

ORACLE®

**TALEO
CLOUD SERVICE**

ORACLE TALEO BUSINESS EDITION

**SINGLE SIGN ON SERVICE
PROVIDER REFERENCE GUIDE**

RELEASE 23C

August, 2023

Part Number: E50271-04

ORACLE®



Oracle is committed to developing practices and products that help protect the environment

Oracle Corporation World
Headquarters 500 Oracle
Parkway Redwood Shores,
CA 94065 U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Copyright © 2023, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Hardware and Software, Engineered to Work Together

CONTENTS

ADVISORY	3
WELCOME.....	3
Audience and Background.....	3
Required Knowledge and Skills.....	3
Support.....	3
QUICK START NOTES.....	4
INTRODUCTION.....	4
HOW IT WORKS	5
CONFIGURING YOUR CONNECTION IN ORACLE TBE.....	8
Getting Started; General Information Settings.....	10
Security Settings	11
User Configuration & Provisioning (Platform Access)	12
Employee Configuration & Provisioning (Talent Center Access for Perform & Onboard Customers)	13
Finish Wizard (Review Page)	15
Save Connection	15
INFORMATION FOR YOUR IDP SET UP	16
SAML SAMPLE XML	18
NEW ACCOUNT PROVISIONING	19
SAML Attributes.....	19
SINGLE SIGN ON ERROR MESSAGES	21
SINGLE SIGN ON ONLY SETTING	21
Displaying SSO Only Field on Page Layouts	22
Single Account Update	23
Mass Account Updates	24

ADVISORY

Please ensure that you are working with the latest version of the Oracle TBE SSO Service Provider Set Up Guide.

The latest version is available on the Oracle Technology Network at:

<https://www.oracle.com/technical-resources/documentation/taleobusiness.html>

WELCOME

Audience and Background

This guide is intended for information technology professionals who plan to configure Oracle Taleo Business Edition single sign on service provider support with their corporate single sign on identity access portal.

Required Knowledge and Skills

Use of this guide assumes you are already familiar with the following:

- Oracle Taleo Business Edition (click Knowledgebase & Help sections from your Taleo instance)
- SAML 2.0
- SSO Identity Portal (IdP) setup experience (with your identity management solution)
- SSO Service Provider (SP) setup experience (with other/similar applications)

An identity provider (IdP) can be purchased by a number of vendors or custom built by/for your organization, Oracle Taleo cannot be responsible for providing IdP set-up support or code. Oracle Taleo assumes that your SSO set-up delegates are experts in their platform of choice. If assistance is needed, please contact your IdP providers/developers or post your question on Oracle Applications Customer Connect for potential feedback by other customers.

Support

Contact Oracle Support for any technical issues as they pertain to the SSO Setup and troubleshooting or to provide feedback regarding this documentation.

- **Online:** Go to [Information Center Portal](#) to submit, update or review a Service Request. You can also access our Knowledge Base, Oracle Applications Customer Connect and our Status Center.
- **Phone:** Call the appropriate phone number based on your location found at [Oracle Support](#).

To ensure that the Service Request is routed correctly right away, please use the **Service Type: Oracle TBE Integration Cloud Service** and the **Problem Type: SSO Setup**.

Customers should be prepared to provide the following information to help expedite the service request:

1. Have you downloaded the SSO guide and completed the initial setup prescribed?
2. What is your Company Code?

3. What SSO Identity Provider (IdP) are you using (ADFS, Azure, Okta, SecureAuth, etc)?
4. Will the SSO connection be used for users, employees, or both?
5. Will there be new users/employees created via the New User/Employee provisioning feature?
6. Will the users/employees be access TBE only via SSO?

QUICK START NOTES

Enabling Service	<p>Access to Single Sign On should be enabled for your Oracle TBE instance.</p> <p>To enable additional Single Sign On connections in your Oracle TBE instance or if Single Sign On is not currently enabled for your Oracle TBE instance, please log a service request with Oracle Support.</p>
Required to Start Setup	<ul style="list-style-type: none"> • Make sure your Identity Provider supports the SAML 2.0 protocol. • Ensure you have licensed enough IdP connection licenses for service. • Have your Host name, Identity Provider ID, and Port details ready. • Have your Identity Provider SSL certificate ready. • Understand what Taleo field will uniquely identify the individual for login.
Authentication Support	IdP initiated and SP initiated SSO supported.
Versioning	SAML 2.0.
SAML Key	Identity Provider SSL certificate.
Supported Access Points	<ul style="list-style-type: none"> • TBE platform (USER access). • TBE employee “self service” website (Talent Center website access for Taleo Perform and OnBoard customers).
SSO Capabilities	<ul style="list-style-type: none"> • Access of existing TBE system account holder (User and/or Employee depending on access URL). • New account provisioning (when SAML attributes sent through that meets minimum requirement for record creation). • If provisioning both new Users and new Employees using the SSO connections, different SAML attribute names must be used as the primary identifier of each.

INTRODUCTION

Single Sign On (SSO) enables users to automatically log into Taleo Business Edition and/or employees to automatically log into a Talent Center Website, bypassing the TBE login pages. The user is first verified by their company network, then they access their single sign on identity portal, and by clicking the pre-configured Taleo Business Edition access link, they can then login to Taleo Business Edition automatically. The authentication occurs in the background and is handled by a SAML certificate and a unique user identifier, most commonly the individual’s email address.

Additionally, if attempting to access a URL resource within TBE and your Company Code is identified in the request, users and/or employees will first need to authenticate in their single sign on identity

portal before access is granted. This will require that the single sign on configuration contains the URL of the SSO identity provider (IdP URL).

Having an SSO infrastructure provides the following benefits:

- Productivity and usage improve as users don't have to remember separate login step and password.
- TBE Administrators spend less time managing users and resetting passwords.
- Ensures Taleo solution aligns with your corporate password and security policies.
- Provides a single place to report on user activity through your Identity Provider (IdP).

The Oracle Taleo Business Edition SSO Service Provider option requires a connection to an existing single sign on corporate infrastructure. The Oracle TBE SSO Service Provider provides the following functionality:

- An SSO Setup Wizard for configuring your IdP attributes and SAML certificates.
- The ability to receive SAML assertions from a configured IdP.
- Direct authentication/login based on SAML assertion success.
- Direct Users and/or Employees to the specified IdP for authentication on attempted access to TBE resources, if configured to do so.

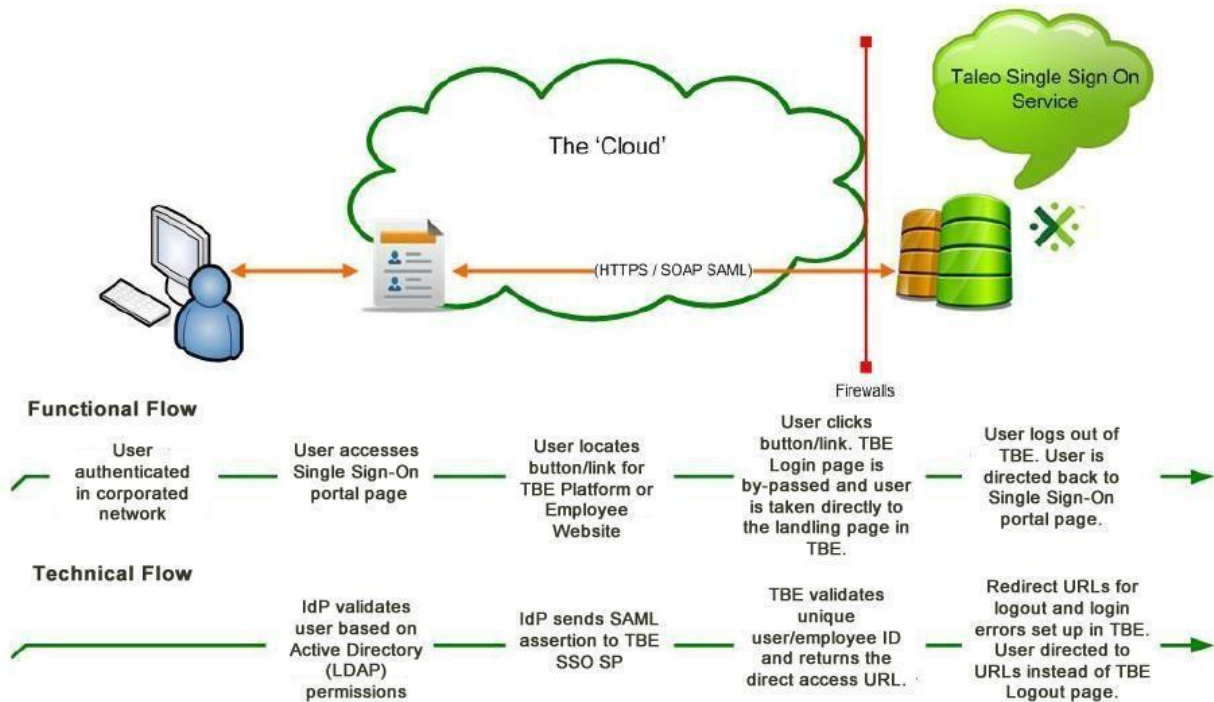
This is a free service offered to Oracle TBE Premium Service. It is activated for one connection on set up of your environment. Additional connections can be added by submitting a Service Request to Oracle Support.

HOW IT WORKS

Single Sign On contains two major components:

- An Identity Provider (IdP), also known as Identity Assertion Provider; which is an authentication module verifying users with their corporate network while also providing single click access to other permission based corporate applications based on permissions.
- A Service Provider (SP) that supports receiving SSO SAML assertions/messages. In this case, Taleo Business Edition is the SSO Service Provider.

From a functional standpoint, a user is permitted to log into their corporate network, from there they will access their IdP which includes a link to either or both the Taleo platform and employee self-service website (for Onboard and Perform customers), and clicking the link provides direct access to the Taleo application (bypassing any Taleo login screen):



From a technical perspective, your IdP sends Taleo a SAML assertion, Taleo responds with authentication and a direct access link. This process requires a supporting infrastructure for SAML 2.0.

Taleo (TBE) also supports Service Provider initiated Single Sign On where attempts to access a resource within Taleo directly, for example from a URL in an Email or from a bookmarked URL, will redirect the user or employee to the customers Identity Provider to first authenticate before granting access.



Please Note: Taleo Single Sign On service is not a mapping or an integration of user details and passwords from a customer's Active Directory or LDAP instance to Taleo. In fact, for security reasons, Taleo does not expose passwords through any system manner (API, reports, merge fields, on-demand backup, etc.) nor does Taleo recommend that customers share externally their LDAP or corporate network details. Instead, Taleo Single Sign On is for customers who have an existing SSO SAML infrastructure that can send SAML assertions for credentialing and identity matching, which corresponds to the SSL certificate and configurations in Taleo.

Customers are responsible for providing the identity provider portal that will send Taleo the SAML assertion/request for single sign on handshaking. Technically apt folks may build their own however there are many benefits to purchasing a provider solution.

Claims Behavior – Taleo requires a specific claim name to be sent in the SAML assertion from the identity provider in order to be properly identified and used for user and/or employee authentication based on the Taleo Field Name chosen to map to:

- For Users:
 - “User.loginName” if authenticating based on Taleo User’s Username
 - “User.email” if authenticating based on Taleo User’s Email

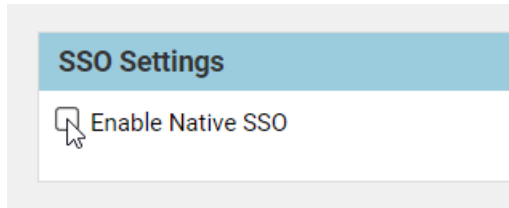
- For Employees:
 - “Employee.ewsLogin” if authenticating based on Taleo Employee’s Talent Center Login ID
 - “Employee.email” if authenticating based on Taleo Employee’s Email
 - “Employee.employeeNumber” if authenticating based on Taleo Employee’s Employee Code

If one of these specific names is not used, TBE will attempt to validate based on the “NameID” value in the SAML assertion.

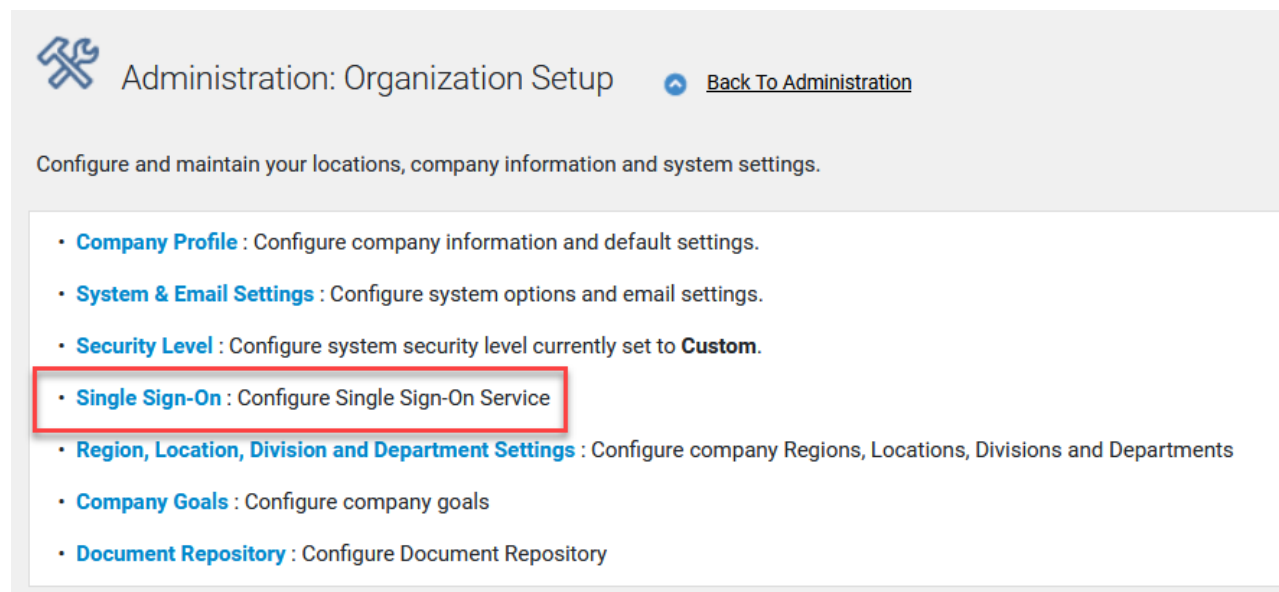
CONFIGURING YOUR CONNECTION IN ORACLE TBE

Enable Native SSO:

Administrator can enable NativeSSO for the customer by selecting the checkbox – “Enable Native SSO”. This option is available to administrators under Administration > Organization > System & Email Settings. Scroll near the bottom of the page.



Once turned on, a single sign-on wizard will be enabled within your Oracle Taleo Business Edition instance. This wizard is available to Administrators under the Administration Organization settings page:



Please Note: If you do not see the 'Single Sign-On' link on this page, please contact Customer Support to enable this feature.

By clicking on the Single Sign-On link you will be taken to your SSO connections listing page.

The top of the page displays the number of connections you have available; this represents the amount of concurrently 'Enabled' IdP connections that are available for your Taleo Business Edition instance. Most customers will have one SSO connection available. You may want to use more than one if your corporation manages more than one IdP for different subsets of users. Additional SSO Connections can be enabled for your Oracle TBE instance at no cost if requested through an Oracle Support service request.

The IdP Connections list view provides a listing of all the IdP connections that are configured in enabled and disabled status, if any, within your Oracle TBE instance in a quick view format.

Administration: Single Sign-On Configuration [Back to Organization Setup](#)

Provision connections to your Identity Providers.
You are set up for up to 5 connection(s) enabled. You currently have 4 additional connection(s) available.

[Delete](#) [Enable](#) [Disable](#) [Sync Connections with Native SSO Server](#) [Export SP Metadata](#)

<input type="checkbox"/>	Name	Description	Status	User Single Sign-On Enabled	User Creation Enabled	Employee Single Sign-On Enabled
<input type="checkbox"/>	IDPOne	Test Connection	Enabled	Yes	Yes	Yes

[Delete](#) [Enable](#) [Disable](#) [Sync Connections with Native SSO Server](#) [Export SP Metadata](#)

The list view provides a quick link “Add Connection” which should be clicked for adding additional connections when required.

In addition, the list view provides an outline of all configured IdP connections including:

- The name of the connection
- A description of the connection
- If SSO is enabled for Users
- If SSO is enabled for new account provisioning
- Action button containing a view and edit action when the drop-down arrow is clicked.



Please Note: Taleo Onboard and Perform customers will also see if Employee SSO is enabled and new employee record creation is enabled per IdP connection. By Definition: An Employee is a user who needs access to the Talent Center while a User is an individual who needs access to the Taleo Business Edition platform as an Administrator, Manager, Review Manager, Review Approver, etc.

There is also a Single Sign On ‘History Log’ at the bottom of the screen. The history log allows for better auditing and tracking of SSO communication and configuration changes. The history log will display the last 10 items with a ‘printable view’ link to access additional logs. The following items will be tracked through the SSO History Log:

IDP:

- Connection created success/error
- Connection enabled success/error
- Connection disabled success/error
- Connection deleted success/error

USER SSO:

- Record created success/error
- Login error to TBE Platform

EMPLOYEE SSO

- Record created success/error
- Login error to Talent Center

History Log Printable View		
Date/Time	User	Content
8/16/23 8:18 AM	TBEAuto, TBEQA	Successfully created IdP connection IDPOne

When adding a new connection, you will be directed through a single sign on configuration wizard allowing you to configure your IdP within Taleo Business Edition. Start the Wizard by clicking the Add Connection link in the IdP Connections list view.

The wizard goes through a collection of screens asking you to enter in the details specific to your SSO set up. The wizard flows through the following stages:



Once you have completed the wizard, the last screen prior to SAVE will display your URL connection details to be saved & configured on your IdP. If you forget to do this at the end of the wizard, you can always choose to 'View' (and Edit) your connection at a later point in time.

'Export Metadata' button :

You may use the new 'Export SSO Metadata' button on the SSO List View. This will produce an SSO Meta Data XML file containing the URL connection details you need to configure the TBE connection(s) in your IdP. Some Identity Providers (Microsoft ADFS or Azure for example) can import the meta data file directly.

Getting Started; General Information Settings

After clicking 'Add Connection' or Edit for an existing connection, the first page you see is the General Information Settings page. This page allows you to:

- Name your connection
- Describe your connection
- Enter in your Identity Provider provided ID for this connection
- Your IdP URL (optional if utilizing SP-Initiated SSO)
- Identify if the IdP URL is the Default IdP (Only one Default IdP can exist at a time and will be the one that Users and/or Employees are redirected to upon accessing a TBE resource directly).
- Define the support protocol (SAML 2.0 is currently the only supported version) and select whether this connection is active/enabled.



Single Sign-On: IdP Connection Setup Wizard

Use the following wizard to configure the connection to your Identity Provider.

Before Starting the Connection Wizard:

1. Make sure you have your Identity Provider's PKI public certificate ready to upload.
2. Understand what Taleo field will uniquely identify the User or Employee for login.
3. Make sure your Identity Provider supports the SAML protocol.

Next > Reset Cancel

Step 1: General Information

Connection Name	<input type="text" value="IDPOne"/>
Description	<input type="text" value="Test Connection"/>
Identity Provider ID	<input type="text" value="http://...48"/>
Identity Provider URL	<input type="text" value="https://...n"/>
Default Identity Provider	<input checked="" type="checkbox"/>
Protocol	<input type="text" value="SAML 2.0"/>
Enabled	<input checked="" type="checkbox"/>

Next > Reset Cancel

Please note: The IdP Connection name must be unique across all Oracle TBE SSO Connections. If the value chosen is already used, the system will notify you when you attempt to save the SSO Connection. A new value will need to be selected that the system will validate as unique.

Security Settings

The next page in the wizard will enable you to upload or select a previously uploaded SSL *token-signing* certificate:



Single Sign-On: IdP Connection Setup Wizard

Please upload or select the PKI public certificate that will be used to validate and/or decrypt messages received from your Identity Provider.

< Previous Next > Reset Cancel

Step 2: Security Settings

Upload New Certificate	<input type="button" value="Choose File"/> No file chosen
... or Choose Existing Certificate	<input type="text" value="file_368775695452725707.cert"/>

< Previous Next > Reset Cancel

User Configuration & Provisioning (Platform Access)

The user configuration and provisioning page of the SSO set-up wizard allows you to define all the user specific attributes for single sign-on.

Not only can you turn on or off user initiated SSO from this page, but in addition are able to define your redirect URL's, define what attribute will unique identify your incoming user and lastly enable you to configure new account provisioning feature of Oracle TBE SSO support.

The screenshot shows the 'Single Sign-On: IdP Connection Setup Wizard' interface. It includes a title bar with a wrench icon and the text 'Single Sign-On: IdP Connection Setup Wizard'. Below the title bar is a subtitle: 'Please specify the Single Sign-On configuration settings that apply to Taleo users.' The interface is divided into three main sections, each with a blue header bar and navigation buttons ('< Previous', 'Next >', 'Reset', 'Cancel').

- Step 3: User Preferences**: Contains a checkbox for 'Enable Single Sign-On for Users' (checked), and two text input fields for 'Logout Page URL' and 'Error Page URL'.
- Step 4: Attribute Mappings**: Contains two dropdown menus. The first is 'Identity Provider Attribute Name' with the value 'User.email'. The second is 'Taleo User Field Name' with the value 'Email'.
- Step 5: Optional New User Provisioning**: Contains a checkbox for 'Allow Creation of New Users' (checked), a dropdown menu for 'Default Role for Created Users' with the value 'Hiring Manager', and a text input field for 'New User Email Notifications'.

Specifically, here is an outline of the available settings on the User configuration page:

Enabling Single Sign-On for Users	Boolean Value: Allows you to enable or disable SSO for platform access. Platform access is for system 'USERS' as visible on the USERS tab of Taleo Business Edition.
Logout Redirect URL	String Value: This is the URL that an IdP initiated user will be redirected too if they have clicked the Taleo logout button. If no IdP redirect URL has been defined, Taleo default logout page will display when the user logs out.
Error Redirect URL	String Value: This is the URL that an IdP initiated user will be redirected too if they have encountered an application error. If no IdP redirect URL has been defined, Taleo default error page will display with the appropriate error message.

Unique Identity Attribute Name	String Value: Allows you to define the name of the SAML attribute that will house the unique identifier you have selected in the “Taleo User Field Name” picklist for uniquely identifying users. Note: If creating new users AND employees in TBE via the SSO connection, you will need to specify unique SAML Attributes for the unique identifier for each type – user and employee.
Taleo Field Name	Picklist Value: Allows you to select the unique identifier in Taleo that you would like to identify users coming in through the SAML assertion. Taleo user unique values are: email and user name.
Allow Creation of Users	Boolean Value: Allows Creation of New Users where Attribute that uniquely identifies an individual is not found in Taleo User table.
Default Role for Created Users	Picklist Value: Allows you to define what user role an individual should be assigned when a new user has been provisioned. Please contact your defined Taleo Administrator to ensure you are selecting the correct role they would like for assignment.
New User Notifications	String Value: Allows you to enter email addresses (comma separated) for the individuals to be notified when a new user has been provisioned.

Employee Configuration & Provisioning (Talent Center Access for Perform & Onboard Customers)

The employee configuration and provisioning page **will only display if you have Taleo Perform and/or Onboard enabled** within your Taleo Business Edition instance. This is enabled for profiles defined in the Employees Tab.

Please Note: Taleo has two different account profiles: Users and Employees. Users are any profiles that require access to the Taleo Business Edition core platform (URL), including Recruiters and Hiring Managers who overlook processes, jobs and subordinates. In addition to Users, Taleo includes an account type of Employees who represents themselves to complete their self-service tasks. Employees access a self-service module called the Talent Center (Employee Website vs. the User platform). Users and Employees are mutually exclusive.

This part of the SSO set-up wizard allows you to define all the Employee specific attributes for single sign-on. You can enable and disable employee SSO from this page. In addition, you can define your redirect URL's, define what attribute will unique identify your incoming employees and lastly enable you to configure new employee creation through SAML.

Single Sign-On: IdP Connection Setup Wizard

Please specify the Single Sign-On configuration settings that apply to Taleo employees.

< Previous **Next >** Reset Cancel

Step 6: Employee Preferences

Enable Single Sign-On for Employees

Logout Page URL

Error Page URL

Step 7: Attribute Mappings

Identity Provider Attribute Name

Taleo Employee Field Name

Step 8: Optional New Employee Provisioning

Allow Creation of New Employees

Default Status for Created Employees

New Employee Email Notifications

< Previous **Next >** Reset Cancel

Specifically, here is an outline of the available settings on the Employee configuration page:

Enable Single Sign-On for Employees	Boolean Value: Allows you to enable or disable SSO for Employee website Talent Center self-service access. EWS access is available for system 'Employees' as visible on the EMPLOYEES tab of Taleo Business Edition.
Logout Redirect URL	String Value: This is the URL that an IdP initiated employee will be redirected too if they have clicked the Talent Center logout button. If no IdP redirect URL has been defined, Taleo default logout page will display when the employee logs out.
Error Redirect URL	String Value: This is the URL that an IdP initiated employee will be redirected too if they have encountered an application error. If no IdP redirect URL has been defined, Taleo default error page will display with the appropriate error message.
Unique Identity Attribute Name	String Value: Allows you to define the name of the SAML attribute that will house the unique identifier you have selected in the "Taleo Employee Field Name" picklist for uniquely identifying employees. Note: If creating new users AND employees in TBE via the SSO connection, you will need to specify unique SAML Attributes for the unique identifier for each type – user and employee.
Taleo User Field Name	Picklist Value: Allows you to select the unique identifier in Taleo that you would like to identify employees coming in through the SAML assertion. Taleo employee unique values are: email, EWS LoginName, and Employee Code.

INFORMATION FOR YOUR IDP SET UP

Once you have completed setting up your SSO connection in TBE, you can display your URL connection details to be saved & configured on your IdP. You can always choose to 'View' (and Edit) your connection at any time in the Single Sign On screen in TBE.

You will need the following data points to configure the connection with Oracle TBE SSO SP in your chosen IdP.

1. Identity Provider ID ("Issuer" ID) & Service Provider ID ("Audience")

General Information Edit

Connection Name: **IDPOne**

Description: **Test Connection**

Identity Provider ID: **http://www**

Identity Provider URL: **https:// /saml**

Default Identity Provider: **No**

Service Provider ID: **http://www.oracle.com/tbe/sp**

Protocol: **SAML 2.0**

Status: **Enabled**

2. Endpoint/ACS/Recipient/Destination/Base URL – varies by server

Single Sign-On Access URLs

User Access URL (Platform): **https://lde.tbe.taleo.net:443/nativesso/login?orgCode &RelayState=https%3A%2F%2Fide.tbe.taleo.net%2Fdispat**

Employee Access URL (Talent Center): **https://lde.tbe.taleo.net:443/nativesso/login?orgCode &RelayState=https%3A%2F%2Fide.tbe.taleo.net%2Fdispatcher%2Fservlet%2FDispatcherServlet%3Forg**

The first part of the Access URL – the domain will vary be server and orgCode = The Taleo Company Code

3. Relay State (TBE Platform/User log in)

Some Identity Provider (IdP) solutions automatically apply URL encoding when the Relay State is entered into the IdP configuration. Enter the Relay State into your IdP configuration unencoded, if you IdP automatically applies URL encoding. Enter the Relay State into your IdP configuration encoded, if your IdP does not include this feature. Ultimately, the Relay State must be encoded when received from the IdP by Taleo Business Edition

Single Sign-On Access URLs

User Access URL (Platform): **https://lde.tbe.taleo.net:443/nativesso/login?orgCode &RelayState=https%3A%2F%2Fide.tbe.taleo.net%2Fdispatcher%2Fservlet%2FDispatcherServlet%3Forg**

Employee Access URL (Talent Center): **https://lde.tbe.taleo.net:443/nativesso/login?orgCode &RelayState=https%3A%2F%2Fide.tbe.taleo.net%2Fdispatcher%2Fservlet%2FDispatcherServlet%3Forg**

4. Relay State (Talent Center)

Some Identity Provider (IdP) solutions automatically apply URL encoding when the Relay State is entered into the IdP configuration. Enter the Relay State into your IdP configuration unencoded, if you IdP automatically applies URL encoding. Enter the Relay State into your IdP configuration encoded, if your IdP does not include this feature. Ultimately,

the Relay State must be encoded when received from the IdP by Taleo Business Edition

Single Sign-On Access URLs	
User Access URL (Platform):	
Employee Access URL (Talent Center):	<code>https://lde.tbe.taleo.net:443/nativesso/login?orgCode= &RelayState=https%3A%2F%2Fde.tbe.taleo.net%2Fdispatcher%2Fservlet%2FDispatcherServlet%3Forg%3F</code>

SAML SAMPLE XML

The following section provides an example of a SAML assertion as expected with Taleo Business Edition SSO SP support. The three items important to note are:

- Taleo expects the IdP issuer ID and SP ID to match what was presented on the last page of the wizard.
- Taleo expects the unique attribute assignment to be provided within the SAML attributes section.
- Taleo expects the SAML attributes section to include all values sent through for new user/employee provisioning.

```
SAML XML
<saml:Assertion Version="2.0" IssueInstant="2012-01-16T21:41:24.203Z" ID="dVHYlrE_uwPwJi7y50Oun6b8-8M"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer><<IDP_Issuer_ID>></saml:Issuer>
  <saml:Subject>
    <saml:<<Unique_User_Attribute>>Format="urn:oasis:names:tc:SAML:1.1:<<Unique_User_Attribute>>
-format:unspecified"><<Unique_User_Identifier>></saml:<<Unique_User_Attribute>>>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2012-01-16T21:46:24.204Z" Recipient="
      https://lde.tbe.taleo.net/nativesso/login?orgCode=<<Company_Code>>"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotOnOrAfter="2012-01-16T21:46:24.204Z" NotBefore="2012-01-16T21:36:24.204Z">
    <saml:AudienceRestriction>
      <saml:Audience><<SSO_SP_ID>></saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2012-01-16T21:41:24.203Z" SessionIndex="dVHYlrE_uwPwJi7y50Oun6b8-8M">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname
format:basic" Name="<<New_User_Creation_Attribute>>">
      <saml:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"><<
        New_User_Creation_Value>></saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="<<New_User_Creation_Attribute>>">
      <saml:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"><<
        New_User_Creation_Value>></saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="<<New_User_Creation_Attribute>>">
      <saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"><<
        New_User_Creation_Value>></saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="<<New_User_Creation_Attribute>>">
      <saml:AttributeValue xsi:type="xs:string" xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"><<
        New_User_Creation_Value>></saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
Name="<<New_User_Creation_Attribute>>">
      <saml:AttributeValue xsi:type="xs:string"
xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"><<
        New_User_Creation_Value>></saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>

```

```
</saml:AttributeStatement>  
< /saml:Assertion>
```

NEW ACCOUNT PROVISIONING

If choosing to enable new account provisioning (for users and/or employees), Taleo expects new account provisioning values to be provided as part of the SAML attributes section. Refer to the SAML Sample Code section for details.

At a minimum for new account provisioning, Taleo expects:

- Last Name
- Email
- User Name (for Users)
- Employee Website Login (for Employees)

Please refer to the SAML Attributes section for details on the supported values, field types and which account provisioning type is supported for the value.

SAML Attributes

User Provisioning

Provision Value	Field Type	Expected Attribute Name
First Name	String	User.firstName
Middle Name	String	User.middleInitial
Last Name	String	User.lastName
Email	String	User.email
Phone #	String	User.phone
Mobile #	String	User.cellPhone
Address	String	User.address
City	String	User.city
State/Territory	String (Match Configured Picklist)	User.state
Country	String (Match Configured Picklist)	User.country
Postal/Zip	String	User.zipCode
Status	String (Match Status Table Values)	User.status
Region Assignment	String (Match Region Table Values)	User.region
Department Assignment	String (Match Department Table Values)	User.department
Division Assignment	String (Match Division Table Values)	User.division
Location Assignment	String (Match Location Table Values)	User.location
User Name	String (Must be unique)	User.loginName

User Role	String (Match Role Assignment Table)	User.role
-----------	--------------------------------------	-----------

Employee Provisioning

Provision Value	Field Type	Expected Attribute Name
First Name	String	Employee.firstName
Middle Name	String	Employee.middleInitial
Last Name	String	Employee.lastName
Email	String	Employee.email
Phone #	String	Employee.phone
Mobile #	String	Employee.cellphone
Address	String	Employee.address
City	String	Employee.city
State/Territory	String (Match Configured Picklist)	Employee.state
Country	String (Match Configured Picklist)	Employee.country
Postal/Zip	String	Employee.zipcode
Status	String (Match Status Table Values)	Employee.status
Region Assignment	String (Match Region Table Values)	Employee.region
Department Assignment	String (Match Department Table Values)	Employee.department
Division Assignment	String (Match Division Table Values)	Employee.division
Location Assignment	String (Match Location Table Values)	Employee.location
Employee Code	String (Must be unique)	Employee.employeeNumber
Employee Website Login	String (Must be unique)	Employee.ewsLogin



Please Note: Taleo Business Edition allows for customization of field names and external values through the Administration panel of your Taleo instance. If any attribute mapping is not working, consult your Administration, Customize Fields, User (or Employee) fields and double check the External Field Name column matches your SAML attribute name.

SINGLE SIGN ON ERROR MESSAGES

If there is a configuration error, users may be shown an error message. Below are examples of errors and possible causes.

Error Message	Possible Cause(s)
"System Error" "500 Error"	Incorrect TBE configuration including: <ul style="list-style-type: none">• Incorrect Identity Provider ID• Incorrect Identity Provider certificate used (should be "signing" certificate)• Incorrect Attribute Settings• Incorrect Identity Provider configuration including: Incorrect use of Access URLs ("Audience", "Target", "Relay State")• SAML assertions are not signed• Attributed not set to Base64 encoding• Mismatched attribute names• Expired certificate
"malformed http request" "Come Back Soon" "The page you are trying to reach is no longer available"	<ul style="list-style-type: none">• Incorrect "Target" or "Relay State" URL in the Identity Provider Configuration• Incorrect URL encoding in Relay State URL
"no protocol id"	Incorrect "Consumer", "Destination" and/or "Recipient" URL(s) used
"Authentication Failed"	Browser cache issue

SINGLE SIGN ON ONLY SETTING

When Single Sign On is licensed, a new user permission field (and employee field for Perform and Onboard customers) will be available within Taleo Business Edition called "Access Only Through SSO".

This Boolean permission (setting field) will enforce the user to come through the IdP solely. It handles this by the following permission restriction features:

- Prevents user from logging in directly to Taleo with any existing credentials a user has. Instead, will display an error notice of:

"Your system administrator has restricted login from outside of your corporate network. Please contact your Taleo Administrator for details."

- Hides the user password reset control from the application (My Settings page), preventing the user the ability to reconfigure any password.

- Prevents user password reset email to be sent out if they click the “Forget your password?” from the TBE login page AND if the Taleo Administrator resets the user’s password.□

Displaying SSO Only Field on Page Layouts

To display the permission field in Taleo Business Edition for viewing and editing, you will need to add the field to your page layouts. This can be done through your Taleo Business Edition Administration panel.

Please go to the Administration tab and navigate to the Customize Recruit, Perform or OnBoard (will vary depending on what modules you have licensed). Under the Customize Pages section, click the Customize Page Layouts hyperlink.

If you want to add the User permission field, navigate to the User Pages area in the Customize Page Layouts section. Click the EDIT button on the User Page Layouts for the View and Add/Edit page layouts.

- **Add/Edit User Page Layout:** is the page displayed when you are editing or creating a new candidate record. Adding the field to this page layout allows a Taleo Administrator to edit the field.
- **View User Page Layout:** is the page displayed when you are viewing into a user record. Adding the field to this page layout allows a Taleo Administrator to just view the field.

Click insert anywhere on the page layout where you want to add this permission/setting field, choose to insert an Input Field, find the “Access Only Through SSO” field in the input field selector drop down list, and select it. The field will then be added to your page layout. You can drag the field to a new section of the page if needed by holding down your mouse button and dragging the field to your new location.

Once you have added the field to the correct spot on the page, simply click Save. Repeat this for any other User page layouts you want to add this permission field too.

Follow the same workflow to add the field on an Employee Page Layout for your employee profiles. The difference is you will need to click on the Customize Perform or Onboard Administration sub-menu to access an employee page layout and you will need to find your employee page layouts to edit. The page layouts you will need to EDIT are:


- Add/Edit Employee Page Layout: is the page displayed when you are editing an existing or creating a new employee record. Adding the field to this page layout allows you to edit the value.
- View Employee Page Layout: is the page displayed when you are viewing in to an employee record from the platform. Adding the field to this page layout allows an approved user to just view the field /permission.

For additional details on field updates, page layouts or other Administration navigation/processing, please work through your Taleo Administrator for guidance, access the Resource Center or contact Oracle Support.

Single Account Update

Once you have enabled the fields on your page layouts, a single account can be edited and/or viewed with the field permission (based on what page layouts you have placed the field on and your permissions to view that page layout).

By selecting the check box to true, the Single Sign On workflow will be active for that account once you have clicked the 'Save' button:

 User: TBEQA TBEAuto

• To temporarily disable this user's account, select the "No Access" role.

General Information:

First name: TBEQA	Fax: <input type="text"/>
* Last name: TBEAuto	Mobile #: <input type="text"/>
Middle: <input type="text"/>	Requisition Approver: <input type="checkbox"/>
* Email: <input type="text"/>	Offer Approver: <input type="checkbox"/>
* User name: <input type="text"/>	Employee: [Select Employee]
Title: <input type="text"/>	Performance Review Manager: <input type="checkbox"/>
Manager: --None-- <input type="button" value="v"/>	Performance Review Approver: <input type="checkbox"/>
Location: Please select <input type="button" value="v"/>	Compensation Manager: <input type="checkbox"/>
* Role: Administrator <input type="button" value="v"/>	Compensation Approver: <input type="checkbox"/>
* Status: Employee <input type="button" value="v"/>	Compensation Contributor: <input type="checkbox"/>
<input type="checkbox"/> Access only through SSO: <input checked="" type="checkbox"/>	Requisition Recruiter: <input type="checkbox"/>

Mass Account Updates

There are two general methods to conducting a mass update of users and/or employees with this permission value:

- Taleo Business Edition web services API (REST and SOAP options available). Please refer to the API guide(s) for additional details. Available here:
<http://www.oracle.com/technetwork/documentation/default-1841567.html>
- Taleo Business Edition import workflow which allows for upsert of fields with existing employee or user accounts.

The rest of this section discusses the later method, using Taleo's import workflow to mass update your accounts with the new permission.

Please Note: Conducting a mass update of any records within the system is not undoable. Taleo recommends you first test the process with a created test record first, and then a subset of test records second. Only after should you try this method with actual live users/employee records and only take a subset of records to update at any one given time. Any user initiated error can affect your profiles in the system permanently.

The process of conducting a mass update requires:

- Add/Edit Employee Page Layout: is the page displayed when you are editing an existing or creating a new employee record. Adding the field to this page layout allows you to edit the value.
- Running a Taleo Insight report to extract the required fields of your accounts
- Exporting that report to Excel
- Adding an additional field of 'SSO' with the correct value of True/False
- Saving that Excel worksheet as a CSV file
- Importing the CSV into Taleo through the Import Wizard with your new permission set

To start the process, assuming it is users you would like to mass update, you will create a user report for export. Navigate to the Reports tab within Taleo Business Edition and select the Create Report option / sub-menu. Choose your topic of Users by Status:

The screenshot shows the 'Create Report: Select Topic' screen. At the top, there is a pie chart icon and the text 'Create Report: Select Topic'. Below this is a navigation bar with tabs for 'Candidates', 'Requisitions', 'Compliance', 'Users', and a gear icon. The 'Users' tab is active. In the main content area, there are three radio button options: 'Users by Status - Report on users by status and role. Includes the Users, Status, and User Manager table.', 'Users' History Log - Report on activity by user. Includes the users and history log tables.', and 'Users by Employee - Report on Users by Employee using any combination of fields from User and Employee'. The first option is selected and highlighted with a red rectangular box. A 'Next >' button is located in the top right corner of the main content area.

Click the Next button to continue to your report builder.

You can name the report whatever your preference is, select the Layout 'Very Wide Table'.

Ensure your selected Display Fields include the following from the Users table, which is available from the More menu:

- User name
- Last name
- Role
- Status
- Email

You can choose a Parameter field of any value that you want to filter out your Users on. Status parameter (of Employee) is what Taleo recommends.

Click the Next button once your report has been configured:

The screenshot shows the Report Designer interface. At the top right, there is a legend: **Red = Required Information**. The main configuration area includes:

- Report Name:** User Report
- Description:** (empty text box)
- Layout:** Very Wide Table (dropdown menu)

Below this is a section for field selection:

Select a field from the table, select a different table under More or click on Expressions.

Buttons: **Add Field**, **Remove Field**, **Add To Expression**

Display Fields: Users, User name, Last name, Status, Role, Email

Parameter Fields: Users, Status

Buttons: **Add Parameter**, **Remove Parameter**

At the bottom right, there are navigation buttons: **< Back**, **Next >**, and **Cancel**.

Status	Expressions	Users	
Division		Email	✓
First name		ID	
Last name		Locale	✓
Location		Mobile #	
Phone #		Role	✓
Status		Title	✓
User name			✓

Once you reach the Report Designer, simply drag and drop your display fields on to the report and click the Save button:

Design Report Layout

Report Name: User Export

Report Description: User report used for mass update of User accounts

Note: The data set that displays in the right panel is a sample data set only.

Refine Fields Assign Access Run Report

Users - User Name	Users - Last Name	Users - Email	Users - Role
			Hiring Manager
			Hiring Manager
			Administrator
			Hiring Manager
			Agency
			Administrator
			Administrator
			Administrator
			Administrator

Please refer to the Help>Reports guide for more detailed information on creating custom reports.

Once your report is saved, you can then run your report by navigating back to the Reports>Run Report, and locating the report under the User's tab. One you hover over the report, click the Run button.

Run Report

Favorites Candidate Requisition User

History Logs - Report on the action logs for each candidate, requisition and user.

User Activity - Report on how often our users are using the system.

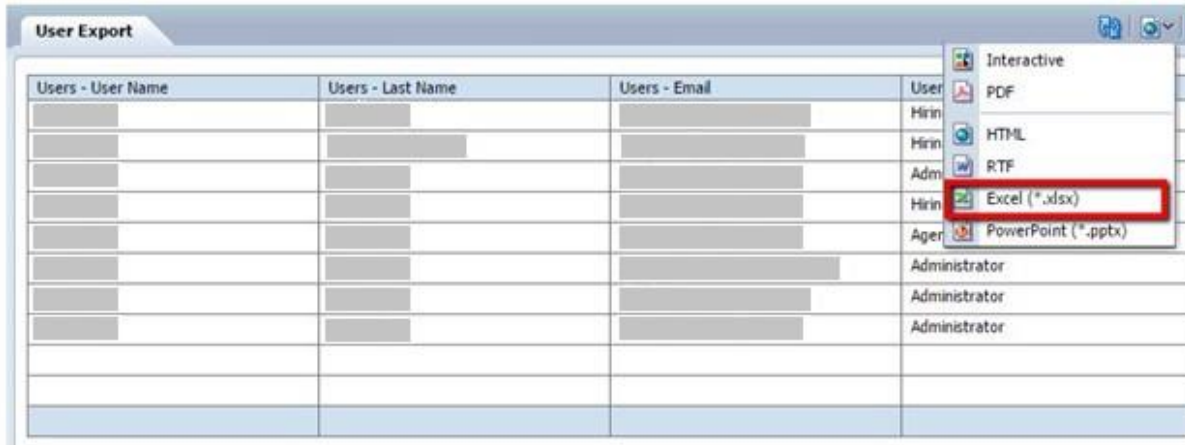
User Report for Export - Sample report created to export user data

Run Schedule Favorite Refresh

Once the report has been executed, select Excel from the menu in the top righthand corner of the report:

Reports will return a maximum of 20,000 rows of data.

Modify Parameters Edit Report Edit Layout Access BIP



The report will automatically open to your local instance in Excel where you can choose to save it on your desktop. The Excel report will need to be manipulated by:

- Adding a column called SSO
- Adding values in your SSO column with either True or False if SSO-Only Permission is checked or not.

* These changes are depicted in Red in the following screenshot:

	A	B	C	D	E
1	Users - User Name	Users - Last Name	Users - Email	Users - Role	SSO
2				Hiring Manager	TRUE
3				Hiring Manager	TRUE
4				Administrator	TRUE
5				Hiring Manager	TRUE
6				Agency	TRUE
7				Administrator	TRUE
8				Administrator	TRUE
9				Administrator	TRUE

Click the Save As and choose to save the Excel report as a CSV file. Choose OK to the removal of formatting warning message.

You can now go through the Taleo Business Edition Import Wizard to process your mass account update.

Navigate to the Users tab and select the Import sub-menu link:

[Home](#)
[Requisitions](#)
[Candidates](#)
[Contacts](#)
[Users](#)
[Reports](#)

Users: Import Wizard

Use this wizard to import User data from Excel. [Read More!](#)

Prepare To Import:

- If you plan to import User records from a CSV file, please see the TBE video for Importing Candidates on the [Resource Center](#) as it will guide you through how to configure a CSV file for upload.
 - * When importing from a CSV file, compare your data to the available User Fields. Check with your Administrator if you need custom fields or custom picklist values.
- You can use the Upload to maintain your Users. If the upload includes the User Login Name, it will match on the existing User and update the User. If the User Login Name does not match with an existing record, a new User will be created. You can use this to set a User to 'No Access' when the User leaves your organization.
- Make sure the file you plan to import is less than 10MB. (a CSV file with 5000 or fewer records)

* **CSV import recommendation:** import a small test file of 5 records before importing all of your data to ensure that your file is properly formatted.

Next > Cancel

User Creation Import Options

This option will allow you to copy configuration and settings from a specific user that currently exists in Taleo Business Edition

Copy settings from existing User: [\[Select User\]](#)

Employee Creation Import Options

Create an Employee - Select this option if you would like the import to create an Employee record and associate it with the User your are uploading. It is a best practice that all Users should have a corresponding Employee record.

Connect Existing Employees - If checked, the system will expect the CSV to include a column for Employee Code. It can use the Employee Code to connect Users within the import file with Employees that already exist. If there is no Employee Code provided, a new Employee Record will be created.

Next > Cancel

Follow the following steps:

- Click Import
- Uncheck any/all Employee Creation Import Options
- Select your CSV file for import
- Do not select any default role or statuses
- Map User name to the correct column of your CSV file
- Map Last name to the correct column of your CSV file
- Map Role to the correct column of your CSV file
- Map Status to the correct column of your CSV file
- Map Email to the correct column of your CSV file
- Map the "Access Only through SSO" field to the correct column of your CSV file
- Select the Update All option and Proceed
- Click OK

Please Note: Updating of records occurs in the background, but you will be emailed once the process has completed. This can take seconds to minutes depending on the number of records you are updated. We recommend first trying a sample file with one or two records in it.

Follow the same process for Employee mass updates, however the following differences are noted:

- The Report will be an Employees report under Perform and/or Onboard:

es Accounts Contacts Employees Onboard/Offboard Reviews Compensation Users **Reports** Position Control Courses

Create Report: Select Topic

Recruit Perform **Onboard**

Employees Onboard/Offboard Tasks More

Next >

- Employees** - Report on employee-specific data. Includes the employees, employee's manager, employee's review manager, locations, employment history, education history, references, certificates and licenses, and residence history tables.
- Employees' History Log** - Report on all employee activity and contact. Includes the employees, tasks, comments, history log, history creator and locations tables.
- Employee Packets** - Report on onboarding and offboarding activities by employee. Includes the employees, employee's manager, activity packets, activity packet creators, and locations tables.

The only fields you require in your report are:

- Employee Code
- Last Name

The Import function for Employees is under the Employees tab in Taleo Business Edition

Choose to "Import Employee data from CSV file" and ensure no status or role values are selected.

Please Note: Conducting a mass update of any records within the system is not undoable. Taleo recommends you first test the process with a created test record first, and then a subset of test records second. Only after should you try this method with actual live users/employee records and only take a subset of records to update at any one given time. Any user-initiated error can affect your profiles in the system permanently.

Document History

Date	Changed By	Comments	Version
11/11/2013	Mark C.	Corrected the base URL examples in the Sample SAML XML and Sample SAML Metadata XML	V135_1
4/17/2015	Mark C.	Updated with SP Initiated SSO configuration options. Clarification of SAML Attribute Name usage if provisioning both Users and Employees using SSO Added Export Meta Data Button description. Updated Mass User/Employee Update section to reflect new Reporting usage.	

10/22/2019	Michael D.	Updated New User Provisioning expected attributes Replaced references of "EWS" with Talent Center Hid Personal Identifiable Information Removed "SAML SP METADATA XML" output Added ERROR MESSAGES table Updated TOC	
7/7/2020	Michael D.	Updated formatting of tables Updated links for OCI Updated new user provisioning First name Field Updated Error Messages for OCI	V20C
8/10/2020	Michael D.	Added claim behavior details Minor grammar fixes Updated UI screen shots	V20Cv2a
8/10/2023	Kathy D	Updated screen shots and information about Native SSO	V23C