric is part of the caldav group. Example: • `iwcmetrics -U Convergence_URL -u user_name -m caldav.responsetime`

Note:

The **iwcmetrics** command cannot collect JMX metrics. See "Overview of Monitoring Convergence" for information about collecting JMX metrics.

12

Troubleshooting Convergence

This chapter describes how to resolve problems you encounter in Oracle Communications Convergence.

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.

For more information on the **iwcadmin** command, see "Using the Convergence Administration Utility" for more information.

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 on the Apache web site:

  `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 "About Log Levels" for more information.

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 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.

13

Setting Up Multiple Corporate Directories

You can configure Convergence to use multiple corporate directories, or configure Convergence to use a directory server other than the user group directory server.

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 -o ab.corpdir.[default].ldaphost -v host.example.com
iwcadmin -o ab.corpdir.[default].ldapport -v 400
iwcadmin -o ab.corpdir.[default].ldapbinddn -v "cn=Directory Manager"
iwcadmin -o ab.corpdir.[default].ldapbindcred -v xyzxyz
```

The corporate directory can be configured with multiple directory servers. In this example *default* is used to identify corporate directory configuration for *host.example.com*. 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.[identifier].ldaphost
   ab.corpdir.[identifier].ldapport
   ab.corpdir.[identifier].ldapbinddn
   ab.corpdir.[identifier].ldapbindcred
   ab.corpdir.[identifier].urlmatch
   ab.corpdir.[identifier].searchattr
   ab.corpdir.[identifier].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/
ou=People,o=example.com,o=usergroup
-o ab.corpdir.[corpdir1].searchattr -v entry/displayname,@uid
-o ab.corpdir.[corpdir1].lookthrulimit -v 3000
-o ab.corpdir.[corpdir1].displayname -v "Second Corporate Book"
```

Note:

By default , `ab.corpdir.[identifier].enableldapssl` parameter is true. So `ab.corpdir.[identifier].ldapport` should be configured as ldaps port.

When `ab.corpdir.[identifier].ldapport` is configured to use ldap port, `ab.corpdir.[identifier].enableldapssl` parameter should be set to false.

2. Restart the Oracle WebLogic 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
```

Even though the Corporate Directories are properly set up and work as designed, they may display errors in the *iwc.log* or the Firebug log.

Disabling Corporate Directory (Newly Added or Default)

To disable a corporate directory, set the **ab.corpdir.[*identifier*].enable** parameter to **false**.

14

Overview of Add-on Services in Convergence

This chapter describes the add-on framework, the add-on configuration files, and instructions for adding or removing these third-party services in the Convergence UI.

About the Add-on Framework

The add-on framework provides access from Convergence to the third-party service through the use of an ID. The ID is provided by the service. The method of getting the ID differs from service to service. See the individual services sections for information on how to obtain the ID.

The add-on services are configured through Convergence configuration files. The available add-on services are listed in Table 14-1.

Table 14-1 Add-On Services

Service Name	Description
Advertising (advertising)	Displays banner ads, text ads, and contextual ads in the Convergence UI. See "Configuring the Advertising Add-On Service in Convergence" for more information.
SMS (sms)	Provides one-way SMS through Convergence. See *Configuring Convergence for SMS* for more information.

About the Add-On Configuration Files

The configuration files for supported add-ons are installed in the **/var/opt/sun/comms/iwc/config/** directory. There are three types of configuration files:

- **add-ons.properties**
- **addon_name.json**
- **addon_name.properties**

add-ons.properties

The **add-ons.properties** file specifies the add-ons that are to be enabled. The following file lists the add-on services that are available in the **add-ons.properties** file that comes with the installation.

1. Add on configuration.
2. A sample entry look like this:

```
# addons= advertising
addons= advertising
```

Verify that the service you want to add to your Convergence deployment is in the **add-ons.properties** file before going onto configuring that service.

addon_name.json

Each add-on has its own **addon_name.json** file, containing **client** configuration parameters for the add-on. You must enable the add-on service in **addon_name.json** in order for the service to be active in your Convergence deployment.

In the following **advertising.json** file, the advertising service is enabled. The comments describe each parameter:

```
{
        enabled: true,
        plugin: "c11n.allDomain.js.widget.advertising.Plugin",
        regions: {
                skyscraper: {
                        enabled: true,
                        width: 160,
                        closeEnable: true,
                        events: {
                                enabled: true,
                                adtime : 30,
                                allEvents: {
                                        mail: true,
                                        calendar: false,
                                        all: false
                                }
                        }

                },
                messageViewer:{
                        enabled: true,
                        locations: {
                                TopAd: {
                                        enabled: true,
                                        height: 60
                                },
                                RightAd: {
                                        enabled: true,
                                        width: 250,
                                        height: 250
                                },
                                LeftAd: {
                                        enabled: false,
                                        width: 250,
                                        height: 250
                                },
                                BottomAd: {
                                        enabled: true,
                                        height: 60
                                }
                        }
                }
        }
}
```

To disable an add-on service, set *enabled:false* in the **addon_name.json** file.

addon_name.properties

The **addon_name.properties** file contains **server** access parameters for add-on services.

Configuring Convergence for SMS

You can configure Convergence to support one-way SMS.

Configuring One-Way SMS for Convergence

This section describes how to configure one-way SMS so that users can send SMS messages that are 160 characters or less through the Convergence UI. In one-way SMS, senders are unable to receive SMS messages.

Configuring Messaging Server for One-Way SMS

To communicate with Short Message Service Centers (SMSCs), Messaging Server implements an MTA SMS channel which serves as an short message peer-to-peer (SMPP) client.

The following instructions describe how to configure Messaging Server for SMS, using either Messaging Server legacy or unified configuration. The two approaches are treated separately.

Configuring the SMS Add-on Service in the Convergence UI

To configure the SMS Add-On Service in so it displays in Convergence, enable SMS in the Convergence add-on services framework.

1. Enable the SMS add-on service and set parameters for it in the **sms.json** file. The **sms.json** file is in the in the **/var/opt/sun/comms/iwc/config/** directory. See the comments in the file for information on each parameter. The contents of the file at installation are:

   ```
   {
       enabled: true,
       twowaysmsenabled:false,
       channel: "sms-handle",
       folder:"SMS",
       NDNFolder:'INBOX',
       numberhintenabled: true
   }
   ```

   - Set **twowaysmsenabled** to **false**, so it enables one-way SMS.
   - The **channel** parameter requires the name of the MTA channel defined for SMS as part of configuring Messaging Server for SMS.
   - Do not change the default settings of the **folder** and **NDNFolder** parameters.
2. Restart Weblogic Managed Server.

Configuring the Advertising Add-On Service in Convergence

This section describes how to configure the advertising add-on service in Convergence.

About the Advertising Add-On Service

The advertising add-on service makes it possible to display banner ads, text ads, and contextual ads in the Convergence UI. A system administrator can determine the events that trigger new ads and the location within the Convergence UI at which ads are displayed.

Ads can be displayed in:

- A *skyscraper* panel that appears on the right side of the Convergence UI. See "Displaying Ads in a Skyscraper Panel" for more information.
- An *ad* box, a box containing an ad that is located within the email-message viewing area and can be positioned above or below email messages or to the right or left of email messages. See "Displaying Ads in an Ad Box" for more information.

Table 14-2 lists the advertising add-on and configuration files.

Table 14-2 Advertising Configuration and Add-on Files

File Name	Directory	Description
add-ons.properties	**/var/opt/sun/comms/iwc/config/**	Add-ons are added to this file to enable specific services.
advertising.json	**/var/opt/sun/comms/iwc/config/**	Provides file path to plug-in file and allows enabling of Skyscraper and Message Box ad placement, height of ads, and other characteristics in the display area
Plugin.js	*c11n_Home*/**allDomain/js/widget/advertising**	Sample configuration on how to create and configure ads. File can be renamed. Provides call back methods for each type of ad (Skyscraper and Ad Box). You can fill in each callback with code to retrieve ad images, assign them to the innerHTML of the supplied object and return.
Skyscraper.js and **Skyscraper.html**	*c11n_Home*/**allDomain/js/widget/advertising/** and *c11n_Home*/**allDomain/js/widget/advertising/templates/**	Sample configuration that's specific to Skyscraper ads. Provides examples on how to receive events from Convergence, what actions can be taken, controlling splitters, and mechanisms for displaying ads. These configuration files are specific to Skyscraper files and cannot be used in combination with Ad box ads.
Sample Ad Images	**iwc_static/layout/images/ads**	Sample ad images

Configuring Advertising for Convergence

See the **plugin.js**, **Skyscraper.js**, and **Skyscraper.html** samples to create and configure advertising for the Convergence UI.

Enabling the Advertising Add-On Service

To enable the advertising add-on:

1. Make sure that the advertising add-on is enabled in the **add-ons.properties** file; by default, the advertising add-on is enabled. See "add-ons.properties" for more information. The **add-ons.properties** file is located in the **/var/opt/sun/comms/iwc/config/** directory. To enable the advertising add-on, if it is not currently enabled, add it as a value of the *addons* parameter, as in the following example:

   ```
   addons=advertising
   ```

2. Enable the *advertising* add-on service in the **advertising.json** file; by default, the add-on is not enabled. The **advertising.json** file is in the **/var/opt/sun/comms/iwc/config** directory. To enable the *advertising* add-on, set the **enabled** parameter at the top of the file to **true**.

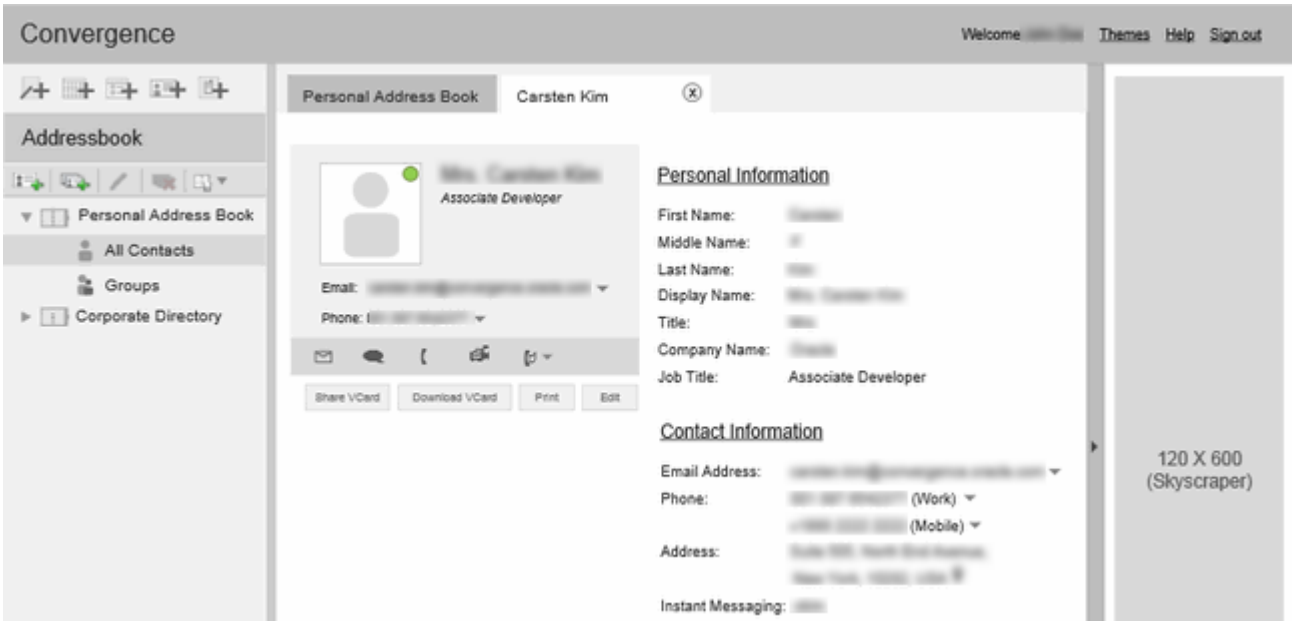
3. Verify that the *c11n_Home* directory exists. If it does not, create it by copying the *c11n_sample* directory. See *Convergence Customization Guide* for more information.
4. Enable the Convergence Server for customization. Use the **iwcadmin** command to set the **client.enablecustomization** parameter to **true**. For example:

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

Displaying Ads in a Skyscraper Panel

Skyscraper panels are displayed on the right side of the Convergence UI, as in the following example:

Figure 14-1 Upper Portion of the Skyscraper Panel in Convergence



To configure an ad to display in a skyscraper panel, you edit the **plugin.js** file. To configure the characteristics of skyscraper panels, you set parameters in the **advertising.json** file.

Parameters for Configuring Skyscraper Panels in the advertising.json File

The **advertising.json** file contains the following parameters for configuring skyscraper panels:

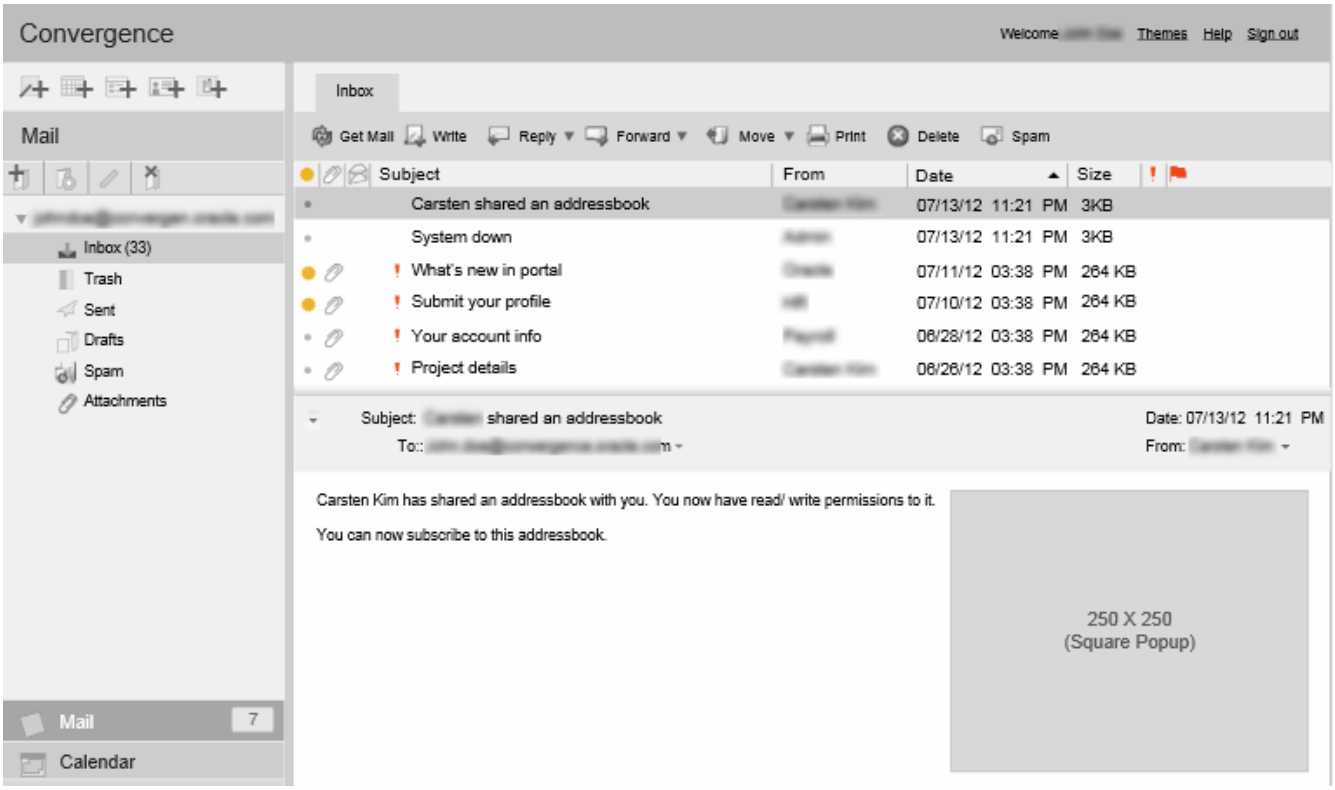
- *enabled*: If set to **true** (the default), a skyscraper panel is added to the right side of the Convergence UI.
- *width*: The width, in pixels, of the skyscraper panel. By default, *width* is set to 160 pixels.
- *closeEnable*: If set to **true** (the default), the user can close the skyscraper panel by clicking a bar tab containing an arrow that appears. Once a user closes the panel, the panel is not displayed again until the user refreshes the Web page, opens Convergence in a new window, tab, or browser, or logs in again.
- *events*: Event parameters:
  - *enabled*: If set to **true**, ads can be displayed for specific events: adtime, mail, or calendar actions.

- *adtime*: The duration of an ad, in seconds. The default is 30 seconds.
- *mail*: An email action, such as opening a new mail tab or clicking through the email message grid can cause a refresh that replaces the current ad with a new ad. you cannot configure which mail actions trigger an ad refresh. You can only determine the frequency of ads, what ad to display, or which events to receive from Convergence (mail or calendar or both).
- *calendar*: User actions involving the calendar can trigger an ad refresh. The calendar actions that can trigger a refresh are configured in the *skyscraper.js* file. Calendar events are similar to mail events in that you cannot configure which calendar actions trigger an ad refresh. You can only determine the frequency of ads, what ad to display, or which events to receive from Convergence (mail or calendar or both).
- *all*: If set to **true**, any event within Convergence can be configured in **advertising.json** to trigger an ad refresh. By default, the *all* parameter is set to **false.**

Displaying Ads in an Ad Box

Boxes containing ads can be displayed above or below an email message, or to the left or right of an email message.

Figure 14-2 Message Ad Box in Convergence



To configure an ad to display in an ad box, you edit the **plugin.js** file. To configure the characteristics of ad boxes, you set parameters in the **advertising.json** file.

The **advertising.json** file contains the following parameters for configuring ad boxes:

- *enabled*: If set to **true** (the default), enables ads in ad boxes.

- *TopAd*: A banner ad displayed above an email message. Parameters:
  - *enabled*: If set to **true** (the default), *TopAd* banner ads are enabled.
  - *height*: The height of the banner ad, in pixels. The default is **60.**
- *RightAd*: An ad box displayed to the right of an email message. Parameters:
  - *enabled*: If set to **true** (the default), enables ad boxes to the right of the message area.
  - *width*: The width of the *RightAd* ad box, in pixels. The default is 250.
  - *height*: The height of the *RightAd* ad box, in pixels. The default is 250.
- *LeftAd*: An ad box displayed to the left of the message area. Parameters:
  - *enabled*: If set to **true**, enables ad boxes to the right of the message area. The default is **false.**
  - *width*: The width of the *LeftAd* ad box,in pixels. The default is 250.
  - *height*: The height of the *LeftAd* ad box,in pixels. The default is 250.
- *BottomAd*: A banner ad displayed below an email message. Parameters:
  - *enabled*: If set to **true** (the default), *BottomAd* banner ads are enabled.
  - *height*: The height of the banner ad, in pixels. The default is **60.**

15

Tuning Oracle WebLogic Server to Enhance Convergence Performance

Oracle Communications Convergence is a Java application bundled into a WAR file that runs inside the Oracle WebLogic server web container. This chapter describes how to optimize the Oracle WebLogic server environment to allow Convergence to deliver the best possible performance.

For general Oracle WebLogic Server performance tuning, see *Oracle Fusion Middleware Tuning Performance of Oracle WebLogic Server Guide*.

Convergence Performance Tuning Overview

Advances in storage, servers, and Java affect 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 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.

For Oracle WebLogic Server:

Use Oracle WebLogic Server's administration browser interface or command-line interface rather than directly editing the **config.xml** file to make changes. The changes do not take effect until the domain instance is restarted. You should restart the Admin Server and Managed Server on which Convergence is deployed.

On Oracle WebLogic Server Administration console, modify the configuration parameters for WebLogic Managed Server on which Convergence is deployed.

Tuning Oracle WebLogic Server Configuration Parameters

Oracle WebLogic Server parameters are set to 10,000 users by assuming the deployment of email, calendar, and address book services.

If you enable the default tuning for Web application in Oracle WebLogic Server, additional tuning is not required. Enable Native Input/Output if it is not enabled.

Configuring Oracle WebLogic Server to Compress Client Files

You can improve server response time by reducing the size of the HTTP response. You can improve server response times by reducing the size of the HTTP response. If you choose to

implement this practice, understand that the server does more work to compress files which might impact the scalability of the server under heavy loads.

To compress files that are sent to client by using the Oracle WebLogic Server, refer to the *Enabling GZIP Compression for Web Applications* section in the *Fusion Middleware Developing Web Applications, Servlets, and JSPs for Oracle WebLogic Server Guide*.

From WebLogic Administration Console, select the Domain Name in which Convergence is deployed and modify the attributes such as **GzipCompressionEnabled**, **GzipCompressionMinCompressionContentLength**, **GzipCompressionContentType** in the **Web Applications** tab.

Enhancing Browser Caching of Static Files for Oracle WebLogic Server

You can configure enhancing browser caching of static files for Oracle WebLogic Server in Oracle HTTP Server.

See the **mod_expires** option in Apache HTTP Server and Third-party Modules in Oracle HTTP Server at: Understanding Oracle HTTP Server Modules.

Tuning the JVM Heap Size

For tuning JVM heap size on Oracle WebLogic Server Administration Console, see *Oracle Fusion Middleware Tuning Performance of Oracle WebLogic Server Guide*.

Generally, set max heap size 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). Reserve space 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 can set the heap size options to:

```
<jvm-options>-Xms3g -Xmx3g</jvm-options>
```

For more information on setting heap size options, see *Oracle Fusion Middleware Administering Server Startup and Shutdown for Oracle WebLogic Server Guide*.

You can update the startManagedWebLogic script with the required Java Heap Size in JAVA_OPTIONS. For example: JAVA_OPTIONS="-Xms3g -Xmx3g" ${JAVA_OPTIONS}.

See *Starting and Stopping Servers* section in the *Administering Server Startup and Shutdown for Oracle WebLogic Server Guide*.

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. Oracle WebLogic Server with Java 8, the following GC options may get better results:

- **-XX:+UseG1GC**: Use the Garbage First (G1) Collector.
- **-XX:MinHeapFreeRatio=10**: Minimum percentage of heap free after GC to avoid expansion.
- **-XX:MaxHeapFreeRatio=50**: Maximum percentage of heap free after GC to avoid shrinking.

- **-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, irrespective of your MaxHeap size.

  For more information about the G1 GC algorithm, see the following Oracle web site:

  http://www.oracle.com/technetwork/tutorials/tutorials-1876574.html

  See the discussion about Java garbage collection settings on the Oracle Technology Network:

  http://www.oracle.com/technetwork/java/javase/tech/g1-intro-jsp-135488.html

Tests show that most of the objects created for Convergence are short-lived, thus benefiting from a larger young generation size.

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, see the following Oracle web site:

http://www.oracle.com/technetwork/java/javase/tech/vmoptions-jsp-140102.html

Monitor your own heap usage with JConsole. See "Monitoring Convergence" for more information.

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 Oracle WebLogic server:

  ```
  jmap -heap java_process_id
  ```

- Monitoring the JVM

  JConsole is a built-in JVM monitoring tool. On the SUT, set the display variable to your local machine and run the following command: jconsole

  See the Jconsole documentation for more information.

- UseConcMarkSweepGC

  The intrepid system administrator may want to consider using **UseConcMarkSweepGC** instead of **UseParallelGC**. See the Java SE VM documentation at the following Oracle web site for more information:

  http://www.oracle.com/technetwork/java/javase/gc-tuning-6-140523.html

- GC 1 Algorithm

See the discussion about Java garbage collection settings on the Oracle Technology Network:

http://www.oracle.com/technetwork/java/javase/tech/g1-intro-jsp-135488.html

- AggressiveOpts

  You can turn on point performance compiler optimizations that are expected to be default in upcoming java releases for better performance using the **AggressiveOpts** option.

  ```
  <jvm-options>-XX:+AggressiveOpts</jvm-options>
  ```

A

ExpiresFilter.java Reference

This appendix shows the contents of the **ExpiresFilter.java** file.

```
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());

    }


}
```

B
Glossary

Account

Information that defines a specific user or user group. This information includes the user name or group name, valid email address or addresses, and how and where email is delivered.

Address

Information in an email message that determines where and how the message must be sent. Addresses are found both in message headers and in message envelopes. Envelope addresses determine how the message gets routed and delivered. Header addresses are present merely for display purposes.

Address Book, Collected Addresses

An optional address book that contains contact information that does not appear in the corporate or personal address books.

Address Book, Corporate

An address book containing the contact information of the members and groups of your organization. The corporate address book contact information is taken from the directory server and cannot be modified by users. The corporate address book is sometimes also called the *corporate directory*.

Address Book, Personal

An address book that users create and maintain containing personal contact information.

davadmin Command-Line Utility

The Oracle Communications Contacts Server and Oracle Communications Calendar Server **davadmin** command-line utility are used to send configuration commands to the Contacts server and Calendar server. See C*ontacts Server System Administrator's Guide* and *Calendar Server System Administrator's Guide* for more information.

imsimta Command-Line Utility

The Oracle Communications Messaging Server **imsimta** command-line utility is used to send configuration commands to the Messaging server. See *Messaging Server System Administrator's Guide* for more information.

iwcadmin Command-Line Utility

The Oracle Communications Convergence **iwcadmin** command-line utility is used to send configuration commands to the Convergence server. See *Convergence System Administrator's Guide* for more information.

Service

One or more capabilities provided by a server, accessed by a client. For example, Convergence provides access to the calendar service, which is provided by Oracle Communications Calendar Server.