



# **Cloud Services Identity Management Administration Guide Version 18**

October 2021



# Contents

---

About the Cloud Administration Identity Management Administration Guide.....	5
About OIM (Oracle Identity Management) and IDCS (Identity Cloud Service) .....	5
Manage Personal Information in Cloud Administration.....	5
About Consent Notices.....	5
About Personal Information.....	6
Cookies Usage in Cloud Administration.....	6
Your Responsibilities.....	6
Personal Information (PI) Data in Cloud Administration.....	6
Configure Consent Notices for Cloud Administration.....	7
Audit Consent Notices for Cloud Administration .....	7
About Notifications .....	7
Manage User Accounts.....	8
About the User Administration Table .....	8
Customize the User Administration Table .....	8
Add Columns.....	8
Remove Columns .....	9
Rearrange Columns.....	9
About User Administration Table Filters .....	9
Add Single User Accounts .....	10
Add Multiple User Accounts .....	11
Create an Import Template.....	11
Export a List of Users .....	12
Import User Accounts.....	13
Delete a User Account.....	13
Modify a User Account .....	13
Manage Application Access .....	14
Manage Application Access for a Single User Account.....	15
Assign Application Access for a Single User Account.....	15
Remove Application Access for a Single User Account .....	15
Manage Application Access for Multiple Users .....	16
Reset Passwords .....	16
Reset the Password for a Single User Account .....	17
Reset Passwords for Multiple User Accounts.....	17
Change User Account Status .....	17
Unlock User Accounts .....	17
Disable User Accounts .....	18
Enable User Accounts .....	18
De-provision User Accounts.....	19

<b>Manage Companies.....</b>	<b>19</b>
About the Manage Companies Table .....	20
About Manage Companies Table Filters .....	20
Add a Partner Company .....	20
Modify a Partner Company .....	21
Change a Company's Password Policy (OIM Only) .....	21
Delete a Partner Company.....	22
<b>Manage Password Policies.....</b>	<b>22</b>
About the Manage Password Policies Table.....	23
About Policy Types.....	23
General Policy Rules for OIM .....	24
Custom Policy Rules.....	24
Add a Password Policy for OIM .....	26
Modify a Password Policy.....	28
Delete a Password Policy for OIM.....	28
Assign a Password Policy to a Company for OIM.....	29
<b>Advanced Identity Management Tasks.....</b>	<b>29</b>
Users Resetting Challenge Questions for OIM.....	30
Users Changing a Password .....	30
<b>Enable Identity Federation with Oracle Primavera .....</b>	<b>31</b>
<b>Actions that Require Service Requests .....</b>	<b>31</b>
<b>Test Bandwidth and Latency .....</b>	<b>31</b>
<b>Context-Sensitive Help.....</b>	<b>33</b>
User Administration.....	33
Manage Companies .....	33
Manage Password Policies .....	34
Consent Settings .....	34
<b>Legal Notices .....</b>	<b>35</b>

# About the Cloud Administration Identity Management Administration Guide

---

This guide will tell you how to complete administration tasks in Cloud Administration.

Within our documentation, some content might be specific for cloud deployments using Oracle Identity Manager (OIM) while other content is relevant for cloud deployments on Identity Cloud Service (IDCS). Any content that applies to only one of these deployments is labeled accordingly.

## About OIM (Oracle Identity Management) and IDCS (Identity Cloud Service)

---

Cloud Services may be deployed with Oracle Identity Management (OIM) or with Identity Cloud Service (IDCS). Both these systems are identity management systems and are used to ensure that your users are able to access your Cloud Service applications securely.

To determine which identity management system you are using:

- 1) Navigate to the Cloud Portal.
  - ▶ If the Supporting Applications pane includes a link to Oracle Identity Management, your deployment is using OIM.
  - ▶ If the Supporting Applications pane includes a link to Identity Cloud Service, your deployment is using IDCS.

## Manage Personal Information in Cloud Administration

---

### About Consent Notices

Consent notices inform users how personally identifiable information (PII) is collected, processed, stored, and transmitted, along with details related to applicable regulations and policies. Consent notices also alert users that the action they are taking may risk exposing PII. Cloud Administration helps you to ensure that you have requested the appropriate consent to collect, process, store, and transmit the PII your organization holds as part of Cloud Administration data.

Consent notices should:

- ▶ be written in clear language which is easy to understand.
- ▶ provide the right level of detail.

- ▶ identify the purpose and legal basis for your collection, processing, storage, and transmission of PII.
- ▶ identify whether data will be transferred to named third parties.
- ▶ identify PII categories and list the data which will be collected, processed, stored, and transmitted.

### About Personal Information

Personal information (PI) is any piece of data which can be used on its own or with other information to identify, contact, or locate an individual or identify an individual in context. This information is not limited to a person's name, address, and contact details. For example a person's IP address, phone IMEI number, gender, and location at a particular time could all be personally identifiable information. Depending on local data protection laws, organizations may be responsible for ensuring the privacy of PI wherever it is stored, including in backups, locally stored downloads, and data stored in development environments.

### Cookies Usage in Cloud Administration

When using Cloud Administration, the server may generate cookies and send them to the user's browser. The user's machine stores the cookies, either temporarily by the browser, or permanently until they expire or are removed manually.

Oracle might use cookies for authentication, session management, remembering application behavior preferences and performance characteristics, and to provide documentation support.

Also, Oracle might use cookies to remember your log-in details, collect statistics to optimize site functionality, and deliver marketing based on your interests.

### Your Responsibilities

Information security and privacy laws can carry heavy penalties and fines for organizations which do not adequately protect PII they gather and store. If these laws apply to your organization, it is your responsibility to configure consent notices before they are required. You should work with your data security and legal teams to determine the wording of the consent notices you will configure in Cloud Administration.

If a consent notice is declined, it is your responsibility to take any necessary action. For example, you may be required to ensure that the data is not stored or shared.

### Personal Information (PI) Data in Cloud Administration


PI may be visible in multiple areas of Cloud Administration, including but not limited to the user administration, company administration, and password policy administration.

PI may be at risk of exposure in multiple areas of Cloud Administration, including but not limited to user export, web services, the API, and DACS.

As part of Cloud Administration, you may be using Oracle Identity Cloud Service (“Oracle IDCS”) to manage your user access and entitlements across a number of cloud and on-premises applications and services. If you are using or accessing Oracle IDCS, you are responsible for deleting your details and data from the Oracle IDCS environment. You are responsible for retrieving your content in Oracle IDCS during your applicable services period.

### Configure Consent Notices for Cloud Administration

To configure consent notices for Cloud Administration:

- 1) On the  **Consent Settings** tab:
  - a. In the **Consent Message** field, enter the text of the consent notice.


**Note:** Work with your data security and legal teams to determine the wording of the consent notice.
  - b. Toggle the **Enable Consent Notice** setting to activate the consent notice field.

**Note:** If you change the text of an already configured consent notice, consent status for all users is reset to Pending and all users will be presented with the new text of the consent notices next time they log in.

### Audit Consent Notices for Cloud Administration

You can see the status of consent acceptance for users.

To audit consent status for Cloud Administration:

- 1) On the  **Consent Settings** tab, in the User Acceptance area:
  - ▶ View the consent status for each user in the Status column.
  - ▶ View the date and time when the status was most recently changed in the Last Modified column.
  - ▶ Click a column heading to order the user acceptance table by that data item.

## About Notifications

The Notifications list shows your activities in Cloud Administration. Typically, Cloud Administration creates a notification any time you attempt to save table changes.


To view the Notifications list, click **View Notifications** at the upper right of the screen.

**Note:** You can only view notifications for the activities of the current user account.

## Manage User Accounts

---

The User Administration table in Cloud Administration enables you to manage user accounts for your Cloud Service applications. You can add user accounts one at a time or import them in bulk. You can also edit the fields associated with a user account.

Click the  **User Administration** tab to view the User Administration table.

### About the User Administration Table

By default, the User Administration table displays all user accounts. See **About User Administration Table Filters** (on page 9) for details on applying filters to control the users accounts that appear.

Each row in the User Administration table represents a single user account. The User Administration table includes the following columns:

- ▶ **Last Name:** The last name of the user.
- ▶ **First Name:** The first name of the user.
- ▶ **Email:** The email address of the user.
- ▶ **User Name:** The user name of the user account.
- ▶ **Company:** The company to which the user account belongs.
- ▶ **User Type:** The type of user in the system. (OIM Only)
- ▶ **Application Access:** The applications that users are permitted to access.
- ▶ **Date and Time Added:** The date and time on which the user was successfully created. The date format is Month/Date/Year.
- ▶ **Added By:** The user name of the cloud administrator that created the user.
- ▶ **Last Action:** The last action applied to the user as well as the date of the action. The format of the date is Month/Date/Year.

See **Customize the User Administration Table** (on page 8) for details on adding, removing, or rearranging columns.

### Customize the User Administration Table

You can customize the User Administration table by adding, removing, or rearranging columns.



---

**Note:** Required fields (including **Last Name**, **First Name**, **Company**, **Email**, **User Name**, and **User Type**) cannot be removed from the User Administration table.

---

### Add Columns

To add columns to the User Administration table:

- 1) On the  **User Administration** tab, click  **Settings**.
- 2) In the **Available Columns** pane, select one or more columns that you want to add to the User Administration table.



- 3) Click **> Add to selected column.**
- 4) Click **Apply.**

Alternatively, you can double-click a column in the **Available Columns** pane to immediately add it.

---

## Remove Columns

**Note:** Required fields (including **Last Name**, **First Name**, **Company**, **Email**, **User Name**, and **User Type**) cannot be removed from the User Administration table. If you multi-select a required field in addition to other fields that you want to remove, the **< Remove from selected column** button will be disabled. To re-enable the button, you must deselect the required fields.

To remove columns from the table:

- 1) On the **User Administration** tab, click **Settings**.
- 2) In the **Selected Columns** pane, select one or more columns that you want to remove from your view of the table.
- 3) Click **< Remove from selected column.**
- 4) Click **Apply.**

Alternatively, you can double-click a column in the **Selected Columns** pane to immediately remove it.

---

## Rearrange Columns

You can rearrange the columns in the table.

To rearrange column using the **Settings** dialog box:

- 1) On the **User Administration** tab, click **Settings**.
- 2) In **Selected Columns**, select one or more columns.
- 3) Click **Move Down** or **Move Up**.
- 4) Click **Apply.**

To rearrange columns by dragging:

- 1) On the table, click and hold the header of a column.
- 2) Drag the column to a new location in the table.

---

## About User Administration Table Filters

By default, the User Administration table displays all user accounts for the companies managed by the current cloud administrator. Use the **Filter** field to apply one or more filters and control the user accounts that appear.

**Note:** If you have more than one filter applied, click **Only** for a filter to

remove all other filters.

---

The following filters are available:

- ▶ **Enabled:** Displays users whose account is enabled.
- ▶ **No Access:** Displays users who have not been assigned access to any application.
- ▶ **Modified:** Displays users whose accounts have been modified in the current session of Cloud Administration, including new users that have not been saved.
- ▶ **Locked:** Displays users whose account has been locked. See **Unlock User Accounts** (on page 17) for details.
- ▶ **Disabled:** Displays users whose account is disabled. Disabled users cannot log in to any Cloud Service applications.

## Add Single User Accounts

Use Cloud Administration to add individual user accounts.

To add single user accounts:

- 1) On the  **User Administration** tab, click **+ Add a new user**.
- 2) In the **Last Name** field, enter the user's last name.
- 3) In the **First Name** field, enter the user's first name.
- 4) In the **Email** field, enter the user's email address.
- 5) In the **Username** field, enter the user name for the user account.
- 6) In the **Company** field, click **... Select** and select a company for the user account.
- 7) In the **User Type** field, click the list and select the user type for each account. (OIM only)
- 8) In the **Application Access** field, triple-click **... Select** and do the following:

---

**Note:** This step is optional. You can assign application access later.

---

- a. In the **Available** pane, select the application assignments for the user account. Hold down the **Control** key and click to select more than one application.
  - b. Click **> Add to selected column**.
  - c. Click **Apply**.
- 9) Repeat these steps for each user account you want to add.
  - 10) Do one of the following:
    - a. Click **Save** to commit your changes and save your users.
    - b. Click **Export Changes** to save a CSV file (**Create\_User\_<date>.csv**) in your Downloads folder. No users are saved at this time. You can import the CSV file and save your users later.

**Notes:**

- If user creation fails, one reason might be that you have exceeded your Primavera Unifier license limits. See "Working with the License Manager" in the *Primavera Unifier Help* for details.
- After creating a user account, you must reset that password for the account. If your deployment uses IDCS, resetting a password sends the user an email with a link to allow them to change their own password. If your deployment uses OIM, resetting a password notifies the user about their new account and provides them a temporary password. On logging in with the temporary password, the user is prompted to change the password and set challenge questions. See **Reset Passwords** (on page 16) for details.

## Add Multiple User Accounts

Use an import template to add multiple user accounts to your cloud environment. You can either import a custom import template or a CSV file created from a previous session.

The import template is a CSV file that you can download from Cloud Administration. After you add information on your users accounts to the template, you can import that information to the User Administration table.

Use the following topics to add multiple user accounts:

- 1) **Create an Import Template** (on page 11)
- 2) **Import User Accounts** (on page 13)
- 3) **Reset Passwords** (on page 16)

## Create an Import Template

You can download the import template from Cloud Administration. The import template contains the following columns:


- ▶ **Last Name**
- ▶ **First Name**
- ▶ **Email**
- ▶ **Username**
- ▶ **Company**
- ▶ **User Type** (OIM only)
- ▶ **Application Assignment Columns:** When you download the import template, you select the application assignments that you want to include in the template. The import template contains a column for application assignment you select. Each application assignment column is prefixed with **#R#** (for examples, **#R#BI Authors**).

---

**Caution:** Do not modify the header row of the import template. Modifying the header row will produce unpredictable results when you import users to Cloud Administration.

---

To create an import template:

- 1) On the  **User Administration** tab, click **Actions** ▼ and select **Download Import Template**.
- 2) In the of the **Select Application Access** dialog box, in the **Available** pane, select the application assignments that you want to include in the template. Hold down the **Control** key and click to select more than one application assignment.
- 3) Click > **Add to selected column**.
- 4) Click **Select**.
- 5) Save the template locally and open it.

---

**Note:** The default name of the import template is `User_Import_Template.csv`.

---

- 6) Enter the following information for each user account:
  - ▶ **Last Name:** The user's last name.
  - ▶ **First Name:** The user's first name.
  - ▶ **Email:** The user's email address.
  - ▶ **Username:** The user name for the user account.
  - ▶ **Company:** The company for the user account.
  - ▶ **User Type:** The user type for the user account. (OIM only)
- 7) In the application assignment fields, enter **Y** or **Yes** to assign application access to the user account.  
If you do not want to assign application access, leave these fields empty. You can assign application access later.
- 8) Repeat steps 6 and 7 for each user you want to add.
- 9) Save and close the template.

## Export a List of Users

When you export the user list, all the columns on the User Administration page are exported. Two extra columns are also exported:


- ▶ **Locked:** Shows whether the account is locked, for example following a failure to authenticate the password.
- ▶ **Active:** Shows whether the account is disabled.

To export a list of all users to a CSV file:

- 1) On the  **User Administration** tab, click **Actions** ▼ and select **Export All Users**.

## Import User Accounts

To import user accounts:

- 1) On the  **User Administration** tab, click **Actions** ▼ and select **Import Users**.
- 2) Click ... **Browse** and select the import template.

---

**Note:** The default name of the import template is `User_Import_Template.csv`.

---

- 3) Click **OK**.
- 4) Review the User Administration table to ensure there are no errors.
- 5) Click **Save**.

---

**Notes:**

- If user creation fails, one reason might be that you have exceeded your Primavera Unifier license limits. See "Working with the License Manager" in the *Primavera Unifier Help* for details.
  - After creating a user account, you must reset that password for the account. If your deployment uses IDCS, resetting a password sends the user an email with a link to allow them to change their own password. If your deployment uses OIM, resetting a password notifies the user about their new account and provides them a temporary password. On logging in with the temporary password, the user is prompted to change the password and set challenge questions. See **Reset Passwords** (on page 16) for details.
- 

## Delete a User Account

User accounts cannot be deleted from Cloud Services. Instead, you can disable a user account to block access to the Cloud Portal and Cloud Service applications. See **Disable User Accounts** (on page 18) for details.

## Modify a User Account

You can modify the following fields for a user account in the User Administration table:

- ▶ **First Name**
- ▶ **Last Name**
- ▶ **Email**
- ▶ **Application Access**
- ▶ **Company**

---

**Notes:**

- To modify a user name, submit a Service Request to My Oracle Support. See **Actions that Require Service Requests** (on page 31)

for details.

---

## Manage Application Access

Assigning application access is the process by which you authorize specific employees in your company to access specific Cloud Service applications. User accounts that are not assigned access cannot use Cloud Service applications.

---

**Note:** In addition to being assigned access to one or more Cloud Service applications, application-specific security assignments must be provided for your user accounts in the target application. See the Administration Guide for your Cloud Service application for details.

---

The following access types are available for each Cloud Services application:

### BI

- ▶ **BI Production Authors:** Users have access to BI Publisher and can create, run, and view all of the reports that were made available to their folders.
- ▶ **BI Production Consumers:** Users have access to BI Publisher and can run and view all of the reports that were made available to their folders.

### Cloud

- ▶ **Cloud Administrator:** Users have access to Cloud Administration and can administer users.

### Primavera Analytics

- ▶ **Primavera Analytics Production:** Users have administrative access to Primavera Analytics and can manage and run the extract, transform, and load (ETL) process.

### Primavera Gateway

- ▶ **Primavera Gateway Production Administrator:** Users have complete access to Primavera Gateway as a user, developer, and administrator. The Primavera Gateway administrator has complete administration privileges and access to data.
- ▶ **Primavera Gateway Production Administrator (Limited Access):** Users have complete administration privileges, but no access to integrated data.
- ▶ **Primavera Gateway Production Developer:** Users have access to Primavera Gateway the data dictionary, workflows, and configuration global settings. They can also create data mappings and flow types.
- ▶ **Primavera Gateway Production User:** Users have access to Primavera Gateway to create, run, and monitor synchronization jobs in Primavera Gateway. Primavera Gateway users only have access to data.
- ▶ **Primavera Gateway Production User (Limited Access):** Users have access to Primavera Gateway to create, run, and monitor synchronization jobs in Primavera Gateway, but no access to integrated data.

### Primavera P6

- ▶ **Primavera P6 Production:** Users have access to P6 EPPM applications, including P6, P6 Team Member, and P6 EPPM Web Services.
- ▶ **Primavera P6 Virtual Desktop User:** Users can use Primavera Virtual Desktop to access P6 Professional using a virtual desktop. Note: Primavera Virtual Desktop is not available with P6 Standard Service.

### Primavera Unifier

- ▶ **Primavera Unifier Production:** Users have access to Primavera Unifier.
- ▶ **Primavera Unifier Production REST Webservices:** Users have access to Primavera Unifier REST Web Services.

**Note:** By default, data sources to product schema, such as P6 EPPM and Primavera Unifier, are automatically assigned to the BI Consumer and BI Author access types.


## Manage Application Access for a Single User Account

Use the **Select Application Access** dialog box to assign application access for a single user account.


In the **Select Application Access** dialog box, the **Available** pane (on the left) shows the available applications. The **Selected** pane (on the right) shows the applications that the user account can access.

### Assign Application Access for a Single User Account

To assign application access for a single user account:


- 1) On the  **User Administration** tab, select the check box for a user account.
- 2) Click **Manage Application Access**.
- 3) In the **Available** pane, select one or more applications.

**Note:** Hold the **Control** key and click to select more than one application.

- 4) Click  **Add to selected column**.
- 5) Click **Select**.
- 6) Click **Save**.

### Remove Application Access for a Single User Account

To remove application access for a single user account:

- 1) On the  **User Administration** tab, select the check box for a user account.
- 2) Click **Manage Application Access**.
- 3) In the **Selected** pane, select one or more applications.

---

**Note:** Hold the **Control** key and click to select more than one application.



---

- 4) Click  **Remove from selected column.**
- 5) Click **Select.**
- 6) Click **Save.**


## Manage Application Access for Multiple Users

Use the **Manage Application Access** dialog box to manage application access for multiple user accounts.

The Manage Application Access dialog box shows each available access type. Icons indicate the status of the access for the selected user accounts.

- ▶  **All selected users have access:** All of the selected user accounts have been assigned this access type.
- ▶  **Some of the selected users have access:** Some of the selected user accounts have been assigned this access type.
- ▶ **No icon:** None of the selected user accounts have been assigned this access type.

To assign application access to multiple user accounts:

- 1) On the  **User Administration** tab, select the check boxes for multiple user accounts.
- 2) Click **Manage Application Access.**
- 3) In the **Available Application Access** pane, select the access type you want to manage.
- 4) In the **Select or Deselect Users** table, select and deselect the check boxes to assign and remove access as needed.
- 5) Repeat steps 3 and 4 to manage other access types.
- 6) Click **OK.**
- 7) Click **Save.**

## Reset Passwords

You can reset passwords for a single user account or for multiple user accounts. When you reset passwords for multiple user accounts, an email is sent to each selected user with a link to follow to reset their password. When you reset the password for a single user account, you also have the option of manually generating a password.

---


**Note:** After creating a user account, you must reset that password for the account. If your deployment uses IDCS, resetting a password sends the user an email with a link to allow them to change their own password. If your deployment uses OIM, resetting a password notifies the user about their new account and provides them a temporary password. On logging in with the temporary password, the user is prompted to change the password and set challenge questions.

---



## Reset the Password for a Single User Account

To reset a password for a single user account:

- 1) On the  **User Administration** tab, select the check box for a user account.
- 2) Click **Reset Password**.
- 3) Do one of the following:
  - a. Select **Auto-generate the Password** to send the user an email containing a link to allow them to change their own password (on IDCS) or to send an email with a temporary password (on OIM).
  - b. Select **Manually Change the Password** to enter a new password (on IDCS) or a temporary password (on OIM).
- 4) Click **Reset Password**.
- 5) Click **OK**.


---

**Note:** On IDCS, if you select the option to generate the password automatically, the link in the email that the user receives automatically expires after 60 minutes.

---

## Reset Passwords for Multiple User Accounts

To reset passwords for multiple user accounts:

- 1) On the  **User Administration** tab, select the check boxes for multiple user accounts.
- 2) Click **Reset Password**.
- 3) Click **Yes**.

The passwords are reset and each selected user is sent an email containing a link to follow to reset their password (on IDCS) or an automatically generated temporary password (on OIM).

## Change User Account Status

A user account can be locked, enabled, or disabled.

This section describes how to unlock a user account, enable a disabled user account, and disable an enabled user account.

## Unlock User Accounts

When a user account becomes locked, the user is unable to log in to the Cloud Portal or Cloud Service applications. In this case, the user account must be unlocked.

The following are some typical reasons why a user account becomes locked:

- ▶ The user attempts to log in too many times with an incorrect password.
- ▶ The user's password expires.


---

**Note:** A user with an expired password can also unlock their account by

attempting to log in with their expired password.

---

To unlock a user account:

- 1) On the  **User Administration** tab, select the check boxes for one or more locked user accounts.

---

**Note:** Apply the **Locked** filter to display only Locked user accounts in the User Administration table. See **About User Administration Table Filters** (on page 9) for details.

---

- 2) Click **Unlock**.

---


**Note:** The **Unlock** button appears only when you select the check boxes for one or more locked user accounts. If you select one or more unlocked user accounts, the **Unlock** button will not appear.

---

## Disable User Accounts

When you disable a user account, the user is blocked from accessing the Cloud Portal and Cloud Service applications. In addition, a cloud administrator is unable to perform most tasks for the user in Cloud Administration (other than enabling the account). For example, you might choose to disable a user account if a user moves to a different role in your organization or takes a sabbatical.

To disable a user account:

- 1) On the  **User Administration** tab, select the check boxes for one or more enabled user accounts.

---

**Note:** Apply the **Enabled** filter to display only enabled user accounts in the User Administration table. See **About User Administration Table Filters** (on page 9) for details.

---

- 2) Click **Disable**.


### Notes:

- The **Disable** button appears only when you select the check box for one or more enabled user accounts. If you select one or more disabled user accounts, the **Disable** button will not appear.
  - To ensure that a user is removed from P6 and shown as disabled in Unifier, you must also de-provision the account. See **De-provision User Accounts** (on page 19) for details.
- 

## Enable User Accounts

When you enable a user account, the user can access Cloud Portal and Cloud Service applications.

To enable a user account:

- 1) On the  **User Administration** tab, select the check boxes for one or more disabled user accounts.

**Note:** Apply the **Disabled** filter to display only disabled user accounts in the User Administration table. See **About User Administration Table Filters** (on page 9) for details.

- 2) Click **Enable**.



**Note:** The **Enable** button appears only when you select the check box for one or more disabled user accounts. If you select one or more enabled user accounts, the **Enable** button will not appear.

## De-provision User Accounts

When you de-provision a user account, the user is blocked from accessing the Cloud Portal and any of the applications. A cloud administrator is unable to perform most tasks for the user in Cloud Administration until the account is re-enabled.

**Note:** When you de-provision a user from access to P6 EPPM, the user account will be deleted from P6 EPPM. Deleting a user from P6 EPPM deletes all data associated with that user. If a user has P6 Team Member module access or is associated with a resource and has actual working hours on a project Oracle recommends you do not de-provision that user. See the *P6 EPPM Application Administration Guide* for further information.

To de-provision a user account:

- 1) On the  **User Administration** tab, select the check box for an enabled user account.
- 2) Click **Disable**.
- 3) Double click in the **Application Access** cell for the user in the grid.
- 4) In the Select Application Access dialog box:
  - a. Select all the columns in the Selected list.
  - b. Select  **Remove from selected column**.
  - c. Select **Select**.


## Manage Companies

The Manage Companies table in Cloud Administration enables you to manage companies for your Cloud Service applications. A company represents a logical container of users in Cloud Administration.

Two types of companies can exist in Cloud Services:

- ▶ **Owner company:** An owner company has been created for you. A single owner company is required by Cloud Administration. You can modify certain aspects of the owner company (including the company full name and the password policy). It is not possible to delete an owner company.
- ▶ **Partner companies:** A partner company is a separate entity from the owner company that needs to access your Cloud Service applications. Examples of partner companies include vendors, resellers, subcontractors, suppliers, and other consultants. Partner companies are listed under the owner company on the left side of the **Manage Companies** page.

When you add a partner company in Cloud Administration, you can also assign one or more applications to the company. If you assign Primavera Unifier, the partner company is also created within that application.

Click the  **Manage Companies** tab to view the Manage Companies table.

### About the Manage Companies Table

By default, the Manage Companies table displays the owner company and all partner companies. See **About Manage Companies Table Filters** (on page 20) for details on applying filters to control the companies that appear.

Each row in the Manage Companies table represents a single company. The Manage Companies table includes the following columns:

- ▶ **Company Short Name:** The short name for the company.
- ▶ **Company Full Name:** The full name for the company.
- ▶ **Assign To (Applications):** The application for the company.

### About Manage Companies Table Filters


By default, the Manage Companies table displays the owner company and all partner companies. Use the **Filter** field to apply a filter and control the companies that appear.

The following filter is available:

- ▶ **Primavera Unifier Production:** Displays companies assigned to access to Primavera Unifier.

### Add a Partner Company

To add a company:

- 1) On the  **Manage Companies** tab, click **+ Add Company**.
- 2) In the **Company Short Name** field, enter a short name for the partner company.
- 3) In the **Company Full Name** field, enter the full name for the partner company.
- 4) OIM Only: If you want to use a custom password policy, do the following:
  - a. Deselect the **Inherit Password Policy** check box.
  - b. In the **Password Policy** field, triple-click **... Select**.
  - c. Select a password policy.
  - d. Click **OK**.

---

**Note:** If you want to use the default password policy, skip this step.

---

- 5) Do the following to add the partner company to Primavera Unifier:
  - a. On the **Assign To (Applications)** field, triple-click **... Select**.
  - b. In the left pane, select **Primavera Unifier Production**.
  - c. Click **> Add to selected column**.
  - d. Click **OK**.
- 6) Click **Save**.

### Tips

- ▶ When you add a partner company, the address from the owner company is used by default. To change the address, modify the address details in Primavera Unifier.

## Modify a Partner Company

You can modify any of the fields for a partner company in the Manage Companies table.

---

**Note:** To modify the **Company Short Name** field, submit a Service Request to My Oracle Support. See **Actions that Require Service Requests** (on page 31) for details.

---

## Change a Company's Password Policy (OIM Only)

After you change a company's password policy, all new users that are assigned to the company must create a password according to the new password policy.


Notes:

- If the password policy assigned to a company is modified or a new password policy is assigned to a company, existing users with established passwords are not required to change their password immediately. However, when those users do change their password (for example, due to password expiration or password reset), the new password must conform to the new password policy. Oracle recommends that you reset the passwords of users that belong to a company whose password policy has been changed.
- OIM Only: If a partner company inherits the password policy of the owning company and the owning company password policy is modified, the partner company password policy is modified accordingly.

---

Use the **Select Password Policy** dialog box to change the password policy of a single company. You can also change the password policy for multiple companies using the **Manage Password Policies** page. For more information about changing the password policy for multiple companies, see **Assign a Password Policy to a Company for OIM** (on page 29).

To change a company's password policy:

- 1) On the  **Manage Companies** tab, click ⊕ **Expand** to expand the owner company, if needed, and select the partner company you want to change.
- 2) If needed, deselect the **Inherit Password Policy** check box.
- 3) In the **Password Policy** field, triple-click ... **Select**.
- 4) Select a password policy.
- 5) Click **OK**.
- 6) Click **Save**.

## Delete a Partner Company

You can delete a partner company if the following is true:



- ▶ The company is not assigned to an application.
- ▶ No user accounts have been associated with the company.

---

**Note:** If a partner company is no longer needed, Oracle recommends that you disable that company instead of deleting. See **Modify a Partner Company** (on page 21) for details.

---

To delete a partner company:

- 1) On the  **Manage Companies** tab, click ⊕ **Expand** to expand the owner company, if needed, and select the partner company you want to delete.
- 2) Click  **Context**.
- 3) Select **Delete Row**.
- 4) Click **Yes**.
- 5) Click **Save**.

## Manage Password Policies

The Manage Password Policies table in Cloud Administration enables you to manage the password policy (IDCS) or policies (OIM) for your Cloud Service applications. Password policies are based on policy rules and are assigned to companies (OIM) or users (IDCS). Users must use a password that conforms to their or their company's password policy.

OIM Only: Password policies can be assigned to one or more companies, but companies can only be assigned one password policy. Because a user can only be assigned to one company, users only need to confirm to one password policy.


---

Notes:

- If the password policy assigned to a company is modified or a new password policy is assigned to a company, existing users with established passwords are not required to change their password immediately. However, when those users do change their password (for example, due to password expiration or password reset), the new password must conform to the new password policy. Oracle

recommends that you reset the passwords of users that belong to a company whose password policy has been changed.

- **OIM Only:** If a partner company inherits the password policy of the owning company and the owning company password policy is modified, the partner company password policy is modified accordingly.

Click the  **Manage Password Policies** tab to view the Manage Password Policies table.

## About the Manage Password Policies Table

By default, the Manage Password Policies table displays all password policies.

Each row in the Manage Password Policies table represents a single password policy. The Manage Password Policies table includes the following columns:

- ▶ **Policy Name:** The name of the password policy.
- ▶ **Minimum Length** (OIM Only): the minimum number of characters that users are required to have in their password.
- ▶ **Warn After (days)** (OIM Only): the number of days that will pass before users are warned that their passwords are set to expire on a specific date.
- ▶ **Expires After (days)** (OIM Only): the number of days that will pass before passwords expire.
- ▶ **Disallow Past Passwords** (OIM Only): the frequency at which old passwords can be reused. This policy ensures that users do not change back and forth among a set of common passwords.
- ▶ **Minimum Password Age** (OIM Only): the length of time (in days) users must keep their passwords before they are allowed to change them again.
- ▶ **Policy Type:** The policy type for a password policy. See **About Policy Types** (on page 23) for details.

## About Policy Types

You can control the general policy rules for all policy types. See **General Policy Rules for OIM** (on page 24) for details. Other password rules are determined by the policy type:

- ▶ **Simple:** This password type is available in IDCS only. Each user is required to create a password that conforms to a set of rules designed to create a password of medium strength.
- ▶ **Standard:** This password type is available in IDCS only. Each user is required to create a password that conforms to a set of rules designed to create a strong password.
- ▶ **Complex:** This password type is available in OIM only. Each user is required to create a password that conforms to the following conventions:

Must contain characters from three of the following types:

- English Uppercase Characters (A through Z)
- English Lowercase Characters (a through z)
- Base 10 Digits (0 through 9)
- Non-alphanumeric (for example, !, \$, #, ^)

- Unicode Characters

Cannot contain the following:

- User ID
- First Name
- Last Name

- ▶ **Custom:** Each user is required to create a password that conforms to a custom set of rules. See **Custom Policy Rules** (on page 24) for details.

## General Policy Rules for OIM

All policy types allow you to set the following password rules:

- ▶ **Minimum Length:** Enter the minimum number of characters a password must contain. For example, if you enter **4**, the password must contain at least four characters. This field accepts values from 0 to 999 for custom passwords.
- ▶ **Warn After (days):** Enter the number of days before a user is notified that a password will expire. For example, suppose you enter **20** in this field and **30** in the **Expires After (days)** field. If a user creates a password on November 1, the user will be notified on November 21 (20 days later) that the password will expire on December 1 (30 days later). This field accepts values from 0 to 999.
- ▶ **Expires After (days):** Enter the number of days before a password will expire. For example, if you enter **30** and a user creates a password on November 1, then the password will expire on December 1 (30 days later). This field accepts values from 0 to 999.
- ▶ **Disallow Past Passwords:** Enter the number of old passwords that cannot be reused. This policy ensures that users do not change back and forth among a set of common passwords. For example, if you enter **10**, a user cannot reuse any of the last ten passwords. This field accepts values from 0 to 24.
- ▶ **Minimum Password Age:** Enter the minimum number in days for which users must use a password. For example, if you enter **2**, a user cannot change the password within two days of creating the password. The value of this field must be less than the value of the **Expires After (days)** field. For example, if you enter **30** in the **Expires After (days)** field and **31** in this field, an error occurs.
- ▶ **Policy Type:** The policy type for the password policy: **Complex** or **Custom**. A **Complex** password policy uses a standard set of password rules, as described in **About Policy Types** (on page 23). A **Custom** password policy uses a custom set of password rules, as described in **Custom Policy Rules** (on page 24).

## Custom Policy Rules

If you set **Custom** password policy, you can set the following password rules:

- ▶ **Account Lock Threshold:** This rule is available in IDCS only. Enter the number of times a user can enter an incorrect password before the account will be locked.



- ▶ **Characters Allowed:** This rule is available in OIM only. Enter the characters a password can contain. For example, if you enter a percent sign (%), a password must contain a percent sign. A password would not be valid if it contained any character not in this field. For example, if you enter abc, the password dad is not valid because the character d is not specified. If you specify the same character in this field and Characters Not Allowed field, an error occurs.
- ▶ **Characters Not Allowed:** Enter the characters a password must not contain. For example, if you enter an exclamation point (!), a password cannot contain an exclamation point. If you specify the same character in this field and Characters Allowed field, an error occurs.
- ▶ **Characters Required:** Enter the characters a password must contain. For example, if you enter x, a password must contain the character x. The character you enter in this field must also be entered in the Characters Allowed field. Otherwise, an error occurs. If you specify more than one character, do not provide delimiters. Commas and spaces are also considered characters in this field. For example, if you specify a,x, a valid password would need to contain the character a, the character x, and a comma.
- ▶ **Disallow First Name:** Use this rule to specify whether the user's first name is allowed in a password. If the check box is selected, a password is not valid if it contains the user's first name.
- ▶ **Disallow Last Name:** Use this rule to specify whether the user's last name is allowed in a password. If this check box is selected, a password is not valid if it contains the user's last name.
- ▶ **Disallow Restricted Words:** This rule is available in IDCS only. Use this rule to specify whether restricted words are allowed in a password. When this checkbox is selected, a password is not valid if it contains any of the words on the restricted words list.
- ▶ **Disallow User ID:** Use this rule to specify whether the user ID is allowed in a password. When this check box is selected, a password is not valid if it contains the user ID.
- ▶ **Disallow Whitespace Character:** This rule is available in IDCS only. Use this rule to specify whether a space is allowed in a password. When this rule is switched on, a password is not valid if it contains a space.
- ▶ **Expires After (days):** This rule is available in IDCS only. Enter the number of days after which a user must change their password.
- ▶ **Maximum Length:** Enter the maximum number of characters a password can contain. For example, if you enter 8, a password cannot contain more than eight characters. This field accepts values from 1 to 999.
- ▶ **Maximum Repeated Characters:** Enter the maximum number of times a character can be repeated in a password. For example, if you enter 2, a password is not valid if any character is repeated more than two times. With this setting, the password RL112211 is not valid because the character 1 appears four times (and is therefore repeated three times). This field accepts values from 1 to 999.
- ▶ **Maximum Special Characters:** This rule is available in OIM only. Enter the maximum number of non-alphanumeric characters a password can contain. For example, if you enter 3, a password cannot contain more than three non-alphanumeric characters. This field accepts values from 1 to 999.
- ▶ **Maximum Unicode Characters:** This rule is available in OIM only. Enter the maximum number of Unicode characters that a password can contain. For example, if you enter 8, a password cannot contain more than eight Unicode characters. This field accepts values from 1 to 999.

- ▶ **Minimum Alphabet Characters:** Enter the minimum number of letters a password must contain. For example, if you enter 2, a password must contain at least two letters. This field accepts values from 0 to 999.
- ▶ **Minimum Alphanumeric Characters:** This rule is available in OIM only. Enter the minimum number of letters or digits that a password must contain. For example, if you enter 6, a password must contain at least six letters and digits. This field accepts values from 0 to 999.
- ▶ **Minimum Length:** This rule is available in IDCS only. Enter the minimum number of characters a password must contain. For example if you enter 8, a password must contain at least eight characters.
- ▶ **Minimum Lowercase Characters:** Enter the minimum number of lowercase letters a password must contain. For example, if you enter 5, a password must contain at least five lowercase letters. This field accepts values from 0 to 999.
- ▶ **Minimum Numeric Characters:** Enter the minimum number of digits a password must contain. For example, if you enter 1, a password must contain at least one digit. This field accepts values from 0 to 999.
- ▶ **Minimum Special Characters:** Enter the minimum number of non-alphanumeric characters (for example, #, %, or &) a password must contain. For example, if you enter 1, a password must contain at least one non-alphanumeric character. This field accepts values from 0 to 999.
- ▶ **Minimum Unicode Characters:** This rule is available in OIM only. Enter the minimum number of Unicode characters that a password must contain. For example, if you enter 3, a password must contain at least three Unicode characters. This field accepts values from 0 to 999.
- ▶ **Minimum Unique Characters:** Enter the minimum number of non-repeating characters a password must contain. For example, if you enter 1, a password is must contain at least one character that is not repeated. With this setting, the password 1x23321 is valid because the character x is not repeated (although the remaining characters are repeated). This field accepts values from 0 to 999.
- ▶ **Minimum Uppercase Characters:** Enter the minimum number of uppercase letters a password must contain. For example, if you enter 3, a password must contain at least three uppercase letters. This field accepts values from 0 to 999.
- ▶ **Previous Passwords Remembered:** This rule is available in IDCS only. Enter the number of previously used passwords for each user which will be remembered. A password will not be valid if it matches any of the remembered passwords for the user.
- ▶ **Start With Alphabet:** Use this rule to specify whether a password must begin with a letter. If the check box is selected, the password 123welcome would not be valid because it does not begin with a letter. If the check box is deselected, a password can begin with a letter, digit, or special character.
- ▶ **Substrings Not Allowed:** This rule is available in OIM only. Enter a series of consecutive alphanumeric characters a password must not contain. For example, if you enter dog, a password is not valid if it contains the character d, the character o, and the character g in successive order.

## Add a Password Policy for OIM

To add a password policy:

- 1) On the **Manage Password Policies** tab, click **+ Add Password Policy**.
- 2) In the **Policy Name** field, enter the name of the new password policy.
- 3) (Optional) In the **Minimum Length** field, enter the minimum number of characters that users are required to have in their password.
- 4) In the **Warn After (days)** field, enter the number of days that will pass before users are warned that their passwords are set to expire on a specific date. This value must be less than the value entered in the **Expires After (days)** field.
- 5) In the **Expires After (days)** field, enter the number of days that will pass before users' passwords expire. This value must be greater than the value entered in the **Warn After (days)** field.
- 6) (Optional) In the **Disallow Past Passwords** field, enter the frequency at which old passwords can be reused. This policy ensures that users do not change back and forth among a set of common passwords.
- 7) (Optional) In the **Minimum Password Age** field, enter the length of time (in days) users must keep their passwords before they are allowed to change them again. This value must be less than the value entered in the **Expires After (days)** field.
- 8) In the **Policy Type** menu, select one of the following:
  - **Complex**: The password policy uses a standard set of password rules.
  - **Custom**: The password policy uses a custom set of password rules. If you select **Custom**, the custom policy rules appear on the **Complex Policy Rules** tab in the lower pane. Set the custom policy rules as needed. See **Custom Policy Rules** (on page 24) for details.
- 9) On the **Assigned Companies** tab in the lower pane, do the following to assign the password policy to one or more companies:

---

**Notes:**

- If the password policy assigned to a company is modified or a new password policy is assigned to a company, existing users with established passwords are not required to change their password immediately. However, when those users do change their password (for example, due to password expiration or password reset), the new password must conform to the new password policy. Oracle recommends that you reset the passwords of users that belong to a company whose password policy has been changed.
  - **OIM Only**: If a partner company inherits the password policy of the owning company and the owning company password policy is modified, the partner company password policy is modified accordingly.
  - This step is optional. You can assign the password policy to a company later.
- 
- a. Click **Manage Assignments**.
  - b. In the **Available** pane, select the companies for the password policy. Hold down the **Control** key and click to select more than one application.
  - c. Click **> Add to selected column**.

- d. Click **Assign**.
- 10) Click **Save**.

## Modify a Password Policy

### Notes:

- If the password policy assigned to a company is modified or a new password policy is assigned to a company, existing users with established passwords are not required to change their password immediately. However, when those users do change their password (for example, due to password expiration or password reset), the new password must conform to the new password policy. Oracle recommends that you reset the passwords of users that belong to a company whose password policy has been changed.
- OIM Only: If a partner company inherits the password policy of the owning company and the owning company password policy is modified, the partner company password policy is modified accordingly.

To modify a password policy:

- 1) On the **Manage Password Policies** tab, select the password policy you want to modify.

#### In OIM:

- a. Modify the general policy rules as needed.
- b. If the **Policy Type** is **Custom**, on the **Custom Policy Rules** tab in the lower pane, modify the custom policy rules as needed.
- c. Assign the password policy to one or more companies.
- d. Click **Save**.

#### In IDCS:


- a. On the Policy Type list, select **Custom**.
- b. On the **Custom Policy Rules** tab in the lower pane, modify the custom policy rules as needed.
- c. Click **Save**.

## Delete a Password Policy for OIM

Password policies can only be deleted if they are not assigned to any companies. You can only delete one password policy at a time.

To delete a password policy:

- 1) On the **Manage Password Policies** tab, select the password policy you want to delete.
- 2) On the **Assigned Companies** tab in the lower pane, confirm that the password policy is not assigned to any companies.

- 3) Click  **Context**.
- 4) Select **Delete Row**.
- 5) Click **Yes**.
- 6) Click **Save**.

### Assign a Password Policy to a Company for OIM



Each company has an associated password policy. A partner company can be assigned a custom password policy or can inherit the password policy of their owner company. When you assign a password policy to a company, you replace the previous password policy with the new password policy.

Notes:

- If the password policy assigned to a company is modified or a new password policy is assigned to a company, existing users with established passwords are not required to change their password immediately. However, when those users do change their password (for example, due to password expiration or password reset), the new password must conform to the new password policy. Oracle recommends that you reset the passwords of users that belong to a company whose password policy has been changed.
- OIM Only: If a partner company inherits the password policy of the owning company and the owning company password policy is modified, the partner company password policy is modified accordingly.

Use the **Manage Password Policies** tab to assign password policies to one or more companies. You can also use the **Manage Companies** tab if you only want to assign the password policy for a single company. See ***Change a Company's Password Policy (OIM Only)*** (on page 21) for details.

To assign a password policy to a company:

- 1) On the  **Manage Password Policies** tab, select the password policy you want to assign.
- 2) On the Assigned Companies tab in the lower pane, click **Manage Assignments**.
- 3) In the **Available** pane, select the companies for the password policy. Hold down the **Control** key and click to select more than one application.
- 4) Click  **Add to selected column**.
- 5) Click **Assign**.
- 6) Click **Save**.

## Advanced Identity Management Tasks

The following tasks cannot be performed in Cloud Administration:

- ▶ Users resetting their own password

- ▶ Users managing their challenge questions and answers (OIM only)

To perform these tasks (and only these tasks), you will need to use Oracle Identity Manager (OIM) or Identity Cloud Service (IDCS) directly. Oracle Customer Support will not be able to provide support if you use OIM or IDCS for any other task.

## Users Resetting Challenge Questions for OIM

Users can log in to Oracle Identity Manager (OIM) to update or change their challenge questions.

To change challenge questions:

- 1) In Cloud Portal, click **Oracle Identity Manager**.
- 2) Log in to OIM with your user name and password.
- 3) On the Identity Self Service page, under **My Profile**, click **My Information**.
- 4) On the **My Information** tab, expand **Challenge Questions**.
- 5) Select three challenge questions and enter your answers.
- 6) Click **Apply**.

## Users Changing a Password

Users can log in to Oracle Identity Manager (OIM) to change their password. The new password must comply with the relevant password policy.

To change a password in OIM:

- 1) In Cloud Portal, click **Oracle Identity Manager**.
- 2) Log in to OIM with your user name and password.
- 3) On the Identity Self Service page, under **My Profile**, click **My Information**.
- 4) On the **My Information** tab, expand **Change Password**.
- 5) In the **Old Password** field, enter your current password.
- 6) In the **New Password** field, enter your new password.
- 7) In the **Confirm New Password** field, re-enter your new password.
- 8) Click **Apply**.

To change a password in IDCS:

- 1) In Cloud Portal, click **Identity Cloud Service**.
- 2) Log into IDCS with your user name and password.
- 3) Click **Change My Password**.
- 4) In the **Old Password** field, enter your current password.
- 5) In the **New Password** field, enter your new password.
- 6) In the **Confirm New Password** field, re-enter your new password.
- 7) Click **Submit**.

---

**Note:** Wait five minutes before logging into an account after you have

changing a password.

---

## Enable Identity Federation with Oracle Primavera

---

Identity federation enables companies to provide services and share identity information across their respective security domains. The end user does not need to log in repeatedly to access a remote entity where business is conducted. Users authenticate at their local sites, and the federation mechanism enables this information to be shared with Cloud Services.

The benefits of implementing identity federation for your cloud service include:

- ▶ Users do not need to supply login credentials to access each entity where business is conducted. This also eliminates the need to remember and manage multiple logins/passwords. Users still need accounts at the sites so that the accounts can be linked.
- ▶ Local password management (for example, resetting passwords and creating password policies)

For details on enabling identity federation with Cloud Services, see *Enabling Federated Identity Single Sign-On (SSO) Through SAML 2.0 For Primavera Products Hosted In Oracle Cloud (Doc ID 2087067.1)* on My Oracle Support at <http://support.oracle.com>.

## Actions that Require Service Requests

---

In order to complete the following actions, submit a Service Request in My Oracle Support:

- ▶ Modifying the automatically generated email notification that is sent to users when their account is provisioned or their password is reset.
- ▶ Changing Authorization Codes in an application.

---

**Note:** If you change the Authorization Code in your application and do not submit a Service Request in My Oracle Support, you will experience application assignment errors.

---

- ▶ Changing PARTNER license counts and allocations.
- ▶ Changing a user name.

## Test Bandwidth and Latency

---

The Test Bandwidth and Latency screen displays bandwidth and latency information for your Cloud Services client. All users can access the Test Bandwidth and Latency screen.

Statistics are exposed by reading the cookies generated by loading the page. Depending on your network speed, it can take up to ten seconds to generate the statistics. The expiration time for the cookies is set to thirty minutes. If you need to generate statistics before that time, delete all cookies before accessing the Test Bandwidth and Latency screen.



---

**Note:** The first time you access the Test Bandwidth and Latency screen, you may not see any results. However, refresh your browser to fetch the information from the browser cache.

---

To view remote statistics on your Cloud Services client, complete the following steps:

- 1) Enter the following to display the Test Bandwidth and Latency screen:

`http://cloudadminhost/cloud/p/stats`

- 2) If this is the first time you are using the Test Bandwidth and Latency screen, click **Test**.

---

**Note:** If the Test button doesn't appear, press **F5** to refresh your browser.

---



# Context-Sensitive Help

---

You can access the context-sensitive help topics that are accessible from each page in the user interface directly from this topic.

## User Administration

Manage and administer user accounts in your cloud environment. You can create user accounts one at a time or import them in bulk. You can also assign application access, reset passwords, and change user account status.

### How do I...

**Add Single User Accounts** (on page 10)

**Add Multiple User Accounts** (on page 11)

**Delete a User Account** (on page 13)

**Modify a User Account** (on page 13)

**Manage Application Access** (on page 14)

**Reset Passwords** (on page 16)

**Change User Account Status** (on page 17)

### Learn more about...

**Manage User Accounts** (on page 8)

**About the User Administration Table** (on page 8)

## Manage Companies

Manage companies in your cloud environment. You can create, modify, and delete partner companies. You can also change a company's password policy.

### How do I...

**Add a Partner Company** (on page 20)

**Modify a Partner Company** (on page 21)

**Delete a Partner Company** (on page 22)

**Change a Company's Password Policy (OIM Only)** (on page 21)

### Learn more about...

**Manage Companies** (on page 19)

**About the Manage Companies Table** (on page 20)

## Manage Password Policies

Password policies are based on policy rules and are assigned to companies. Users that are assigned to a company must use a password that conforms to that company's password policy.

### How do I...

**Add a Password Policy for OIM** (on page 26)

**Modify a Password Policy** (on page 28)

**Delete a Password Policy for OIM** (on page 28)

**Assign a Password Policy to a Company for OIM** (on page 29)

### Learn more about...

**Manage Password Policies** (on page 22)

**About the Manage Password Policies Table** (on page 23)

**About Policy Types** (on page 23)

## Consent Settings

Create, preview, and enable a consent message to display to users in your cloud environment. You can also view the consent status and when the status changed for each user.

### How do I...

**Configure Consent Notices for Cloud Administration** (on page 7)

**Audit Consent Notices for Cloud Administration** (on page 7)

### Learn more about...

**About Consent Notices** (on page 5)

**About Personal Information** (on page 6)

**Your Responsibilities** (on page 6)

# Legal Notices

---

Oracle Primavera Cloud Services Identity Management Administration Guide

Copyright © 2016, 2019, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

This software or hardware and documentation may provide access to or information on content, products and services from third-parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.