Oracle Taleo Cloud for Midsize (Taleo Business Edition)

Security Features

RELEASE 18B

ORACLE

TABLE OF CONTENTS

REVISION HISTORY

This document will continue to evolve as existing sections change and new information is added. All updates appear in the following table:

Date	Feature	Notes
01 MAY 2018		Created initial document.

OVERVIEW

This guide outlines the settings in Oracle Taleo Cloud for Midsize (Taleo Business Edition) that are related to security.

GENERAL SECURITY LEVEL SETTINGS

The settings in this section can be accessed by an Administrator by selecting **Administration>Organization>Security Level**.

There are four security levels (Low, Medium, High and Custom) based on how strictly you want to handle user passwords, unsuccessful login attempts, data locks, and session expiration due to inactivity or maximum amount of time logged in.

Defaults are provide for the Low, Medium, and High levels, and cannot be modified. Choose the Custom option to modify the security settings.

Modifications to the security levels affect only new users and passwords added to Taleo Business Edition. For example, if you currently are requiring passwords have a minimum of 6 characters and you change it to 8, existing passwords using only 6 will be accepted until the password is reset or expires.

The password settings apply to user passwords for TBE, as well as candidate passwords for the Career Center and the legacy Careers Website, and employee passwords for the Talent Center and the legacy Employee Website, unless otherwise noted.

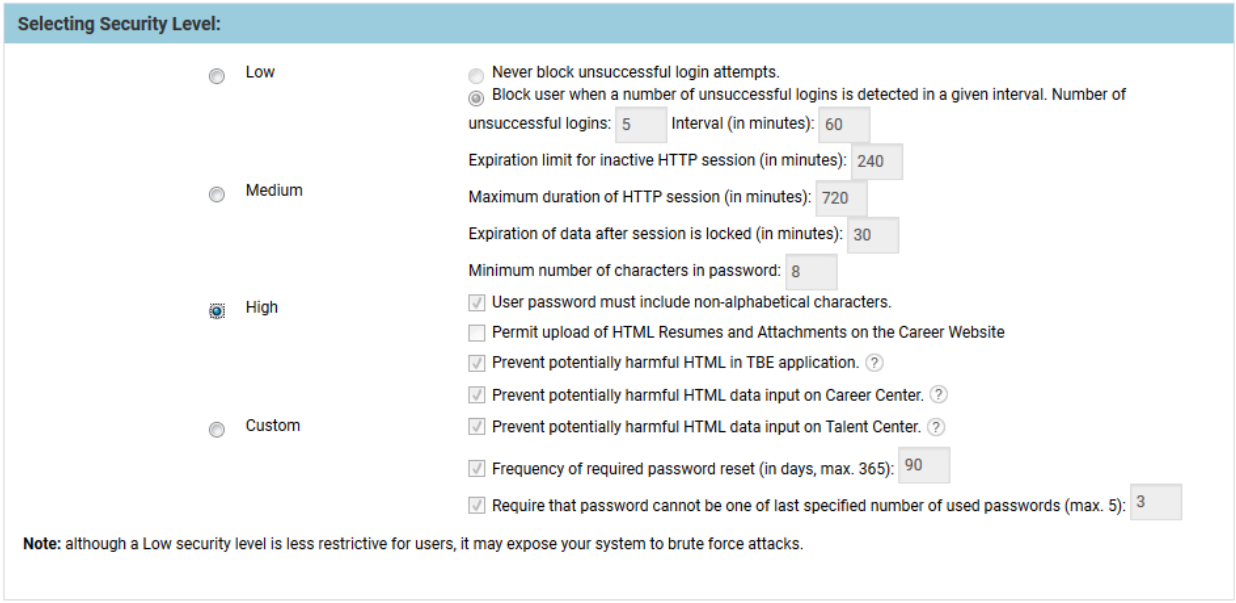
NOTE: The session timeout for the Career Center is 24 hours and cannot be changed.
Also, the settings 'Frequency of required password reset' and 'Require that passwords cannot be one of the last used passwords' do not applies to Candidates on the Career Center/legacy Careers Website. Candidate passwords do not expire.

HIGH SECURITY LEVEL (RECOMMENDED)

The following settings are part of the High security level:

- Block user when a number of unsuccessful logins is 5 in a 60 minute interval
- Expiration limit for inactive HTTP session is 240 minutes
- Maximum duration of HTTP session is 720 minutes
- Expiration of data after session is locked is 30 minutes
- Minimum number of characters in a user password is 8
- Password must include non-alphabetical characters
- Prevent potentially harmful HTML in TBE application
- Prevent potentially harmful HTML data input on Career Center
- Prevent potentially harmful HTML data input on Talent Center

- Frequency of required password reset is every 90 days
- Require that passwords cannot be one of last 5 used passwords



Settings included in the High Security level

The system always checks for potentially harmful HTML when saving data in fields such as the job description and on the Talent Center and Career Center. When these three 'potentially harmful' settings are checked, the user is warned that the data input may contain harmful HTML, and the user can correct the problem manually, or accept the suggestion 'clean' version of the HTML. If these settings are unchecked (available with a Custom setting only) the system still checks for harmful HTML and still gives the warning to the user, but the user has the option to continue, which will save the content with the HTML intact.

MEDIUM SECURITY LEVEL

The following settings are part of the Medium security level:

- Block user when a number of unsuccessful logins is 10 in a 30 minute interval
- Expiration limit for inactive HTTP session is 480 minutes
- Maximum duration of HTTP session is 720 minutes
- Expiration of data after session is locked is 60 minutes
- Minimum number of characters in a user password is 8
- Prevent potentially harmful HTML in TBE application
- Prevent potentially harmful HTML data input on Career Center
- Prevent potentially harmful HTML data input on Talent Center
- Frequency of required password reset is every 120 days
- Require that passwords cannot be one of last 1 used passwords

LOW SECURITY LEVEL

The following settings are part of the Low security level:

- Never block unsuccessful login attempts
- Expiration limit for inactive HTTP session is 720 minutes
- Maximum duration of HTTP session is 1440 minutes
- Expiration of data after session is locked is 240 minutes
- Minimum number of characters in a user password is 6
- Prevent potentially harmful HTML in TBE application
- Prevent potentially harmful HTML data input on Career Center
- Prevent potentially harmful HTML data input on Talent Center

ADDITIONAL SECURITY SETTINGS

Also on the Security Level page is the ability to select **Security Managers**. These are Administrators who have the ability to make security changes pertaining to confidential data in the system. Security Managers have the ability to give user roles or individual users access to confidential data.

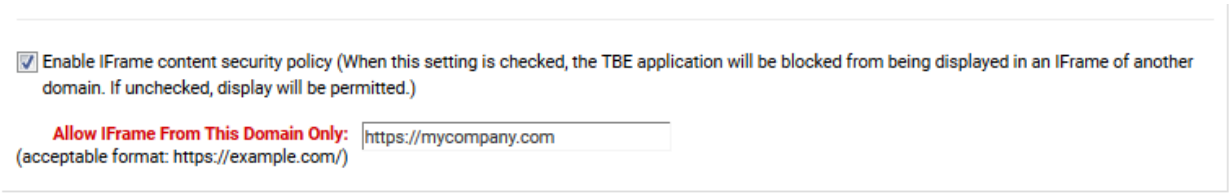
The Access Control section on this page enables you to restrict which IP addresses can gain access to your TBE system. Remove users attempting to log in from an IP address that is not deemed secure are presented with a non-access notification. You can configure this notification on this page.

At the bottom of the Access Control section is the setting:

- Enable IFrame content security policy

When this option is checked, the TBE application will be blocked from being displayed in an iFrame of another domain. It is recommended to check this option.

If you would like to allow an Iframe from one particular domain, you may enter it in the field below this setting, as seen here.



TALENT CENTER SECURITY SETTINGS

TALENT CENTER PASSWORD SECURITY SETTINGS

The Talent Center password settings are as follows, with the defaults shown:

- Lock Employee User out after 3 failed attempts
- Automatically unlock employee after 60 minutes
- Allow Recover Password Reset email option to employee
- Authenticate Employees for Manager View access
- Require username and password for eSignature (unchecked by default)

Password-specific settings, such as the minimum length, non-alphabetic characters, and password reset rules are configured in the Security Level settings.

ACCESS CONTROL

The Access Control section on this page enables you to restrict which IP addresses can gain access to the specific Talent Center. If you only want employees to log in from work, then you can add specific IP addresses to this field.

CAREER CENTER SECURITY SETTINGS

CAREER CENTER PASSWORD SECURITY SETTINGS

Password-specific settings, such as the minimum length, non-alphabetic characters, and password reset rules are configured in the Security Level settings.

ACCESS CONTROL

The Access Control section on this page enables you to restrict which IP addresses can gain access to the specific Career Center. If you have an internal Career Center that you only want employees to access from work, for example, then you can add specific IP addresses to this field.

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

Integrated Cloud Applications & Platform Services