

CA On Demand Portal

Administration Guide

Version 2.0



This documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2010 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: Introduction	7
About This Guide	7
Overview of Administrator Controls	7
Chapter 2: Centralized User Management	9
About Centralized User Management	9
Add Portal Users	9
Assign Portal Users to Application Services	10
Add Tenant Administrators	11
Update User Application Fields	11
Update Portal User Information	12
Remove Portal Users from Application Services	13
Deactivate Portal Users	14
Chapter 3: Security	17
About Security	17
Password Requirements and Security	17
Unlock User Accounts	18
Chapter 4: Managing Organizations	19
About Managing Organizations	19
Configure Organization Pages	19
Subscribe to Application Services	20
Billing	20
Edit Billing Accounts	20
Chapter 5: Working with CA Support	23
About Working with CA Support	23
Support Issues	23
Chapter 6: Bulk User Management	25
Options for Bulk User Management	25
ODUM	25
Web Services	25

How to Add Portal Users Using the ODUM Utility	26
Download ODUM.zip	27
Add Proxy Settings to the ODUM Batch File	27
Preparing the Data Input File	28
Configure the Property File	29
Run the ODUM Utility	31
Supported Web Services Reference	31
Using the WSDL URL to Construct Web Service Requests	32
OdumOptions	32
getOdpUser - Retrieve User Information	33
addOdpUser - Add a Portal User	34
updateOdpUser - Modify a Portal User	35
addModifyOdpUser - Add or Modify a Portal User	35
activateOdpUser - Activate a Portal User	36
deactivateOdpUser - Deactivate a Portal User	37

Chapter 7: Federated Single Sign On **39**

About Federated Single Sign On	39
Federated SSO Terminology	39
Supported Federation	40
SAML 2.0 HTTP POST Binding Information	40
SAML Assertion Examples	42

Glossary **45**

Chapter 1: Introduction

This section contains the following topics:

[About This Guide](#) (see page 7)

[Overview of Administrator Controls](#) (see page 7)

About This Guide

The CA On Demand Portal (Portal) delivers an integrated, suite-like access to our IT Management SaaS offerings. The Portal is an intuitive web interface through which our IT Management SaaS offerings are delivered, administered, and secured.

This Administration Guide provides Portal tenant administrators the concepts, processes, and procedures to do the following:

- Manage users and organization Portal pages
- Subscribe to application services
- Use the Portal to create, view, and manage CA Support issues

A *tenant administrator* is a person who administers the CA On Demand Portal for their organization.

To perform the tasks presented in this guide, you must have the appropriate tenant administrator role credentials.

Overview of Administrator Controls

The Portal has the following two main avenues for administrator control and configuration:

- Control Panel
- Portal Layout controls

These functions are all accessible from the control strip on the home page.

Control Panel

The control panel is where you manage your organization, applications, and users. The control panel button is located in the upper right corner of all Portal pages. From the control panel, you can complete tasks such as the following:

- Add Portal users
- Assign users to application services
- Edit user information and application-specific attributes for subscribed services
- Edit your organization information including billing account details
- Manage the pages that all organization members see when they log in to the Portal

Portal Layout controls

These controls let you configure your organization pages for all organization members. You can set which Portal gadgets are shown, and their layout and other style settings. The two layout controls are located in the upper right corner of the Portal home page.

Administrators also have access to two additional Portal areas:

Applications

The Applications tab lets you learn about other CA On Demand application services. You can review product information and request subscriptions to new services.

Billing

The Billing tab lets you view your invoices for CA On Demand services.

Note: Not all CA On Demand accounts are billing enabled.

Chapter 2: Centralized User Management

This section contains the following topics:

[About Centralized User Management](#) (see page 9)

[Add Portal Users](#) (see page 9)

[Assign Portal Users to Application Services](#) (see page 10)

[Add Tenant Administrators](#) (see page 11)

[Update User Application Fields](#) (see page 11)

[Update Portal User Information](#) (see page 12)

[Remove Portal Users from Application Services](#) (see page 13)

[Deactivate Portal Users](#) (see page 14)

About Centralized User Management

With centralized user management, you can add and maintain users in one place: the Portal. Centralized user management allows you to do the following, all from within the Portal:

- Changes to user information are automatically synchronized with all the application services to which you subscribe.
- Control user access to your organization's application services.
- Access key application fields for all On Demand services for efficient management of user application data.

All aspects of centralized user management to control individual user data are handled in the Control Panel of the Portal. To perform bulk user changes, you can use one of the [options for bulk user management](#) (see page 25).

Add Portal Users

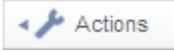
Adding organization members as Portal users is the first step in centralized user management. Once you add people as Portal users, you can assign access to your subscribed application services and then manage user information for those services. Portal users can be added one at a time or in groups using our On Demand User Management utility.

When you add a user, you chose whether to have CA On Demand notify them of their Portal membership. This notification is an automated email that welcomes the new user to the Portal and provides them with their login credentials. Before you begin adding users, determine your notification plan. Some organizations want to send their own custom notification. Others may want their users to access the application services directly and not navigate through the Portal.

This procedure explains how to add a single user.

Note: You can also make [bulk additions](#) (see page 25) using the On Demand User Management utility.

To add a Portal user

1. Log in to the Portal and click  to open the Control Panel.
The Control Panel appears.
2. Click Organizations in the Portal navigation menu.
3. In the list of organizations, click  and select Add User.
The User Information form appears.
4. Complete the User Information fields.
5. If you want an automated email notification to go to the user, select Send Welcome Email to initiate an email to the new user. The email provides login information for the Portal.
6. Click Save.
The user is added to the Portal.

Assign Portal Users to Application Services

You can assign Portal users to the CA On Demand application services to which your organization subscribes. Once you assign a user to a service, the user can access the application through their Portal home page.

To assign a Portal user to an application service

1. Log in to the Portal and click  to open the Control Panel.
2. Click Manage Applications in the Portal navigation menu.
3. In the Manage Applications list, click your organization link.
The Details list appears showing the application services to which your organization subscribes.

4. For each application that you want to grant access to, do the following:
 - a. Click  .
 - b. Click Available for a list of Portal users.
 - c. Locate and select the user you want to assign.
Note: You can select multiple users.
 - d. Click Update Assignments.The user is assigned to the application.

Add Tenant Administrators

Your organization was set up with a single tenant administrator. You can add tenant administrators with assistance from CA Support.

To add a tenant administrator

1. Create the user who will be assigned the tenant administrator role in the Portal.
2. Open a CA Support ticket to request an additional tenant administrator for your organization.
3. In your request, specify the email address of the user whom you want to assign the tenant administrator role.

CA Support processes your request to add a tenant administrator.

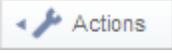
Update User Application Fields

With centralized user management, application user data for all CA On Demand applications is managed from one central location: the Portal.

Once you assign a user to an application service, you can set and update their application-specific attributes from the Control Panel. Unique data can be set for each instance of each service to which the user is assigned. All application user data is stored in the related application service. The Portal queries the application service and displays the data.

Note: This feature is only accessible to administrators. Organization members cannot change view or change this data in the Portal. Application fields are only accessed through the Control Panel. The My Account page does not contain these fields.

To update user application fields

1. Click  to open the Control Panel.
2. Click Users in the Portal navigation menu.
3. Locate the user that you want to update.
4. Click  and select Edit.
5. In the User pane, under Application Fields, select the application for which you want to edit user data.

The application name appears at the center of the Users screen.

6. Select the instance you want to edit and click  .
The attributes for the selected instance appear.
7. Make the desired updates and click Save.

The updates are saved in the specified application instance.

Update Portal User Information

Once you add a Portal user, you can update their Portal user information and settings. This user data consists of the following three types:

- **User Information.** Basic Portal data including login credentials.
- **Identification.** Additional contact information. This data is purely informational and does not drive any Portal functionality.
- **Miscellaneous.** Notifications and display settings.

As the administrator, you can change the settings for all your organization members. Users also have access to their own account from the My Account link.

To update Portal User Information

1. Click  to open the Control Panel.
2. Click Users in the Portal navigation menu.
3. Locate the user you want to update.
4. Click  and select Edit.

5. Select the User Information link you want to update.
6. Depending on the link selected, do the following:
 - **Details.** Update the user name, email address, or job title.
 - **Password.** Change the user password.
 - **Roles.** View the role assigned to the user.
7. Click Save.

The updates to the User Information are saved.

To update Miscellaneous settings

1. Click  to open the Control Panel.
2. Click Users in the Portal navigation menu.
3. Locate the user you want to update.
4. Click  and select Edit.
5. Select the Miscellaneous link you want to update.
6. Depending on the link selected, do the following:
 - **Announcements.** Select how alerts and announcements are delivered.
 - **Display Settings.** Set the display language, user time zone, and Portal greeting message.
7. Click Save.

The updates to the Miscellaneous settings are saved.

Remove Portal Users from Application Services

You can remove a user from an application service. Once access is withdrawn, the user no longer has access to the service. With this procedure, you make selective changes to a user's access to your organization's application services.

Note: You can also deactivate users, which removes all access rights to all services and to the Portal itself.

To remove a Portal user from an application service

1. Log in to the Portal and click  to open the Control Panel.
2. Click Manage Applications in the Portal navigation menu.

3. In the Manage Applications list, click your organization link.

The Details list appears showing the application services to which your organization subscribes.

4. For each application that you want to withdraw access to, do the following:

- a. Click .

The list of current users assigned to the application appears.

- b. Locate and clear the checkbox for the user that you want to remove from the service.

Note: You can remove multiple users.

- c. Click Update Assignments.

The user's access to the application is withdrawn.

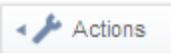
Deactivate Portal Users

A deactivated user cannot log in to the Portal. When a user is deactivated, he is simultaneously deactivated from all application services to which he is assigned.

The user record remains in the database and can be reactivated at a later time. You cannot delete user records.

Note: You can also selective [remove access to individual application services](#) (see page 13).

To deactivate a user

1. Click  to open the Control Panel.
2. Click Users in the Portal navigation menu.
3. Locate the user you want to deactivate.
4. Click  and select Deactivate.

A dialog appears asking you to confirm your action.

5. Click Yes.

The user is deactivated in the Portal and in all applications to which he is assigned.

To activate a user

1. Click  to open the Control Panel.
2. Click Users in the Portal navigation menu.

3. Locate deactivated users with Advanced Search, by selecting No in the Active drop-down list.

4. For the user you want to activate, click  and select Activate.

The user is activated in the Portal and in all applications to which he is assigned.

Note: The user's password must be reset before they can access the Portal.

Chapter 3: Security

This section contains the following topics:

[About Security](#) (see page 17)

[Password Requirements and Security](#) (see page 17)

[Unlock User Accounts](#) (see page 18)

About Security

The CA On Demand security architecture is comprised of SAS70 Type II controls and security measures across facility, network, and server infrastructure. You can read more about these security measures in the *CA Clarity On Demand Technical Overview* available on CA Support Online.

The Portal provides login security through user authentication controls. The Portal supports SSO for the Portal and all CA On Demand application services. Login is controlled through user name and password authentication.

Password Requirements and Security

Password construction and management have the following requirements:

- **Single-use password.** New users and users who request password help receive a single-use password which must be changed the first time they log in. Passwords are changed on the My Account screen.
- **Password rules.** The following rules apply to the construction of all passwords:
 - The password cannot be a word found in a dictionary.
 - The password must be at least eight characters long.
 - You cannot reuse any of your previous 24 passwords.
- **Expiration.** Passwords expire every 13 weeks (91 days).
- **Lockout.** Users are locked out after three failed login attempts. Only an administrator can unlock accounts.
- **Lockout duration.** Locked accounts remain locked for a period of one hour.
- **Session Timeout.** Users are logged out after 30 minutes of inactivity.

Note: Some of these password requirements can be modified with assistance from CA Support. To request changes, open a CA Support ticket.

Unlock User Accounts

If a user has three failed sign-in attempts, their account is locked. Once locked, the user cannot log in and no other changes can be made to the account until it is unlocked. A locked user is also deactivated from all application services to which he is assigned.

Only Portal administrators can unlock a user account.

Note: Accounts remain locked for a period of one hour. After that time, the user can reattempt to log in.

To unlock a user account

1. Click  to open the Control Panel.
2. Click Users in the Portal navigation menu.
3. Using the basic or advanced Search to locate the desired user record.
4. Click  and select Edit.

The record appears with an account locked warning at the bottom right.

5. Click Unlock.

The account is unlocked and access to the Portal and all assigned applications services is restored.

Chapter 4: Managing Organizations

This section contains the following topics:

[About Managing Organizations](#) (see page 19)

[Configure Organization Pages](#) (see page 19)

[Subscribe to Application Services](#) (see page 20)

About Managing Organizations

Managing your organization includes the following tasks:

- Configuring the content and layout of the Portal
- Subscribing to application services

Configure Organization Pages

This topic covers configuration options and tasks for setting up your organization's pages in the Portal. These settings affect how all organization members see and interact with content in the Portal.

The Portal displays applets, named gadgets. These gadgets are windows of functionality and information and you can choose which gadgets your organization members see in the Portal. Some of the gadgets are specific to your organization's application services. For these gadgets, users must be assigned to the service to have the service information display.

You can also control the general layout and style of the gadgets which you chose to display.

To configure organization pages

1. Log in to the Portal and navigate to the home page.
2. Click Add Gadget.
The Add Gadget control window appears.
3. For each gadget you want to add to your organization pages, click Add.
Added gadgets appear in the home page.
4. Close the Add Gadget window.

5. For each gadget that you want to remove from your organization pages, click the X in the upper right of the gadget. Removed gadgets disappear from the home page; they can be added back at any time.

Note: If the gadget controls are not visible, click  to switch on the edit controls.

6. Click Layout Template.
The Layout dialog appears.
7. Select a layout and click Save.
The home page appears using the selected layout.

Subscribe to Application Services

The Portal is your gateway to all CA On Demand application services. Product information about these services is available from the Portal. When you are ready to request a subscription to a new service for your organization, you can enter that request directly from within the Portal.

To subscribe to application services

1. Log in to the Portal and click the Applications tab.
2. Review the available product information.
3. To request a subscription order for a service, click Request Order.

Once you confirm your interest, your request is sent to CA Technologies and a representative contacts you to complete your subscription.

Billing

Your organization's CA On Demand billing information is available from the Portal. The Billing tab lets administrators review any existing invoices for their subscribed services.

Note: Your Portal environment may not have all of the features discussed in this topic.

Edit Billing Accounts

Tenant administrators can edit the details of their organization's billing account. These details include the billing contact's name and mailing address.

To edit a billing account

1. Log in to the Portal and click  to open the Control Panel.
2. Click Billing Accounts in the Portal navigation menu.
3. Click the Edit link for your organization.
4. Update the fields as necessary.
5. Click Save.

The billing account is updated.

Chapter 5: Working with CA Support

This section contains the following topics:

[About Working with CA Support](#) (see page 23)

[Support Issues](#) (see page 23)

About Working with CA Support

You can log a Support issue directly from the Portal home page. The Portal supports SSO with CA Support Online, so your Portal login credentials give you automatic access to our support site.

Note: Your email address must be the same for both the Portal and CA Support Online for SSO between these applications to work.

The user that is logged on to the Portal is the user that can access the CA Links resources through SSO. For example, you are logged on to the Portal as bill.smith@xyz.com. If you have a CA Support account under that same email address, you can access CA Support directly from the CA Links section on the home page using SSO.

Support Issues

As an administrator, you can manage most Portal functions, but there are a few tasks that require assistance from CA Support.

For a tenant administrator, these tasks include things such as the following:

- Replacing the CA Technologies logo with your own custom logo
- Requesting the tenant administrator role for an additional user

Chapter 6: Bulk User Management

This section contains the following topics:

[Options for Bulk User Management](#) (see page 25)

[How to Add Portal Users Using the ODUM Utility](#) (see page 26)

[Supported Web Services Reference](#) (see page 31)

Options for Bulk User Management

CA On Demand provides two options for making bulk changes to user accounts:

- On Demand User Management utility (ODUM)
- Web Services

Both of these solutions let you make bulk changes to add or modify users and grant or withdraw access to any of the CA On Demand application services. These changes automatically percolate down to the application services, creating the defined user data in the named service.

ODUM

ODUM is a utility for making bulk edits to Portal users. ODUM is a lightweight Java-based client that can be installed in Windows or UNIX and does not require any programming or development work to use.

The utility uses an XML or CSV data file, which you prepare by following a defined format, containing your organization's user information. The utility is run from a command line and shows the users being added to the application instance. Once the ODUM upload has completed, you can review the user changes through the Portal.

This utility is recommended for the initial loading of Portal users for organizations with many users, and who want a simple solution that does not require additional development.

Web Services

The Portal uses web services for data exchange. These web services are application programming interfaces (API) or web APIs that are accessed over the HTTPS protocol. Your organization can use these web services to manage Portal users, including providing access to CA On Demand application services. The ODUM utility is built on these web services.

Using web services is recommended for organizations who want to integrate their internal user data stores to automate ongoing Portal user management. This method requires custom programming by your organization.

How to Add Portal Users Using the ODUM Utility

Understanding the process for adding Portal users in bulk with the ODUM utility helps you better plan and prepare for this task. The process involves several steps, including prerequisites, configuration, and user data set up.

Important: ODUM v2.0 or above is required. If you use an earlier version of the utility, your bulk changes will fail. You can verify the version number of the utility by looking in the README.txt file that is part of the download. The version number appears at the top of the document.

To use the ODUM utility to make bulk changes to Portal users, do the following:

1. Verify that JAVA JRE 6.0 or later is installed on the client computer that will run the utility.
2. Add the JAVA_HOME environment variable with a value of the full path to the JRE installation. Refer to the online help for your operating system for information about how to add an environment variable.
3. [Download and unzip the latest release of ODUM](#) (see page 27). ODUM is packaged in a Zip file containing the utility and all supporting files. The Zip file is available for download from the Portal, in the Downloads gadget.

Note: ODUM v2.0 or above is required.

4. If you are using ODUM from behind a proxy server, modify the ODUM batch file to [add your proxy settings](#) (see page 27).
5. Determine which data input file format you will use. The data input file contains the source Portal user data. ODUM works with XML and CSV data input files. While the CSV data is simpler to set up, we recommend that you use XML. This format lets you create application-specific data so you can register additional user data that is particular to the application service. Samples for each format are provided with the ODUM utility.
6. [Preparing your data input file](#) (see page 28). Use the supplied sampleuserdata file as a guide to create your data input file.
7. [Configure the Property File](#) (see page 29). The Property File contains property definitions which the ODUM utility uses to execute your user data updates.
8. [Run the ODUM utility](#) (see page 31), review the error log and make any required changes to resolve, and rerun ODUM. We recommend that you start with a test run using only a subset of your data input file. By running a test, you confirm that the Property file, data file, and proxy settings are working as expected.

Download ODUM.zip

The ODUM utility is available in a Zip file which you can download from the Portal. Make sure to download the latest version of the utility and the supporting files.

Note: Only Portal administrators have access to the ODUM download.

To download ODUM.zip

1. Login to the Portal as an administrator and navigated to the home page for your organization.
2. Locate the Downloads gadget at the lower left of the screen.
3. Click ODUM.zip to initiate the download.
4. Save the ODUM.zip file to your computer.
5. Extract the ODUM files to the desired location on your computer.

The ODUM utility and all supporting files are downloaded to your computer.

Add Proxy Settings to the ODUM Batch File

The ODUM utility communicates with CA On Demand Portal web services. If you are using the ODUM utility from behind a proxy server (firewall), modify the ODUM batch file to add your proxy settings. You can configure the settings with or without requiring authentication, for either HTTP or HTTPS protocol.

To complete this procedure, you must have already downloaded and extracted the ODUM utility and supporting files.

To add HTTP or HTTPS proxy settings to the ODUM batch file

1. Locate the ODUM batch file odum.bat. This file is in the bin folder.
2. Edit the odum.bat file to add your proxy host and port settings using one of the following:
 - To access the web proxy over HTTP:
-Dhttp.proxyHost=<proxy host>
-Dhttp.proxyPort=<proxy port>
 - To access the web proxy over HTTPS:
-Dhttps.proxyHost=<proxy host>
-Dhttps.proxyPort=<proxy port>

These settings are added to the batch file immediately following @java.

3. If proxy authentication is required, then additionally configure the proxy user ID and password using one of the following:
 - To access the web proxy over HTTP:
-Dhttp.proxyUser=<network user ID>
-Dhttp.proxyPassword=<network password>
 - To access the web proxy over HTTPS:
-Dhttps.proxyUser=<network user ID>
-Dhttps.proxyPassword=<network password>
4. Save and close the file.

The proxy settings are added to the ODUM batch file.

Example ODUM Batch File

Add proxy settings to the ODUM batch file to allow ODUM to communicate with the On Demand Portal web services through an HTTPS proxy server. This proxy server requires authentication. For this example, we use the following definitions:

- proxyHost = GenServer05
- proxyPort = 8080
- proxyUser = SMITHJ25
- proxyPassword = passW0rd

The added proxy settings are shown in bold in the following odum.bat sample:

```
@java -Dhttps.proxyHost=GenServer25 -Dhttps.proxyPort=8080
-Dhttps.proxyUser=SMITHJ25 -Dhttps.proxyPassword=passW0rd
-Dlog4j.configuration=..\lib\log4j.properties -cp
"%dp0/..\lib/axis.jar;%dp0/..\lib/commons-beanutils.jar;%dp0/..\lib/odum-parse
r.jar;%dp0/..\lib/commons-discovery.jar;%dp0/..\lib/commons-logging.jar;%dp0/
..\lib/jaxrpc.jar;%dp0/..\lib/log4j.jar;%dp0/..\lib/odum.jar;%dp0/..\lib/odp-cl
ient.jar;%dp0/..\lib/saaj-api.jar;%dp0/..\lib/wsd14.jar;%dp0/..\lib/ws-util.j
ar;" com.ca.odp.odum.Odum %*
```

Preparing the Data Input File

The data input file contains all the information about the Portal users that you are adding or modifying. The file includes basic Portal user information, such as name and email address, and application details such as access rights to application services. If you are using an XML data input file, you can also create additional application-specific data.

ODUM works with XML and CSV data input files. While the CSV data is simpler to set up, we recommend that you use XML. Samples for each format are provided with the ODUM utility. The ODUM README.txt contains information about how to set up a CSV data input file.

To prepare an XML data input file, use the following resources provided with the ODUM utility:

sampleuserdata.xml

Illustrates a sample XML data input file showing how to add, deactivate, and activate users. This file also shows you how to assign application access rights and record additional application-specific data. Use an XML editor to edit a copy of this file to create your data input file.

Odum.xsd

Provides the schema for the XML data input file.

The following table provides some additional definition for some of the parameters in the XML data input file:

Parameter	Detail	Values
operation	Defines what action to take on the user.	add modify deactivate activate
AppInstances	<p>Defines the applications to grant access to for the user. You can list multiple applications, separated by commas.</p> <p>Note: If you modify an existing user and do not list an application to which the user previously had access, then that access is revoked.</p>	Valid values are found in the Portal Control Panel under Manage Applications. All values listed in the APPLICATION column are valid for this parameter.

Make note of the full path to the completed file. You add this information to the Property file before running the ODUM utility.

Configure the Property File

The Property File contains property definitions which the ODUM utility uses to execute your user data updates. These properties identify critical information such as the location of your data input file and your administrator credentials.

To complete this procedure, you must have already downloaded and extracted the ODUM utility and supporting files.

Note: You can run the utility in a way that does not require the Property file. However this method only allows for a CSV data input file.

To configure the Property File

1. Open the sample.properties file that came with the ODUM utility.
2. Save a copy of the file under a new name as *name*.properties.

Example: aaa.properties

3. Edit the new file to record the following information, making sure to remove the Comment marks before the properties you enter. The sample.properties file provides full detail on each parameter.

input

Identifies the location of the input data file.

userid

Identifies the email address of the Portal administrator running ODUM.

password

Identifies the password of the Portal administrator running ODUM.

tenant_name

Identifies the organization name of the users you are modifying.

sendwelcomeemail {TRUE | FALSE}

Specifies whether the generic CA On Demand welcome email is sent to new users.

force_password_reset {TRUE | FALSE}

Specifies if new users are forced to change their password on initial login.

input_format {CSV | XML}

Specifies the format of the input data file.

4. Save and close the file.

The Property file is configured.

Example Properties File

In this example, the .properties file is configured for the administrator of CompanyX, and identifies the XML input data file to be used with ODUM. The bolded text shows the values provided for the parameters.

```
input=C:\\Program Files\\CA\\Clarity\\ODUM\\bin\\ComapnyXClarityUsers.xml
userid=admin@companyx.com
password=admin1234
tenant_name=CompanyX
sendwelcomeemail=false
input_format=xml
```

Run the ODUM Utility

Before you run the ODUM utility to make bulk changes to Portal users, you must have completed all the prior steps in the process [How to Add Portal Users Using the ODUM Utility](#) (see page 26).

This procedure describes how to run the ODUM utility using a Property file. We recommend this method. The ODUM README.txt contains information about how to run ODUM without a Property file.

Important: The data input file must be in the location specified in the Property file for the utility to execute correctly.

To run the ODUM utility with a Property File

1. Open a Command Prompt and change directories to navigate to the bin folder that contains the odum.bat file.
2. Run ODUM by typing the following:
`ODUM -propertyfile full_path_to_property_file`
3. Review the results shown in the Command Prompt window for errors, make any necessary corrections and rerun ODUM.

Your bulk user changes are complete.

Supported Web Services Reference

The Portal web service API provides the following web services:

getOdpUser

Retrieves user information from the Portal.

addOdpUser

Adds the user to the Portal.

updateOdpUser

Updates the user details on the Portal.

addModifyOdpUser

Adds or modifies a user to the Portal.

activateOdpUser

Grants access for a user to the Portal and all application services.

deactivateOdpUser

Withdraws access for a user to the Portal and all application services.

Using the WSDL URL to Construct Web Service Requests

You construct web service xml requests by using a web service client, such as soapUI and the Portal Web Services Description Language (WSDL) URL. The WSDL URL is as follows:

`https://ondemand.ca.com/tunnel-web/secure/axis/Portlet_Odp_OdpUserService?wsdl`

Log in to the WSDL using your Portal user name and password credentials.

OdumOptions

The requests that you send to the Portal web APIs to add or modify users include the following options:

tenant_name

The name of the tenant to which all the users will belong. If not specified, the tenant of the logged-in user is used. If the logged-in user belongs to multiple tenants AND tenant name is not specified, then all add operations fail.

sendwelcomeemail

If set to true, a welcome email is sent to all the users that were added to the system during this interaction.

Default: False

new_user_default_password

If specified, all users added during the interaction have this value as the password. If not specified, new users are assigned a random password by the system.

additiveAppInstList

If set to true, then the list of application instance name specified (in update operations) is considered additive; access is granted to the specified application instances in addition to the ones the user already has. If set to false, then the list is considered exhaustive; so (during an update operation) the user is granted access only to the application instances specified and any additional access the user might already have are revoked.

Default: True

forcePasswordReset

If set to true, all newly added users are forced to change their password on initial login.

Default: False

getOdpUser - Retrieve User Information

The getOdpUser web service retrieves user information for a single Portal user. Your request specifies the user's identification. The web service returns all the details of the user, including the application instances to which the user has access.

Requests to the getOdpUser web service contain the following parameters:

emailAddress

Provides the email address of the user to retrieve.

tenantName

Provides the tenant name to which the user belongs.

The following error conditions result in a null response:

- User not found
- Incomplete information passed (when either email address or user id is specified)
- User does not belong to the specified tenant

Example - getOdpUser request

This example requests the user information for a user with the email address john@xyz.com who belongs to the tenant organization xyz.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:http.service.odp.ondemand.ca.com"
xmlns:odum="http://odum.service.odp.ondemand.ca.com">
  <soapenv:Header/>
  <soapenv:Body>
    <urn:getUserRequest>
      <odum:emailAddress>john@xyz.com</odum:emailAddress>
      <odum:tenantName>xyz</odum:tenantName>
    </urn:getUserRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Example - getOdpUser response

This example response provides the user details for john@xyz for the xyz tenant organization.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Body>
    <getOdpUserReturn xmlns="urn:http.service.odp.ondemand.ca.com">
      <active>true</active>
      <addresses xsi:nil="true"/>
      <appInstances>
```

```
        <item xmlns="">Testing</item>
    </appInstances>
    <emailAddress> john@xyz.com </emailAddress>
    <firstName>John</firstName>
    <greeting xsi:nil="true"/>
    <jobTitle xsi:nil="true"/>
    <languageId>en_US</languageId>
    <lastName>Smith</lastName>
    <lockout>>false</lockout>
    <middleName xsi:nil="true"/>
    <modifiedDate>2010-08-11T18:13:17.409Z</modifiedDate>
    <phones xsi:nil="true"/>
    <prefix xsi:nil="true"/>
    <serviceDeskDetails xsi:nil="true"/>
    <suffix xsi:nil="true"/>
    <tenantName>xyz</tenantName>
    <timezone>UTC</timezone>
    <userId>10954</userId>
</getOdpUserReturn>
</soapenv:Body>
</soapenv:Envelope>
```

addOdpUser - Add a Portal User

The addOdpUser web service adds a single Portal user. Your request specifies the OdumOptions and user details. The web service returns all the details of the added user.

Requests to the addOdpUser web service contain the following parameters:

OdumOptions

Sets key properties for the user. See [OdumOptions](#) (see page 32) for details.

User Details

Includes basic user information and what applications the user is granted access to.

The following error conditions result in a null response:

- User email address already exists
- User id was specified
- User save failed
- Incomplete information passed
- Invalid App Instance Name specified
- Tenant name not specified (and logged-in user belongs to multiple tenants)

updateOdpUser - Modify a Portal User

The updateOdpUser web service modifies a single Portal user. Your request specifies the OdumOptions and user details. The web service returns all the details of the modified user.

Requests to the updateOdpUser web service contain the following parameters:

OdumOptions

Sets key properties for the user. See [OdumOptions](#) (see page 32) for details.

User Details

Includes the user details to modify. If any of the fields are not specified, those fields retain their original value and are not modified. If an email address is specified (and not the user id), then the user with the specified email address is modified.

If the user id is specified and the corresponding user has an email address different from the one specified in the user details, then the email address is updated.

The following error conditions result in a null response:

- User does not exist
- Updated user email address exists for another user
- User update failed
- Incomplete information passed
- Invalid App Instance Name specified
- User does not belong to the Tenant specified in the OdumOptions

addModifyOdpUser - Add or Modify a Portal User

The addModifyOdpUser web service adds or modifies a single Portal user. Your request specifies the OdumOptions and user details. The web service returns all the details of the modified user.

Requests to the addModifyOdpUser web service contain the following parameters:

OdumOptions

Sets key properties for the user. See [OdumOptions](#) (see page 32) for details.

User Details

Includes the user details to add or modify, determined as follows:

- **Add.** Email address is specified, and that email address does not exist in the system.
- **Modify.**
 - a. User id field is specified
 - b. Email address is specified, and that email address exists in the system

For modify requests, if any of the fields are not specified, those fields retain their original value and are not modified. If an email address is specified (and not the user id), then the user with the specified email address is modified.

If the user id is specified and the corresponding user has an email address different from the one specified in the user details, then the email address is updated.

The following error conditions result in a null response:

- User id does not exist
- Updated user email address exists for another user
- User save failed
- Incomplete information passed
- Invalid App Instance Name specified
- Tenant name not specified (if logged-in user belongs to multiple tenants and the data is interpreted as an add user)
- User does not belong to the Tenant specified in the OdumOptions

activateOdpUser - Activate a Portal User

The activateOdpUser web service grants access for a user to the Portal and all application services. The web service returns all the details of the activated user.

Requests to the activateOdpUser web service contain the following parameters:

OdumOptions

Sets key properties for the user. See [OdumOptions](#) (see page 32) for details.

emailAddress

Provides the email address of the user to retrieve.

tenantName

Provides the tenant name to which the user belongs.

The following error conditions result in a null response:

- User does not exist
- User activation failed
- Incomplete information passed
- Incorrect information passed (when a user exists with the specified user id, but has a different email address than specified in the input)
- The user does not belong to the tenant specified in the OdumOptions

deactivateOdpUser - Deactivate a Portal User

The deactivateOdpUser web service withdraws access for a user to the Portal and all application services. The web service returns all the details of the deactivated user.

Requests to the deactivateOdpUser web service contain the following parameters:

emailAddress

Provides the email address of the user to retrieve.

tenantName

Provides the tenant name to which the user belongs.

The following error conditions result in a null response:

- User does not exist
- User activation failed
- Incomplete information passed
- The user does not belong to the tenant specified.

Chapter 7: Federated Single Sign On

This section contains the following topics:

[About Federated Single Sign On](#) (see page 39)

[Federated SSO Terminology](#) (see page 39)

[Supported Federation](#) (see page 40)

[SAML 2.0 HTTP POST Binding Information](#) (see page 40)

[SAML Assertion Examples](#) (see page 42)

About Federated Single Sign On

The Federated Single Sign On (SSO) integration allows customers to create a trusted relationship with the CA On Demand network. This relationship delivers the following benefits:

- **Seamless integration between networks and environments.** Users can move easily between their intranet, and the various regions of the CA On Demand environment.
- **Simplified password management.** Customers do not have to manage their users' passwords separately for any of the CA On Demand application services because they are handled by their existing user management system.
- **CA Supported.** Support is handled by a dedicated CA On Demand delivery organization.

Detailed technical information about implementing Federated SSO is presented in the following topics. As the first step in your implementation, contact your CA Technologies representative. As part of the process, there is an exchange of information pertaining to Identity Provider (the customer) and Service Provider (the Portal) configuration details.

Federated SSO Terminology

The following terminology may be helpful to you in learning about implementing Federated SSO for the Portal.

Assertion

An Assertion is the XML packet that contains the security information that is sent between the Identity and Service Provider.

Identity Provider (IdP)

An Identity Provider is a producer of assertions. In our case, this is the CA On Demand customer.

Service Provider (SP)

A Service Provider is a consumer of assertions. In our case, this is the On Demand Portal.

SAML (Security Assertion Markup Language)

SAML is an XML-based standard for exchanging authentication and authorization data between security domains.

SAML Binding

A SAML binding is a mapping of a SAML protocol message onto standard messaging formats and communications protocols. For example, the SAML SOAP binding specifies how a SAML message is encapsulated in a SOAP envelope, which itself is bound to an HTTP message.

SAML profiles

A SAML profile describes in detail how SAML assertions, protocols, and bindings combine to support a defined use case. The most used SAML profile is the Web Browser SSO Profile.

Supported Federation

There are many different ways to handle Federated SSO. CA On Demand supports a single method. In the future, additional methods may be enabled depending on customer demand and resource availability.

CA On Demand supports federation as follows:

Version

SAML 2.0

Binding

HTTP POST Binding

Profile

Web Browser SSO Profile

SAML 2.0 HTTP POST Binding Information

This section contains the information to exchange between the Identify Provider and the Service Provider to establish a Federated SSO relationship.

Configuration

The following configuration points are implementation-specific and are agreed to during the implementation:

- Service Provider ID: The ID that is shared between your organization and CA On Demand to represent the Service Provider (CA)
- Identity Provider ID: The ID that is shared between your organization and CA On Demand to represent the Identity Provider (Customer)
- Encryption (Name ID or Assertion): Encryption is optional but highly recommended
- Signature Processing: Recommended as it is more secure
- Skew Time: The amount of time in seconds that is different between the Service Provider and Identity Provider systems.

Set Parameters

CA On Demand sets the following configuration points:

- SAML Version: SAML 2.0
- SAML Binding: HTTP POST Binding
- SAML Profile: Web Browser SSO Profile
- Assertion Consumer Service:
<https://fedssso.ondemand.ca.com/affwebservice/public/saml2assertionconsumer/>
- User IDs:
 - CA On Demand uses the Email Address unique identifier for the user. If the email address is already used as user ID, it can simply be passed
 - If Email Address is not used as user ID, then you set a Name ID with the following settings:
 - Name ID Format: Set as Email Address
 - Name ID Type: Set to User Attribute
 - Name ID Field Attribute Name: Set to mail
- Assertion Validity Duration: The timespan that the assertion is valid for
- If your organization wants Encryption for (Name ID or Assertion)
 - Encryption Block: Valid choices tripledes, aes-128 & aes-256
 - Key Algorithm: Valid choices are rsa-r15 and rsa-oaep

Parameters from Identity Provider

You provide the following configuration points to CA On Demand:

- Identity Provider SSO Consumer Web Service URL: This URL is the site that the Identity Provider sends the Assertion to
- Signature Processing Issue DN: Specifies the distinguished name of the issuer of the certificate
- Signature Processing Certification: Certification that we store in our key store. Certification gives us the Signature Processing Serial Number
- Identity Provider SSO Service URL: The Identity Provider's Web Service used in case of time-outs, log-outs, and Service Provider Initiated SSO

SAML Assertion Examples

There are two different options for SAML assertions:

1. **Pass Email.** This is the recommended option. The user's email address is passed as the "NameID"
2. **Pass Attribute.** If passing the email address as the "NameID" is not acceptable, then it can be added as an attribute. If this case is used, more configurations are necessary

Example - Pass Email in NameID

```

<Response
Destination="https://ondemand.ca.com/affwebservices/public/saml2assertionconsumer
/" ID="_3c4ba8284eb2bae5c924cd819a47b1877ac
a" IssueInstant="2009-07-17T02:30:13Z" Version="2.0"
xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <ns1:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion">idp.demo</ns1:Issu
er>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </Status>
  <ns2:Assertion ID="_8e60ee2c8854a69b03db2e234e9c023e2a98"
IssueInstant="2009-07-17T02:30:13Z" Version="2.0" xmlns:ns2="urn:oasis:names:tc:
SAML:2.0:assertion">
    <ns2:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp.demo</ns2:Issuer>
    <ns2:Subject>
      <ns2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">testuser@example.
com</ns2:NameID>
      <ns2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <ns2:SubjectConfirmationData NotOnOrAfter="2009-07-17T02:31:43Z"
Recipient="https://ondemand.ca.com/affwebservices/public/saml
2assertionconsumer/">
        </ns2:SubjectConfirmation>
      </ns2:Subject>
      <ns2:Conditions NotBefore="2009-07-17T02:29:43Z"
NotOnOrAfter="2009-07-17T02:31:43Z">
        <ns2:AudienceRestriction>
          <ns2:Audience>sp.ondemand.ca</ns2:Audience>
        </ns2:AudienceRestriction>
      </ns2:Conditions>
      <ns2:AuthnStatement AuthnInstant="2009-07-17T01:52:27Z"
SessionIndex="ey2QazXHqzLqRwLAiMV629I49oU=mvQs2g=="
SessionNotOnOrAfter="2009-07-17T02:31:43Z">
        <ns2:AuthnContext>
          <ns2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</ns2:Au
thnContextClassRef>
        </ns2:AuthnContext>
      </ns2:AuthnStatement>
    </ns2:Assertion>
  </Response>

```

Example - Pass Email in an Attribute

```
<Response
Destination="https://rwrh8.ca.com/affwebservices/public/saml2assertionconsumer/"
ID="_869db60f4d205f0c51210637cdd3ad54ec55" IssueInstant="2010-08-05T22:42:31Z"
Version="2.0" xmlns="urn:oasis:names:tc:SAML:2.0:protocol">
  <ns1:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:ns1="urn:oasis:names:tc:SAML:2.0:assertion">idp.demo</ns1:Issuer>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </Status>
  <ns2:Assertion ID="_d054e815d4ebc522f3ee8af0fff75fef45fa"
IssueInstant="2010-08-05T22:42:31Z" Version="2.0"
xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
    <ns2:Issuer
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp.demo</ns2:Issuer>
    <ns2:Subject>
      <ns2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">test@ca.com</ns2:
NameID>
      <ns2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <ns2:SubjectConfirmationData NotOnOrAfter="2010-08-05T22:55:51Z"
Recipient="https://rwrh8.ca.com/affwebservices/public/saml2assertionconsumer/">
        </ns2:SubjectConfirmation>
      </ns2:Subject>
      <ns2:Conditions NotBefore="2010-08-05T22:37:31Z"
NotOnOrAfter="2010-08-05T22:55:51Z">
        <ns2:AudienceRestriction>
          <ns2:Audience>sp.demo</ns2:Audience>
        </ns2:AudienceRestriction>
      </ns2:Conditions>
      <ns2:AuthnStatement AuthnInstant="2010-08-05T22:32:09Z"
SessionIndex="j0znIAkllqJNL1zHRFr+MLPa0AE=z3RsNQ=="
SessionNotOnOrAfter="2010-08-05T22:55:51Z">
        <ns2:AuthnContext>
          <ns2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</ns2:Au
thnContextClassRef>
        </ns2:AuthnContext>
      </ns2:AuthnStatement>
      <ns2:AttributeStatement>
        <ns2:Attribute Name="name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
          <ns2:AttributeValue>test@ca.com</ns2:AttributeValue>
        </ns2:Attribute>
      </ns2:AttributeStatement>
    </ns2:Assertion>
  </Response>
```

Glossary

Instance

An *instance* is a particular application service with its own data store. Most CA On Demand application services are available to customers in a production and non production environment. For example, CA Clarity On Demand can be configured for customers with a production, development, and test instance.

Organization

An *organization* is a business entity that contracts with CA Technologies for CA On Demand Portal services.

Tenant Administrator

A *tenant administrator* is a person who administers the CA On Demand Portal for their organization.