Advanced Employee Permissions

2022.2

February 1, 2023

If this document is in private pre-General Availability status:

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility.

Access to Oracle Support

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

Sample Code

Oracle may provide sample code in SuiteAnswers, the Help Center, User Guides, or elsewhere through help links. All such sample code is provided "as is” and “as available”, for use only with an authorized NetSuite Service account, and is made available as a SuiteCloud Technology subject to the SuiteCloud Terms of Service at www.netsuite.com/tos.

Oracle may modify or remove sample code at any time without notice.

No Excessive Use of the Service

As the Service is a multi-tenant service offering on shared databases, Customer may not use the Service in excess of limits or thresholds that Oracle considers commercially reasonable for the Service. If Oracle reasonably concludes that a Customer’s use is excessive and/or will cause immediate or ongoing performance issues for one or more of Oracle’s other customers, Oracle may slow down or throttle Customer’s excess use until such time that Customer’s use stays within reasonable limits. If Customer’s particular usage pattern requires a higher limit or threshold, then the Customer should procure a subscription to the Service that accommodates a higher limit and/or threshold that more effectively aligns with the Customer’s actual usage pattern.

Beta Features

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, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or “commercial computer software documentation” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. 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 fail-safe, 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.

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, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

This documentation is in pre-General Availability status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Send Us Your Feedback

We'd like to hear your feedback on this document.

Answering the following questions will help us improve our help content:

- Did you find the information you needed? If not, what was missing?
- Did you find any errors?
- Is the information clear?
- Are the examples correct?
- Do you need more examples?
- What did you like most about this document?

Click here to send us your comments. If possible, please provide a page number or section title to identify the content you're describing.

To report software issues, contact NetSuite Customer Support.

Table of Contents

Advanced Employee Permissions

This chapter includes the following help topics:

Advanced Employee Permissions Overview

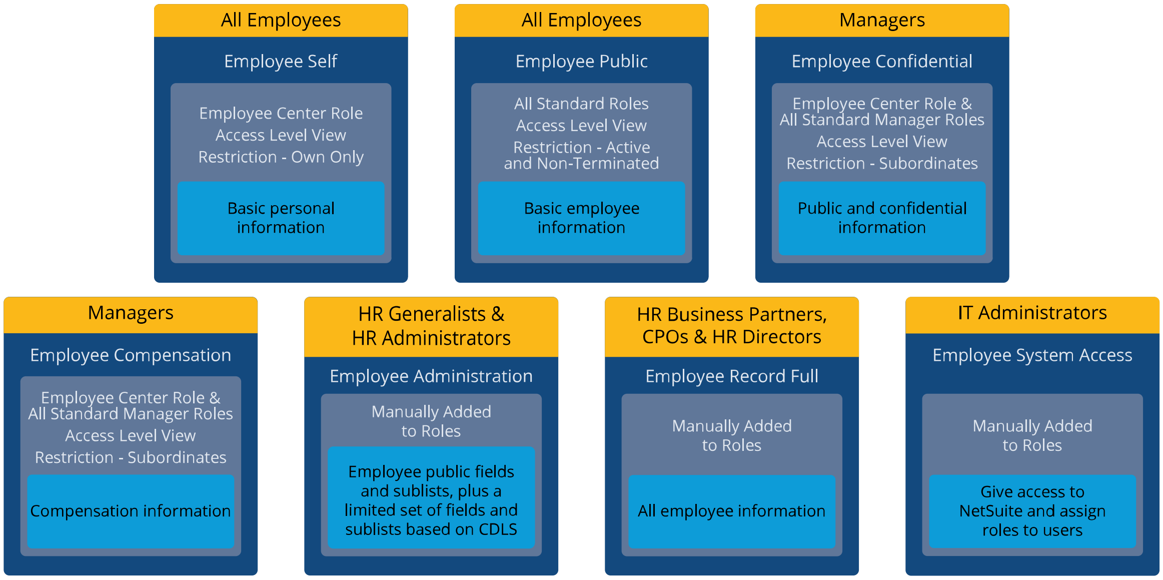
The Advanced Employee Permissions feature gives administrators control over which fields and sublists on the employee record are available to the role. This availability is based on the assigned employee permissions.

This feature includes the following permissions, which are automatically assigned to a set of standard NetSuite roles, except where otherwise noted. For more information, see Advanced Employee Permissions and Standard NetSuite Roles.

- **Employee Self –** Roles with this permission have access to basic personal information about themselves on their employee record. They can also use their Employee Center role by clicking **My Profile** under **My Information**. For more information, see Employee Self Permission Overview.
- **Employee Public –** Roles with this permission have access to basic employee information, such as job title. For more information, see Employee Public Permission Overview.
- **Employee Confidential –** Roles with this permission have access to a set of fields and sublists. For example, the **Billing Class** field, and the **Time-Off** subtab. For more information, see Employee Confidential Permission Overview.
- **Employee Compensation –** Roles with this permission have access to compensation information, such as base wage and base wage type. For more information, see Employee Compensation Permission Overview.
- **Employee Access Tab –** Roles with this permission can give users access to NetSuite and assign roles to users. The Employee Access Tab permission is not automatically assigned to any roles when the feature is enabled. For more information, see Employee Access Tab Permission Overview.

- **Employee Administration –** Roles with this permission have access to basic employee information, and fields and sublists based on Class, Department, Location, and Subsidiary (CDLS). The Employee Administration permission is not automatically assigned to any roles when the feature is enabled. For more information, see Employee Administration Permission Overview.
- **Employee Record Full –** Roles with this permission have access to all employee information. For more information, see Employee Record Full Permission Overview.

> **Note:** The Advanced Employee Permissions feature is available only for accounts with SuitePeople HR provisioned. For more information, see the help topic SuitePeople Overview.



All Employees
Employee Self
Employee Center Role Access Level View Restriction - Own Only
Basic personal information

All Employees
Employee Public
All Standard Roles Access Level View Restriction - Active and Non-Terminated
Basic employee information

Managers
Employee Confidential
Employee Center Role & All Standard Manager Roles Access Level View Restriction - Subordinates
Public and confidential information

Managers
Employee Compensation
Employee Center Role & All Standard Manager Roles Access Level View Restriction - Subordinates
Compensation information

HR Generalists & HR Administrators
Employee Administration
Manually Added to Roles
Employee public fields and sublists, plus a limited set of fields and sublists based on CDLS

HR Business Partners, CPOs & HR Directors
Employee Record Full
Manually Added to Roles
All employee information

IT Administrators
Employee System Access
Manually Added to Roles
Give access to NetSuite and assign roles to users

If your role has appropriate permission, you can create custom employee permissions to include standard fields and sublists from the employee record. You can also add custom fields and sublists to custom employee permissions. For more information, see Custom Advanced Employee Permissions.

If your role has the appropriate permission, you can also customize restrictions for Advanced Employee Permissions. For more information, see Custom Restrictions for Advanced Employee Permissions.

> **Note:** Inline editing is available only with the Lists > Employees permission at access level Edit or higher.

> **Note:** Advanced Employee Permissions lets users who have access to effective dating logs see content based on the permissions and restrictions assigned to their role. For example, roles with the Employee Confidential permission see effective dating logs only for their direct reports and below. For more information, see the help topic Effective Dating for Employee Information.

Advanced Employee Permissions Videos

Watch the following help videos for information about using the Advanced Employee Permissions feature.

- Advanced Employee Permissions Overview — Video 1 of 4
- Creating Custom Advanced Employee Permissions — Video 2 of 4
- Customizing a Role Using Advanced Employee Permissions — Video 3 of 4

Using Advanced Employee Permissions — Video 4 of 4

Before Enabling the Advanced Employee Permissions Feature

Note: The Advanced Employee Permissions feature is available only for accounts with SuitePeople HR provisioned. For more information, see the help topic SuitePeople Overview.

Warning: The Advanced Employee Permissions feature changes the way employee information is exposed to users. This feature should only be enabled by an administrator who has a thorough understanding of NetSuite. Because these changes extend to all parts of NetSuite, test this feature in a sandbox account before enabling it in a production account.

This section describes how access to the employee record, using different contexts, changes when the Advanced Employee Permissions feature is enabled. You should go through the following list before you enable the feature. If required, complete any of the recommended actions. For more information, contact NetSuite Customer Support.

- Advanced Employee Permissions and Employee Searches
- Advanced Employee Permissions and Saved Searches
- Advanced Employee Permissions and Employee List View Results
- Advanced Employee Permissions and NetSuite Reports
- Advanced Employee Permissions and Employee Templates
- Advanced Employee Permissions and Contact Records
- Advanced Employee Permissions and Subrecords
- Advanced Employee Permissions and SuiteScript
- Advanced Employee Permissions and SuiteFlow
- Advanced Employee Permissions and SuiteAnalytics Connect
- Advanced Employee Permissions and CSV Import
- Advanced Employee Permissions and SOAP Web Services
- Advanced Employee Permissions and Customizations

Advanced Employee Permissions and Employee Searches

Important: Before you enable Advanced Employee Permissions, review existing saved employee searches, and limit access to any searches that are not relevant to some users.

Note: The Advanced Employee Permissions feature is available only for accounts with SuitePeople HR provisioned. For more information, see the help topic SuitePeople Overview.

When Advanced Employee Permissions is not enabled, employees can only perform employee searches if they have the following permissions:

- Lists > Employees

- Lists > Employee Record
- Lists > Perform Search

However, when Advanced Employee Permissions is enabled, many standard NetSuite roles automatically have the Employee Public permission, and the Lists > Employee Record permission. These permissions give them the ability to perform employee searches.

Advanced Employee Permissions and Saved Searches

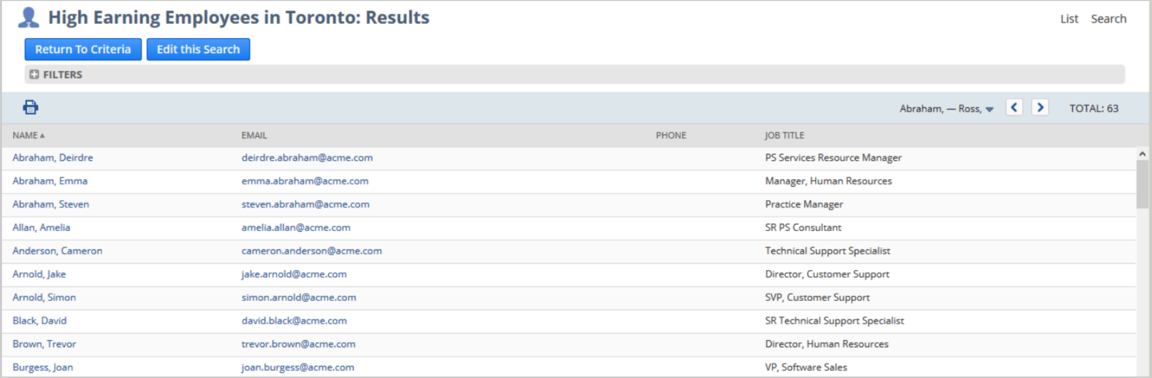
Based on the employee permissions assigned to the role, users see different results when viewing the same employee saved search. Some columns in the search results are hidden, depending on what the role has access to. When the filter criteria of a saved search uses a field unavailable to the employee permissions assigned to the role, the filter is not applied.

The following examples outline what information is exposed to a role when a saved search is run using the same filter criteria. The examples use different Advanced Employee Permissions.

Example 1 – Saved Search Results with Employee Public Permission

Advanced Employee Permissions	Filter Criteria	Reference
Employee Public	Location – Toronto Base Wage – Greater than $100,000	Employee Public Permission Overview

When a role using this permission runs the saved search, the results filter by Location because this permission does not have access to Base Wage.



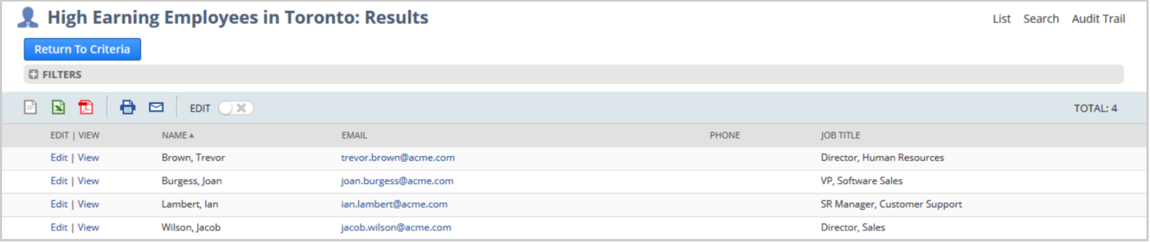
NAME ▲	EMAIL	PHONE	JOB TITLE
Abraham, Deirdre	deirdre.abraham@acme.com		PS Services Resource Manager
Abraham, Emma	emma.abraham@acme.com		Manager, Human Resources
Abraham, Steven	steven.abraham@acme.com		Practice Manager
Allan, Amelia	amelia.allan@acme.com		SR PS Consultant
Anderson, Cameron	cameron.anderson@acme.com		Technical Support Specialist
Arnold, Jake	jake.arnold@acme.com		Director, Customer Support
Arnold, Simon	simon.arnold@acme.com		SVP, Customer Support
Black, David	david.black@acme.com		SR Technical Support Specialist
Brown, Trevor	trevor.brown@acme.com		Director, Human Resources
Burgess, Joan	joan.burgess@acme.com		VP, Software Sales

Example 2 – Saved Search Results with Employee Administration Permission

Advanced Employee Permissions	Filter Criteria	Reference
Employee Administration	Location – Toronto	Employee Administration Permission Overview

Advanced Employee Permissions	Filter Criteria	Reference
	Base Wage – Greater than $100,000	

When a role using this permission runs the same saved search different results are shown. Only the employees who are located in Toronto and who have a base wage greater than $100,000.00 are shown in the saved search results. In the image below, you can see that four employees meet this search criteria.



EDIT | VIEW	NAME ▲	EMAIL	PHONE	JOB TITLE
Edit | View	Brown, Trevor	trevor.brown@acme.com		Director, Human Resources
Edit | View	Burgess, Joan	joan.burgess@acme.com		VP, Software Sales
Edit | View	Lambert, Ian	ian.lambert@acme.com		SR Manager, Customer Support
Edit | View	Wilson, Jacob	jacob.wilson@acme.com		Director, Sales

Advanced Employee Permissions and Employee List View Results

The Employees List page generates the available columns, based on the fields the role has access to. The employees listed depend on which employees the role has permission to view all the fields, and that meet the set restrictions. Seeing different employees with a different combination of permissions and restrictions is expected behavior.

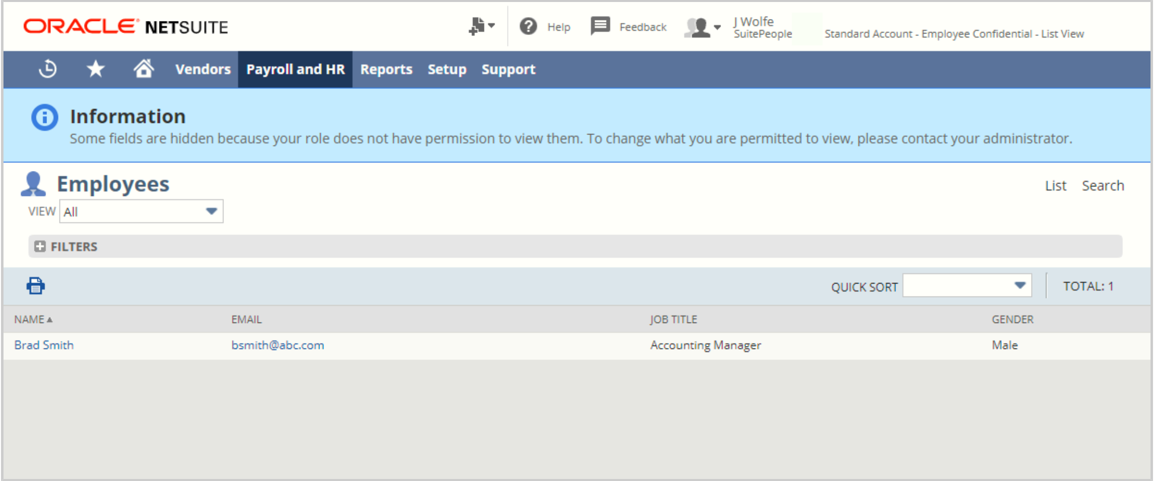
The following section gives examples of how the displayed information changes when using Advanced Employee Permissions.

Important: When using Advanced Employee Permissions you should view the Employees List page using the Basic view, instead of the default All view. With the Basic view, you see a more extensive list of employees because the basic field set is contained in most standard employee permissions. With the All view, there are more columns displayed, however, it may restrict the number of employees you see. For more information, see Example 3 – Employee List Page Results with Employee Confidential and Employee Self Permissions.

Example 1 – Employees List Page Results with Employee Confidential Permission

Advanced Employee Permissions	Default Access Level and Restriction?	Default Restriction	Fields Exposed	View	Reference
Employee Confidential	View	Subordinates	▪ First Name ▪ Last Name ▪ Email ▪ Gender ▪ Job Title	All	Employee Confidential Permission Overview

The employees that directly report to the user are shown in the list. In this example, the user has one direct report and each of the fields that are part of the Employee Confidential permission appear. The Employee Confidential permission has the default restriction of Subordinates.



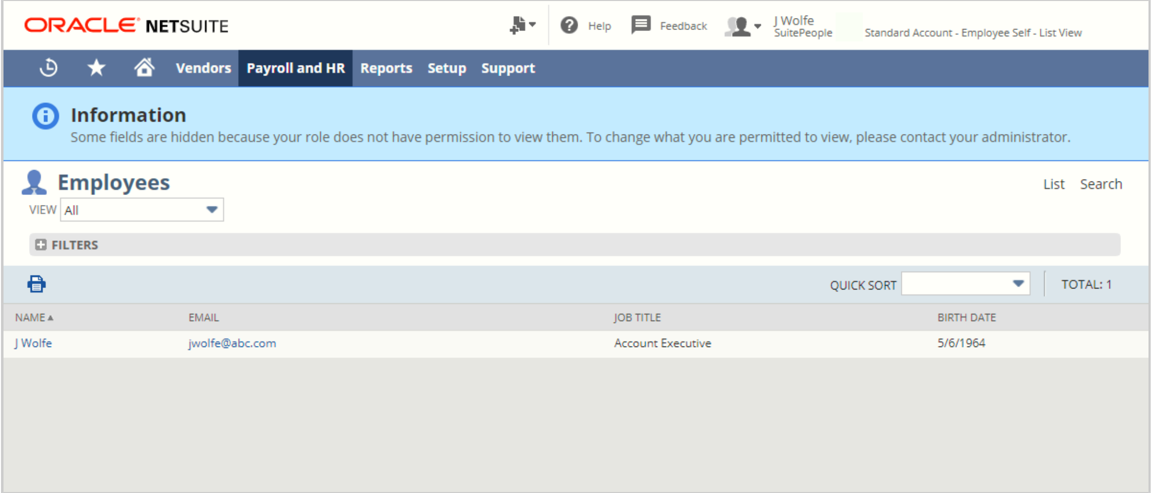
Information
Some fields are hidden because your role does not have permission to view them. To change what you are permitted to view, please contact your administrator.

NAME ▲	EMAIL	JOB TITLE	GENDER
Brad Smith	bsmith@abc.com	Accounting Manager	Male

Example 2 – Employees List Page Results with Employee Self Permission

Advanced Employee Permissions	Default Access Level	Default Restriction	Fields Exposed	View	Reference
Employee Self	View	Own Only	■ First Name ■ Last Name ■ Email ■ Job Title ■ Birth Date	All	Employee Self Permission Overview

The user sees the fields exposed with the Employee Self permission only for themselves. The Employee Self permission has the default restriction of Own Only. Therefore, the user only has access to this information for themselves on their employee record.



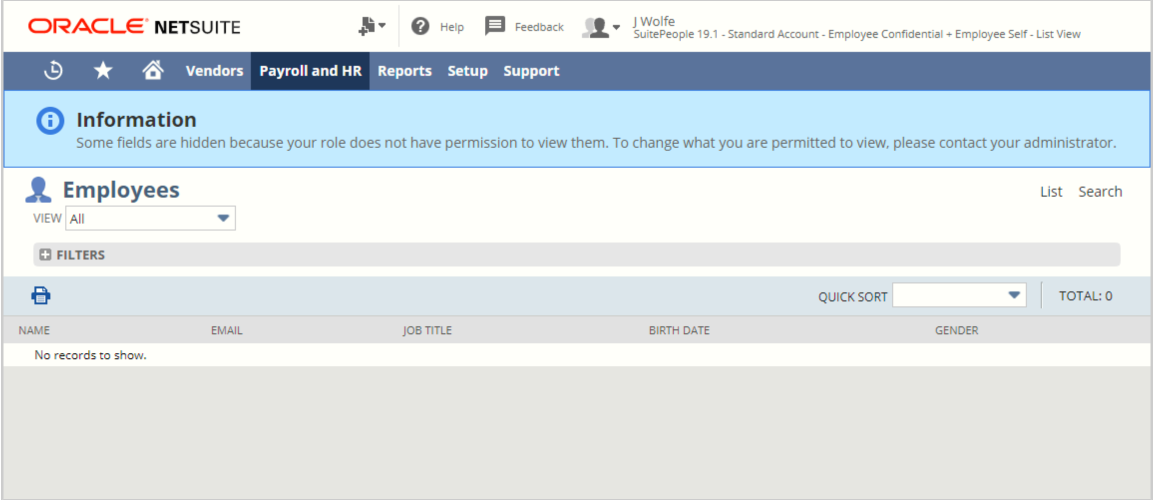
Information
Some fields are hidden because your role does not have permission to view them. To change what you are permitted to view, please contact your administrator.

NAME ▲	EMAIL	JOB TITLE	BIRTH DATE
J Wolfe	jwolfe@abc.com	Account Executive	5/6/1964

Example 3 – Employee List Page Results with Employee Confidential and Employee Self Permissions

Advanced Employee Permissions	Default Access Level	Default Restrictions	Fields Exposed	Views	References
■ Employee Confidential ■ Employee Self	View	■ Subordinates ■ Own Only	■ Employee Confidential Permission □ First Name □ Last Name □ Email □ **Gender** □ Job Title ■ Employee Self Permission □ First Name □ Last Name □ Email □ Job Title □ **Birth Date**	All and Basic	Employee Confidential Permission Overview Employee Self Permission Overview

With the Employee Confidential and Employee Self permission combination, the user sees an empty list. The **All** view on the Employees List page generates the available columns, based on field access for the role, across all roles. It displays all of the employees that match all the fields that the user has access to. When fields are removed from the view, you will see a generated information message.



Information

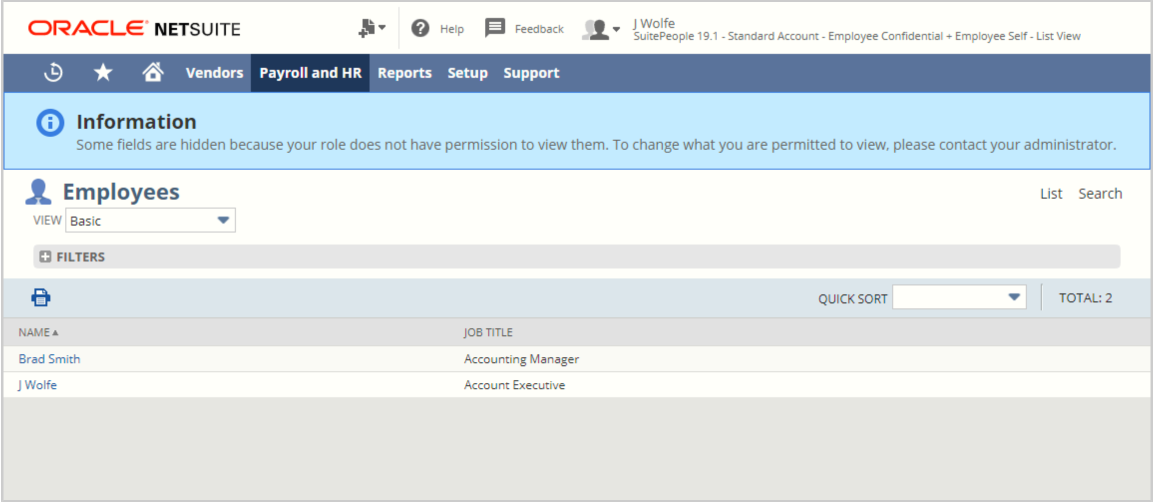
Some fields are hidden because your role does not have permission to view them. To change what you are permitted to view, please contact your administrator.

VIEW All

TOTAL: 0

NAME	EMAIL	JOB TITLE	BIRTH DATE	GENDER
No records to show.				

With the Employee Confidential and Employee Self permission combination, the **Basic** view of the Employees List page displays the users name all their direct reports. The field set contained in the Basic view is contained in most standard employee permissions.



J Wolfe
SuitePeople 19.1 - Standard Account - Employee Confidential + Employee Self - List View

Information

Some fields are hidden because your role does not have permission to view them. To change what you are permitted to view, please contact your administrator.

Employees

TOTAL: 2

NAME ▲	JOB TITLE
Brad Smith	Accounting Manager
J Wolfe	Account Executive

Advanced Employee Permissions and NetSuite Reports

Information in NetSuite reports is not governed by Advanced Employee Permissions. This means that it could be possible to accidentally disclose more information than an employee should have access to through a report. Use caution when giving employees access to reports. For more information, see the help topic Access to Reports.

Advanced Employee Permissions and Employee Templates

When Advanced Employee Permissions is enabled you can view employee templates, however you cannot create or edit employee templates. Editing or creating employee templates is supported only with the Lists > Employees permission. For more information about employee templates, see the help topic Creating an Employee Template.

Advanced Employee Permissions and Contact Records

When Advanced Employee Permissions is enabled, the **Show Employees as Contacts** field on the General Preferences page is not available. Any employees saved to a contact record do not appear on the Contacts list page. In addition, any information specific to an employee's contact record is no longer accessible.

If required, move any custom fields from the contact record to the employee record before enabling Advanced Employee Permissions.

Advanced Employee Permissions and Subrecords

Subrecords are supported only with the Lists > Employees permission.

Advanced Employee Permissions and SuiteScript

In NetSuite, account administrators have access to all the information on all record types, including the employee record. This can create issues in the following situations:

- When a user is assigned a role that has permission to create scripts.
- When a user sets a script to run as administrator.

A user could write or deploy a script that gains access to employee information that they would normally not have access to. This could potentially be used to compromise employee information.

When Advanced Employee Permissions is enabled, carefully track which roles have permission to create or alter scripts. In addition, track which scripts execute as administrator, and what they do to make sure employee information is not unintentionally leaked.

Assigning any of the Advanced Employee Permissions to a role gives partial access to the employee record. Some scripts (including third-party scripts) may fail when users attempt to access parts of the employee record that they are not permitted to access. For more information, see Advanced Employee Permissions Overview.

If needed, consider running these scripts as administrator, or revise the scripts to handle cases where some fields and sublists are not accessible.

If you have any scripts that add buttons to the employee record, ensure that they appear only when appropriate. Configure scripts so that the action being added respects the restrictions on the employee record.

Script Access

The following section outlines how script access changes when Advanced Employee Permissions is enabled.

The fields and sublists a user has access to can change depending on which employee record is being viewed or edited. This is different from other records in NetSuite, where permissions granted to a role determine just the instances of the record the role can see.

The search columns available to users are also dependent on the permissions assigned to the role.

In general, scripts should always check to see if the role has access to a field or sublist before trying to do something with it. Simply calling functions and methods that interact with fields and sublists before checking whether the role has access may result in inconsistent behavior.

For example, the **Department** field is permitted on the employee record. You do not have access, therefore, a null value is returned. If the field is empty, an empty string is returned.

Script Access Examples

When you run the following script, errors generate because the script does not check if the field exists, or whether you have access to it.

```
var employeeRecord = nlapiLoadRecord('employee', '115');
employeeRecord.setFieldValue('department', '2');
nlapiSubmitRecord(employeeRecord);
```

To check if your role has access to a field for a specific employee, load the employee record object and call `getAllFields().includes()`. If the field exists and you do have access, a `true` value is returned. In the following example, the user has access to the **Department** field for the employee with ID:115.

```
var accessToDepartment = nlapiLoadRecord('employee', '115').getAllFields().includes('department');
```

Taking the previous two script examples into consideration, you should use the following example to make sure your scripts do not fail.

```
var employeeRecord = nlapiLoadRecord('employee', '115');
var hasAccessToDepartment = employeeRecord.getAllFields().includes('department');
if (hasAccessToDepartment)
{
      employeeRecord.setFieldvalue('department', '2');
}
nlapiSubmitRecord(employeeRecord);
```

For more information about working with SuiteScript, see the help topics Suitelets and UI Object Best Practices and Client Script Best Practices.

Advanced Employee Permissions and SuiteFlow

In NetSuite, account administrators have access to all the information on all record types, including the employee record. This can create issues in the following situations:

- When a user is assigned a role that has permission to create workflows.
- When a user sets a workflow to run as administrator.

A user could write or deploy a workflow that gains access to employee information that they would normally not have access to. This could potentially be used to compromise employee information.

When Advanced Employee Permissions is enabled, carefully track which roles have permission to create or alter workflows. In addition, track which workflows execute as administrator, and what they do to make sure employee information is not unintentionally leaked.

It is not possible to know what fields or sublists are present on any employee record when Advanced Employee Permissions is enabled. This means that workflows cannot safely perform operations, such as setting a default value on a field. To avoid this, utilize an After Submit workflow as administrator, which gives access to the complete set of fields and sublists on the employee record.

If you have any workflows that add buttons to the employee record, make sure that they appear only when appropriate. Configure scripts so that the action being added respects the restrictions on the employee record.

For more information about workflows, see the help topic Working with Workflows.

Advanced Employee Permissions and SuiteAnalytics Connect

SuiteAnalytics Connect access to the employee record, meaning access through ODBC, JDBC, or ADO.NET drivers, is supported only with the Lists > Employees permission. SuiteAnalytics Connect access is not supported for roles with other employee permissions.

Advanced Employee Permissions and CSV Import

CSV import is supported only with the Lists > Employees permission.

Advanced Employee Permissions and SOAP Web Services

Access to the employee record through SOAP web services respects the permissions that are assigned to a role. However, be aware of the following:

- A value for a field is set on the employee record in a SOAP web services program. The current role does not have access to that field. The program completes without errors, but the field is not set or updated.
- Fields and sublists to which the current role does not have access are not returned through search or filtering.

Advanced Employee Permissions and Customizations

The following section outlines how customizations change when Advanced Employee Permissions is enabled.

Custom Roles

Custom roles created in your NetSuite account are not automatically updated with the employee permissions introduced by Advanced Employee Permissions. You must manually update custom roles to include any of the required employee permissions. For more information, see the help topic Setting Employee Access for Advanced Employee Permissions.

Roles Using the SuiteScript Permission

Roles that have the Setup > SuiteScript permission can configure scripts to run as administrator, which bypasses the Advanced Employee Permissions feature. Before creating custom roles with this permission, make sure that the role should have access to the information that is being exposed.

SuiteBuilder

By default, any customization created with NetSuite SuiteBuilder that are included with the standard Lists > Employees permission are preserved. If you customize the permission, the customizations created with SuiteBuilder are not preserved. If required, you must manually add customizations to the custom Lists > Employees permission. For more information, see Custom Advanced Employee Permissions.

Advanced Employee Permissions and Standard NetSuite Roles

The following table highlights which Advanced Employee Permissions are automatically assigned to standard NetSuite roles. It also provides the default access levels and restrictions for each. The Employee Administration and Employee Access Tab permissions are not automatically assigned to any standard roles. If required, you can manually add these permissions to a role.

Warning: When you assign permissions, be aware that:

- If you change the access level of the Employee Self permission to Edit, employees can make changes to the fields exposed with this permission. This includes their compensation information. You should use the default access level View, however, if required, you can create a custom permission. For more information, see Custom Advanced Employee Permissions.
- If you change the access level of the following permissions to Edit, employees can create employees in NetSuite:
  - Employee Public
  - Employee Confidential
  - Employee Compensation
  - Employee Record Full
  - Employee Administration

Important: The standard NetSuite Lists > Employees permission takes precedence over any of the employee permissions in Advanced Employee Permissions. This change is a step in separating the legacy permission model from the Advanced Employee Permissions feature. The Lists > Employees permission gives full-record access to employee records. You should review the standard and custom roles in your account that include the Lists > Employees permission. Ensure that all users with these roles have full access to employee records. Users who should not have full access to employee records should be assigned a role that does not include the Lists > Employees permission. If you have the Administrator role, you can create alternate custom roles for these users. For more information, see Setting Employee Access for Advanced Employee Permissions, Creating Custom Advanced Employee Permissions, and Custom Restrictions for Advanced Employee Permissions.

Standard Role	Employee Permissions	Level of Access	Restriction
A/P Clerk	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
A/R Clerk	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Accountant	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Edit	–
Accountant (Reviewer)	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	View	–
Bookkeeper	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Edit	–

Standard Role	Employee Permissions	Level of Access	Restriction
Buyer	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
CEO	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Full	–
CEO (hands off)	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	View	–
CFO	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Full	–
Chief People Officer (CPO)	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Full	–
Employee Center	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Self	**View**	**Own Only**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	Edit	–
Engineer	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Engineering Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
Human Resources Generalist	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Full	–
Intranet Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–

Standard Role	Employee Permissions	Level of Access	Restriction
Issue Administrator	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Marketing Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
Payroll Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	Full	–
	Employees	Full	–
Payroll Setup	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Full	–
PM Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
Product Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Support Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
QA Engineer	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
QA Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
Resource Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–

Standard Role	Employee Permissions	Level of Access	Restriction
	Employees	View	–
Retail Clerk	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Retail Clerk (Web Services Only)	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	View	–
Sales Administrator	**Employee Public**	**View**	–
	Employee Record	Full	–
	Employees	Full	–
Sales Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
Sales Person	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Sales Vice President	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	View	–
Store Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–
System Administrator	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Record	Full	–
	Employees	Full	–
Warehouse Manager	**Employee Public**	**View**	**Active and Non-Terminated**
	Employee Confidential	**View**	**Subordinates**
	Employee Compensation	**View**	**Subordinates**
	Employee Record	View	–

Employee Self Permission Overview

The Employee Self permission is intended for all employees. Roles that have this permission can view basic personal information on their employee record. Basic personal information includes things such as home address, and passport information. When you enable the Advanced Employee Permissions feature, NetSuite automatically assigns this permission to the Employee Center role. By default, the access level for this permission is set to View, and the restriction is set to Own Only, but you can make changes. For more information, see Setting Employee Access for Advanced Employee Permissions.

Note: Users are not able to view or edit future or past-dated changes to their employee information if they have an assigned role with this permission.

Employee Self Permission Fields

This section outlines the default employee record fields that are exposed with the Employee Self permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Self Permission Fields
Primary Information ▪ Employee ID ▪ Mr/Ms ▪ Name ▪ Initials ▪ Job ▪ Supervisor ▪ Image
Email | Phone | Address ▪ Email ▪ Phone ▪ Office Phone ▪ Mobile Phone ▪ Home Phone ▪ Fax ▪ Address
Classification ▪ Subsidiary ▪ Department ▪ Class ▪ Location

Employee Self Permission Sublists

This section outlines the default employee record sublists, and the fields associated with them that are exposed with the Employee Self Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Self Permission Sublists
Address ▪ Default Shipping

Employee Self Permission Sublists

- Home
- Label
- Address
- Edit

Human Resources

- Social Security
- Birth Date
- **Job Information**
  - Job Description
- **Education**
  - Level of Education
  - Degree
  - Date Conferred
- **Personal**
  - Marital Status
  - Ethnicity
  - Gender
- **Subordinates**

  Subordinates is a subtab on the Human Resources subtab.
  - Image
  - Name
  - Job Title
  - Location
  - Department
  - Subsidiary
  - Contact Info

Time-Off

- **Available Now**
  - Type
  - Available this Year
  - Used this Year
  - Schedules this Year
  - Available Now
- **Balances**
  - Type
  - Carried Over
  - Accrued
  - Used
  - Expired Carryover
  - Balance

Compensation Tracking

Employee Self Permission Sublists
■ Compensation Currency ■ Base Wage Type ■ Base Wage ■ Bonus Target ■ Target Type ■ Target Frequency ■ Target Comments ■ Bonus Type* ■ Percentage* ■ Amount* ■ Award Date* ■ Comments*
*These fields are a part of the bonus record. The Employee Self Permission allows access to these fields, but Advanced Employee Permissions cannot further restrict access to these fields.

Employee Public Permission Overview

The Employee Public permission is intended for all employees. Roles that have this permission can view basic employee information. Basic information includes non-sensitive information, such as job title and reporting relationships. When you enable the Advanced Employee Permissions feature, NetSuite automatically assigns this permission to a set of standard roles. By default, the access level for this permission is set to View. The restriction is set to Active and Non-Terminated, but you can makes changes. For more information, see Setting Employee Access for Advanced Employee Permissions.

Employee Public Permission Fields

This section outlines the default employee record fields that are exposed with the Employee Public Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Public Permission Fields
Primary Information ■ Employee ID ■ Name ■ Initials ■ Supervisor ■ Image
Email | Phone | Address ■ Email ■ Phone ■ Office Phone ■ Mobile Phone ■ Fax
Classification

Employee Public Permission Fields
■ Subsidiary
■ Department
■ Class
■ Location

Employee Public Permission Sublist

This section outlines the default employee record sublist, and the fields associated with it that are exposed with the Employee Public Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions

Employee Public Permission Sublist
Subordinates
■ Image
■ Name
■ Job Title
■ Location
■ Department
■ Subsidiary
■ Contact Info

Employee Confidential Permission Overview

The Employee Confidential permission is intended for manager roles. In addition to the employee public fields and sublists, roles with this permission can also access confidential employee information. Confidential information includes job and education information. This permission is automatically added to a set of standard roles when the Advanced Employee Permissions feature is enabled. For more information, see Advanced Employee Permissions and Standard NetSuite Roles. By default, the access level for this permission it set to View, and the restriction is set to Subordinates, but you can make changes. For more information, see Setting Employee Access for Advanced Employee Permissions.

Employee Confidential Permission Fields

This section outlines the default employee record fields that are exposed with the Employee Confidential Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Confidential Permission Fields
Primary Information
■ Employee ID
■ Name
■ Initials
■ Supervisor
■ Job
■ Image

Employee Confidential Permission Fields

Email | Phone | Address

- Email
- Phone
- Office Phone
- Mobile Phone
- Fax

Classification

- Subsidiary
- Department
- Class
- Location
- Billing Class

Employee Confidential Permission Sublists

This section outlines the default employee record sublists, and the fields associated with them that are exposed with the Employee Confidential Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Confidential Permission Sublists

Human Resources

- **Job Information**
  - Type
  - Employee Status
  - Job Description
  - Sales Rep
  - Support Rep
  - Project Resource
  - Project Manager
  - Default Project Resource Role
  - Work Calendar
  - Labor Cost
  - Hourly Rate
  - Hire Date
  - Last Review Date
  - Next Review Date
- **Expenses and Purchasing**
  - Expense Limit
  - Expense Approver
  - Expense Approval Limit
  - Purchase Limit
  - Purchase Approver

Employee Confidential Permission Sublists
□ Purchase Approval Limit □ Account ■ **Subordinates** □ Image □ Name □ Job Title □ Location □ Department □ Subsidiary □ Contact Info ■ **Education** □ Level of Education □ Degree □ Date Conferred
Time-Off ■ Time-Off Plan ■ Start Date for Time-Off Calculations ■ Available Now: □ Type □ Available this Year (HRS) □ Used this Year (HRS) □ Scheduled this Year (HRS) □ Available Now (HRS) ■ Balances: □ Type □ Carried Over (HRS) □ Accrued (HRS) □ Used (HRS) □ Expired Carryover (HRS) □ Balance (HRS)
Time Tracking ■ Time Approver
Commission ■ Eligible for Commission ■ Pay Commissions Using

Employee Compensation Permission Overview

The Employee Compensation permission is intended for managers. Roles that have this permission can access compensation information. This permission is automatically added to a set of standard roles when the Advanced Employee Permissions feature is enabled. For more information, see Advanced Employee

Permissions and Standard NetSuite Roles. By default, the access level for this permission it set to View, and the restriction is set to Subordinates, but you can make changes. For more information, see Setting Employee Access for Advanced Employee Permissions.

Employee Compensation Permission Sublists

This section outlines the default employee record sublists, and the fields associated with them that are exposed with the Employee Compensation Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Compensation Permission Sublists
Compensation Tracking - Base Wage - Base Wage Type - Bonus Target - Target Comments - Target Frequency - Target Type - Compensation Currency - Bonus Type* - Percentage* - Amount* - Award Date* - Comments* *These fields are a part of the bonus record. The Employee Compensation Permission allows access to these fields, but Advanced Employee Permissions cannot further restrict access to these fields.
Payroll - Compensation Type

The following fields are a part of the Compensation Tracking feature:

- Base Wage
- Base Wage Type
- Bonus Target
- Target Comments
- Target Frequency
- Target Type
- Compensation Currency
- Compensation Type

The Compensation Type field is a part of SuitePeople U.S. Payroll. For more information, see the help topics Recording Base Pay Compensation for an Employee and Including an Employee in Payroll.

Employee Access Tab Permission Overview

The Employee Access Tab permission is intended for IT administrators. Roles with this permission give users access to NetSuite and assign roles to users who fall into the restriction policy defined on the Role page. For example, when restricted by location, a role with this permission can give access and assign roles to employees in their location only.

Note: When the Advanced Employee Permissions feature is enabled, the Employee Access Tab permission is not automatically assigned to any standard roles.

Employee Access Tab Permission Fields

This section outlines the default employee record fields that are exposed with the Employee Access Tab Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Access Tab Permission Fields
Primary Information - Employee ID - Name
Email | Phone | Address - Email

Employee Access Tab Permission Sublist

This section outlines the default employee record sublist, and the fields associated with this permission that are exposed with the Employee Access Tab Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Access Tab Permission Sublist
Access - Give Access - IP Address Restriction - Inherit IP Rules from Company Roles: - Role Global Permissions: - Permission - Level History: - Date/Time - User - Change

Employee Administration Permission Overview

The Employee Administration permission is intended for Human Resources Generalists and Human Resources Administrators. Users with this permission have access to the Employee Public fields and sublists. They also have access to a limited set of fields and sublists, based on the restrictions defined on the Role page.

Note: When the Advanced Employee Permissions feature is enabled, the Employee Administration permission is not automatically assigned to any standard roles.

Employee Administration Permission Fields

This section outlines the default employee record fields that are exposed with the Employee Administration Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Administration Permission Fields
Primary Information ▪ Employee ID ▪ Initials ▪ Supervisor ▪ Mr/Ms ▪ Job ▪ Image ▪ Name
Email | Phone | Address ▪ Email ▪ Mobile Phone ▪ Address ▪ Phone ▪ Home Phone ▪ Office Phone ▪ Fax
Classification ▪ Subsidiary ▪ Class ▪ Location ▪ Department

Employee Administration Permission Sublists

This section outlines the default employee record sublists, and the fields associated with them that are exposed with the Employee Administration Permission. If required, you can customize this permission. For more information, see Custom Advanced Employee Permissions.

Employee Administration Permission Sublists
Address ▪ Default Shipping ▪ Home

Employee Administration Permission Sublists

- Label
- Address
- Edit

Human Resources

- Birth Date
- Job Information:
  - Type
  - Termination/Release Date
  - Employee Status
  - Job Description
  - Work Calendar
  - Hire Date
  - Last Review Date
  - Next Review Date
  - Expense and Purchasing:
    - Expense Limit
    - Expense Approver
    - Expense Approval Limit
    - Purchase Limit
    - Purchase Approver
    - Purchase Approval Limit
    - Account
    - Default Account for Corporate Card Expenses
  - Subordinates:
    - Image
    - Name
    - Job Title
    - Location
    - Department
    - Subsidiary
    - Contact Info
  - Education:
    - Level of Education
    - Degree
    - Date Conferred
  - Personal:
    - Marital Status
    - Ethnicity
    - Gender

Employee Record Full Permission Overview

The Employee Record Full permission is intended for Human Resources Business Partners, Chief People Officers (CPOs), and Human Resources Directors. Users with this permission have access to all information about the employee record, except for fields and sublists exposed by the Employee Access Tab permission. Roles with this permission can give users access to NetSuite. They can also assign roles to users who fall into the restriction policy defined on the Role page. For more information, see Employee Access Tab Permission Overview.

Advanced Employee Permissions Use Cases

The following section provides five use cases illustrating how to use Advanced Employee Permissions. These are examples only. They are meant to illustrate how using a combination of permissions exposes only the information that a particular type of employee requires access to.

For a complete list of the fields and sublists exposed with each advanced employee permission, see the following help topics:

- Employee Self Permission Overview
- Employee Public Permission Overview
- Employee Confidential Permission Overview
- Employee Compensation Permission Overview
- Employee Access Tab Permission Overview
- Employee Administration Permission Overview
- Employee Record Full Permission Overview

Note: These examples use the default Advanced Employee Permissions and the default restrictions, but you can customize both. For more information, see Custom Advanced Employee Permissions and Custom Restrictions for Advanced Employee Permissions.

Use Case 1: Employee Access for All Employees

The following table provides the permissions, access levels, and restrictions required to give employees access to basic employee information about other employees. It also provides relevant information about themselves.

Important: The Lists > Employee Record and Lists > Perform Search permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to access employee menus in NetSuite and to be able to perform searches. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

Permission	Access Level	Restriction	Gives Employees Access To
Lists > Employee Record	Edit	–	Ability to see NetSuite menus related to employees. For example, List > Employees. This permission does not give access to the employee record.

Permission	Access Level	Restriction	Gives Employees Access To
Lists > Perform Search	Full	–	Search for employees.
Employee Public	View	Active and Non-Terminated	View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.
Employee Self	View	Own Only	View relevant information about themselves on their employee record, such as job description and compensation.

Use Case 2: Employee Access for Managers

The following table gives an example of how to use Advanced Employee Permissions to give the required access to employee information for a manager.

⚠ **Important:** The Lists > Employee Record and Lists > Perform Search permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to access employee menus in NetSuite and to be able to perform searches. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

Permission	Access Level	Restriction	Gives Managers Access To
Lists > Employee Record	View	–	Ability to see NetSuite menus related to employees. For example, List > Employees. This permission does not give access to the employee record.
Lists > Perform Search	Full	–	Search for employees.
Employee Confidential	View	Subordinates	View and search confidential employee information, such as hire date and expense limit, for direct reports and below.
Employee Compensation	View	Subordinates	View and search compensation information for direct reports and below.
Employee Public	View	Active and Non-Terminated	View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.
Employee Self	View	Own Only	View relevant information about themselves on their employee record, such as job description and address.

Use Case 3: Employee Access for Human Resources Generalists

The following table gives an example of how to use Advanced Employee Permissions to give required access to employee information for a Human Resources Generalist.

Important: The Lists > Employee Record and Lists > Perform Search permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to access employee menus in NetSuite and to be able to perform searches. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

Permission	Access Level	Restriction	Gives Human Resources Generalists Access To
Lists > Employee Record	Full	–	Ability to see NetSuite menus related to employees. For example, List > Employees. This permission does not give access to the employee record.
Lists > Perform Search	Full	–	Search for employees.
Employee Administration	Full	Inherit from Role	View, create, edit, and search for personal information, such as home phone, for employees who match the restrictions defined on the Role page. If no restrictions are defined, this information is available for all employees.
Employee Confidential	View	Subordinates	View and search confidential employee information, such as hire date and expense limit, for direct reports and below.
Employee Compensation	View	Subordinates	View compensation information for direct reports and below.
Employee Public	View	Active and Non-Terminated	View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.

Use Case 4: Employee Access for Human Resources Directors

The following table gives an example of how to use Advanced Employee Permissions to give required access to employee information for a Human Resources Director.

Important: The Lists > Employee Record and Lists > Perform Search permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to access employee menus in NetSuite and to be able to perform searches. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

Permission	Access Level	Restriction	Gives Human Resources Directors and Above Access To
Lists > Employee Record*	Full	–	Ability to see NetSuite menus related to employees. For example, List > Employees. This permission does not give access to the employee record.
Lists > Perform Search*	Full	–	Search for employees.

Permission	Access Level	Restriction	Gives Human Resources Directors and Above Access To
Employee Record Full	Full	Inherit from Role	View, create, edit, and search all employee record information for employees who match the restrictions defined on the Role page. If no restrictions are defined, this information is available for all employees.
Employee Public	View	Active and Non-Terminated	View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.

Use Case 5: Employee Access for IT Administrators

The following table gives an example of how to use Advanced Employee Permissions to give the required access to employee information for an IT administrator.

⚠ **Important:** The Lists > Employee Record and Lists > Perform Search permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to access employee menus in NetSuite and to be able to perform searches. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

Permission	Access Level	Restriction	Gives IT Administrators Access To
Lists > Employee Record	View	–	Ability to see NetSuite menus related to employees. For example, List > Employees. This permission does not give access to the employee record.
Lists > Perform Search	Full	–	Search for employees.
Employee Access Tab	Full	Inherit from Role	Give access and assign roles to employees who match the restrictions defined on the Role page.
Employee Public	View	Active and Non-Terminated	View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.

Setting Employee Access for Advanced Employee Permissions

You can specify additional levels of restrictions and access to employee information on the **Employee Access** subtab of the Role page.

To set employee access:

1. Go to Setup > Users/Roles > Manage Roles.
2. From the Manage Roles list page, you can either create a custom or new role that you want to customize employee access for:
   - To create a custom role, click **Customize** or **Edit** beside the role. All of the permissions associated with the parent role are inherited. You can make changes as necessary.

> ⚠ **Important:** The Lists > Employees permission takes precedence over any of the employee permissions that are part of the Advanced Employee Permissions feature. This change is a step in separating the legacy permission model from the Advanced Employee Permissions feature. The Lists > Employees permission gives full-record access to employee records. When customizing a role, check if this permission is present. If this role should not have full access to employee records, remove the permission.

- To create a new role that does not contain a list of associated permissions, click **New Role**.

> ⚠ **Important:** When creating a new role using Advanced Employee Permissions you must add the Lists > Employee Record permission to the role. This permission is required to see NetSuite menus related to employees. For example, List > Employees.

3. Click the **Employee Access** subtab.
4. From the **Permission** list, select the employee access you want to add to the role. Select from the following:
   - **Employee Administration** – This permission is intended for Human Resources Generalists and Human Resources Administrators. Users assigned to a role with this permission have access to HR-related fields on the employee record. For more information, see Employee Administration Permission Overview.
   - **Employee Compensation** – This permission is intended for managers. Users assigned to a role with this permission have access to compensation information on the employee record. For more information, see Employee Compensation Permission Overview.
   - **Employee Confidential** – This permission is intended for managers. Users assigned to a role with this permission have access to public and confidential information on the employee record. For more information, see Employee Confidential Permission Overview.
   - **Employee Public** – This permission is intended for employees. Users assigned to a role with this permission have access to basic employee information on the employee record. For more information, see Employee Public Permission Overview.
   - **Employee Record Full** – This permission is intended for Human Resources Business Partners, Chief People Officers (CPOs), and Human Resources Directors. Users assigned to a role with this permission have access to all information on the employee record. For more information, see Employee Record Full Permission Overview.
   - **Employee Self** – This permission is intended for employees. Users assigned to a role with this permission have access to basic personal information on the employee record. For more information, see Employee Self Permission Overview.
   - **Employee Access Tab** – This permission is intended for IT Administrators. Users assigned to a role with this permission can give access and assign roles to employees. For more information, see Employee Access Tab Permission Overview.

> ⓘ **Note:** When you select a permission, the default access level and restriction are applied, but you can change these.

5. If required, change the access level for the selected restriction from the **Level** list. For more information, see the help topic Access Levels for Permissions.

Note: When two employee permissions, one at level View and another at level Edit, are included with a role, note the following. Users assigned to the role see a combination of the fields and sublists they are permitted to view on the employee record. In edit mode, only the fields and sublists that the user can edit are visible on the employee record.

Warning: When you assign permissions, be aware that:

- If you change the access level of the Employee Self permission to Edit, employees can make changes to the fields exposed with this permission. This includes their compensation information. You should use the default access level View, however, if required, you can create a custom permission. For more information, see Custom Advanced Employee Permissions.
- If you change the access level of the following permissions to Edit, users can create employees in NetSuite:
  - Employee Public
  - Employee Confidential
  - Employee Compensation
  - Employee Administration
- The Employee Record Full permission gives roles access to all information on the employee record. This permission is intended for Human Resources Business Partners, Chief People Officers (CPO), and Human Resources Directors. To restrict these roles to see only employee administration information, remove the Employee Record Full permission, and add the Employee Administration permission. For more information, see Employee Administration Permission Overview.

6. If required, from the **Restrictions** list, select a new restriction level. Select from the following:
   - **Active and Non-Terminated –** Select this when you want to restrict the permission to active and non-terminated employees. For example, you could add this restriction to the Employee Public permission. Then, users assigned to this role would have access to basic employee information for all active and non-terminated employees only.
   - **Inherit from Role –** Select this when you want the permission to inherit the restrictions set on the Role page. For more information about setting restrictions on the Role page, see the help topic Customizing or Creating NetSuite Roles.
   - **Own Only –** Select this when you want to restrict the permission to the employee’s own record only. Users assigned to this role have access to the fields and sublists exposed with the permission for only themselves. For example, you could add this restriction to the Employee Self permission. Then, users assigned to this role would have access only to basic personal employee information for themselves.
   - **Subordinates –** Select this when you want to restrict the permission by subordinates. For example, you could add this restriction to the Employee Confidential permission. Then, users assigned to this role would have access to public and confidential employee information only for their subordinates.

> **Note:** You can also create custom restrictions. For more information, see Custom Restrictions for Advanced Employee Permissions.

7. Click **Add**.
8. Repeat steps 4 to 7 for each permission you want to assign to the role.
9. To finish, click **Save**.

> **Note:** If you change access to a role that a user currently logged in to NetSuite is using, note the following. That user must log out and log back in to see the newly-assigned access.

Custom Advanced Employee Permissions

This section describes how to create custom Advanced Employee Permissions.

For more information, see the following topics:

- Before Creating Custom Advanced Employee Permissions
- Prerequisites for Creating Custom Advanced Employee Permissions
- Creating Custom Advanced Employee Permissions
- Adding Standard Fields to Custom Advanced Employee Permissions
- Adding Standard Sublists to Custom Advanced Employee Permissions

Before Creating Custom Advanced Employee Permissions

Both inline editing and inactivating employees from the Employees List page are disabled for users assigned to a role that has a custom employee permission.

Before deploying client or server side scripts that gain access to employee information, make sure:

- The employee field or sublist is available to the role.
- The role has the correct employee permission to see the employee field or sublist for the types of employees being viewed or edited.
- Some scripts may fail, including third-party scripts. Scripts fail when they attempt to access parts of the employee record they are not permitted to access with the assigned role and permissions.

For more information, see Before Enabling the Advanced Employee Permissions Feature.

Prerequisites for Creating Custom Advanced Employee Permissions

To create custom Advanced Employee Permissions, you need the Setup > Manage Custom Permissions permission at access Level Full. The standard role that comes with this permission is the Administrator role. You can also create custom roles that include this permission. For more information, see the help topic Customizing or Creating NetSuite Roles.

Creating Custom Advanced Employee Permissions

You have two choices when creating custom Advanced Employee Permissions:

- You can create a new permission using a custom set of fields and sublists from the employee record.
- You can customize a standard employee permission to include a subset of the fields and sublists that are exposed. You can also customize it to include additional fields and sublists.

Standard employee permissions cannot be modified. Use these permissions as templates to create your own custom employee permissions.

⚠ **Important:** Some fields on the employee record have dependencies on other fields. Do not add or remove these fields individually. For example, you customize the Employee Access Tab permission. But you have only a partial set of the standard fields that come with this permission. Therefore, the employee record cannot load. The employee record only loads when it has either all or none of the access fields.

To create custom Advanced Employee Permissions:

1. Go to Setup > Users/Roles > Manage Permissions.
2. From the Manage Permissions page, you can either create a custom or new employee permission.
   - To create a custom employee permission, click **Customize** beside the employee permission you want to customize. All of the standard fields and sublists associated with the parent permission are inherited. You can make changes as necessary.
   - To create a new employee permission that does not start with a list of associated fields and sublists, click **New Permission** page.
3. If required, you can add standard and custom fields to the permission. For more information, see the following help topics:
   - Adding Standard Fields to Custom Advanced Employee Permissions
   - Adding Standard Sublists to Custom Advanced Employee Permissions
   - Creating Custom Fields for Advanced Employee Permissions
   - Adding Custom Fields to Advanced Employee Permission
   - Creating Custom Sublists for Advanced Employee Permissions
   - Adding Custom Sublists to Advanced Employee Permission
4. To finish, click **Save**.

✓ **Tip:** To remove the permission, from the **Actions** list, select **Delete**. When the permission is assigned to a role you need to remove it from the role before you can delete it.

Adding Standard Fields to Custom Advanced Employee Permissions

When you create a custom Advanced Employee Permissions you can include all or a set of standard employee record fields to the permission.

To add standard fields to custom Advanced Employee Permissions:

1. Go to Setup > Users/Roles > Manage Permissions.
2. From the Manage Permissions page, click **Customize** beside the employee permission you want to customize. All of the standard fields and sublists associated with the parent permission are inherited. You can make changes as necessary.

3. To add a standard field, select the **Fields** subtab, and then the **Standard Fields** subtab.
4. Click a line in the list.
5. From the **Record Type** list, select **Employee.**
6. From the **Field** list, select the field to add to the permission.
7. Click **Add.**
8. Repeat steps 4 to 7 for each field you want to include.
9. To finish, click **Save**.

Adding Standard Sublists to Custom Advanced Employee Permissions

When you create a custom Advanced Employee Permissions you can include all or a set of standard employee record sublists to the permission.

> ⚠ **Important:** When you add a sublist to a custom permission that is associated with another feature in NetSuite, note the following. You must also add the specific permission for the feature to the role. If the role does not have the required permission for the feature, users do not see any information in the sublist. For example, the Accrued Time and Available Now sublists are associated with the Time-Off Management feature. If you add these sublists to a custom Advanced Employee Permission, ensure that the Time-Off Administration permission is included. For more information, see the help topics SuitePeople Permission Requirements and Permissions Documentation.

To add standard sublists to custom Advanced Employee Permissions:

1. Go to Setup > Users/Roles > Manage Permissions.
2. From the Manage Permissions page, click **Customize** beside the employee permission you want to customize. All of the standard fields and sublists associated with the parent permission are inherited. You can make changes as necessary.
3. To add a standard sublist, select the **Sublists** subtab, and then the **Standard Sublists** subtab.
4. Click a line in the list.
5. From the **Record Type** list, select **Employee.**
6. From the **Sublist** list, select the sublist to add to the permission.
7. Click **Add.**
8. Repeat steps 4 to 7 for each sublist you want to include.
9. To finish, click **Save**.

Creating Custom Fields for Advanced Employee Permissions

You can create custom employee fields, which you can then add to custom Advanced Employee Permissions.

Important: When an Advanced Employee Permission is assigned to a role, the permission access level is set on the Role page. Not on the custom entity record. For example, an Advanced Employee Permission is assigned to a role at access level View. Any custom fields that are added to the permission respect that access level.

To create custom fields for Advanced Employee Permissions:

1. Go to Customization > Lists, Records, & Fields > Entity Fields > New.
2. In the **Label** field, enter a name or description for the custom field. You can enter up to 200 characters for the label.
3. On the **Applies To** subtab, check the **Employee** box.
4. Click the **Employee Access** subtab.
5. Click a line in the list.
6. From the **Permission** list, select the custom permission with which you want to associate this custom field. This list displays each of the custom Advanced Employee Permissions that have been created.
7. Click **Add**. Alternatively, click **+Insert**, select the permission, and click **Add**.

   ✓ **Tip:** To remove a permission, select it from the list, and click **Remove**.

8. Repeat steps 5 to 7 for each custom permission you want to associate this custom field with.
9. To finish, click **Save**.

The custom field is automatically added to the custom permission. To see a list of the custom fields associated with a permission, click the **Fields** subtab. Then, click the **Custom Fields** subtab on the Permission page.

Note: The Show In List box on the custom entity field record is not supported with Advanced Employee Permissions. This means that custom fields are not shown on the Employees List page when this box is checked. To display custom fields with Advanced Employee Permissions, you need to create a custom view that contains the custom fields. To do this, click Edit from the Employees List page and manually add the custom fields.

Adding Custom Fields to Advanced Employee Permission

Use the following procedure to add custom fields to the Advanced Employee Permission.

To add custom fields to the Advanced Employee Permissions:

1. Go to Setup > Users/Roles > Manage Permissions.
2. Click **Customize** or **Edit** beside the permission to which you want to add a custom sublist to.
3. Select the **Fields** subtab.
4. Select the **Custom Fields** subtab.
5. Click a line in the list.
6. From the **Record Type** list, select **Employee**.
7. From the **Field** list, select the custom field to add to the permission.
8. Click **Add**. Alternatively, click **+Insert**, select the record type and sublist, and click **Add**.

9. Repeat steps 5 to 8 for each custom field you want to add to the permission.
10. To finish, click **Save**.

Creating Custom Sublists for Advanced Employee Permissions

You can create a custom employee sublist, which you can then add to Advanced Employee Permissions.

> ⚠ **Important:** When an Advanced Employee Permission is assigned to a role, the permission access level is set on the Role page. Not on the custom entity record. For example, an Advanced Employee Permission is assigned to a role at access level View. Any custom fields that are added to the permission respect that access level.

To create custom sublists for Advanced Employee Permissions:

1. Go to Customization > Forms > Sublists > New.
2. From the **Type** list, select **Entity**.
3. Check the **Employee** box.
4. From the **Search** list, select the saved search that returns the results you want to appear on the record. If the saved search does not appear in the list, check the saved search settings. The first item listed on the **Available Filters** subtab must be a List/Record type. Otherwise, the saved search is not available to assign as a sublist. For more information, see the help topic Saved Searches for Custom Sublists.
5. In the **Label** field, enter a label for this sublist.
6. From the **Tab** list, select the subtab under which you want the sublist to appear.
7. Repeat these steps for each custom sublist you want to create.
8. To finish, click **Save**.

The custom sublist you created automatically appears in the **Custom Sublists** subtab on the Permission page. For more information, see Adding Custom Sublists to Advanced Employee Permission.

Adding Custom Sublists to Advanced Employee Permission

Use the following procedure to add custom sublists to Advanced Employee Permission.

To add custom sublists to Advanced Employee Permissions:

1. Go to Setup > Users/Roles > Manage Permissions.
2. Click **Customize** or **Edit** beside the permission to which you want to add a custom sublist to.
3. Select the **Sublists** subtab.
4. Select the **Custom Sublists** subtab.
5. Click a line in the list.
6. From the **Record Type** list, select **Employee**.
7. From the **Sublist** list, select the custom sublist to add to the permission.
8. Click **Add**. Alternatively, click **+Insert**, select the record type and sublist, and click **Add**.

9. Repeat steps 5 to 8 for each custom sublist you want to add to the permission.
10. To finish, click **Save**.

Custom Restrictions for Advanced Employee Permissions

By default, when Advanced Employee Permissions is enabled there are four pre-defined restrictions. This includes, Own Only, Active and Non-Terminated, Subordinates, and Inherit from Role. This section describes how to create custom restrictions for Advanced Employee Permissions and how to assign custom restrictions to a role.

For more information, see the following topics:

- Prerequisites for Creating Custom Restrictions for Advanced Employee Permissions
- Creating Custom Restrictions for Advanced Employee Permissions
- Assigning Custom Restrictions to Advanced Employee Permissions

Prerequisites for Creating Custom Restrictions for Advanced Employee Permissions

To create custom restrictions for Advanced Employee Permissions, the Setup > Manage Custom Restrictions Permission is required at access Level Full. The standard role that comes with this permission is the Administrator role. You can also create custom roles that include this permission. For more information, see the help topic Customizing or Creating NetSuite Roles.

Creating Custom Restrictions for Advanced Employee Permissions

You can create custom restrictions to restrict the instances that a role has access to the employee record by class, department, location, and subsidiary. For example, you may have a Human Resources department that is physically located in one location, but who support staff located in a different location. You can create custom Advanced Employee Permissions' restrictions to give this department access to sensitive employee data for the staff they support. You can limit them to less sensitive information for the employees in their location that they do not support.

> **Note:** You cannot make changes to the standard restrictions that come with the Advanced Employee Permissions feature. This includes: Active and Non-Terminated, Inherit from Role, Own Only, and Subordinates.

To create custom restrictions for Advanced Employee Permissions:

1. Go to Setup > Users/Roles > Manage Restrictions > New.
2. In the **Name** field, enter a unique name for the restriction. The name entered here appears on the Role page, under the **Employee Access** subtab, in the **Restrictions** list.
3. If required, enter a description for the restriction.
4. In the **Class** list, select the classes that you want to include with the restriction. The classes selected from this list determine the classes this restriction is limited to. This means that roles that have

a permission with this restriction can only access employee information for employees in the selected classes. Hold down the Ctrl key to select multiple classes or to deselect a class from the list.

5. From the **Department** list, select the departments that you want to include with the restriction. The departments selected from this list determine the departments this restriction is limited to. This means that roles that have a permission with this restriction can only access employee information in the selected departments. Hold down the Ctrl key to select the multiple departments or to deselect a location from the list.
6. From the **Locations** list, select the locations that you want to include with the restriction. The locations selected from this list determine the locations this restriction is limited to. This means that roles that have a permission with this restriction can only access employee information for employees in the selected locations. Hold down the Ctrl key to select multiple locations or to deselect a location from the list.
7. From the **Subsidiaries** list, select the subsidiaries that you want to include with the restriction. The subsidiaries selected from this list determine the subsidiaries this restriction is limited to. This means that roles that have a permission with this restriction can only access employee information for employees in the selected subsidiaries. Hold down the Ctrl key to select multiple subsidiaries or to deselect a subsidiary from the list.
8. Click **Save**.

✓ **Tip:** To remove the restriction, from the **Actions** list, select **Delete**. When the restriction is assigned to a role you need to remove it from the role before you can delete it.

Assigning Custom Restrictions to Advanced Employee Permissions

You can assign a custom restriction to Advanced Employee Permissions on the Role page.

To assign a custom restriction:

1. Go to Setup > Users/Roles > Manage Roles.
2. From the list, click **Customize** or **Edit** beside the role to which you want to assign the custom restriction to.
3. Select the **Employee Access** subtab.
4. From the **Permission** list, select the permission you want to add to the role. Select from the following:
   - **Employee Administration** – This permission is intended for Human Resources Generalists and Human Resources Administrators. Users assigned to a role with this permission have access to HR-related fields on the employee record. For more information, see Employee Administration Permission Overview.
   - **Employee Compensation** – This permission is intended for managers. Users assigned to a role with this permission have access to compensation information on the employee record. For more information, see Employee Compensation Permission Overview.
   - **Employee Confidential** – This permission is intended for managers. Users assigned to a role with this permission have access to public and confidential information on the employee record. For more information, see Employee Confidential Permission Overview.
   - **Employee Public** – This permission is intended for employees. Users assigned to a role with this permission have access to basic employee information on the employee record. For more information, see Employee Public Permission Overview.

- **Employee Record Full** – This permission is intended for Human Resources Business Partners, Chief People Officers (CPOs), and Human Resources Directors. Users assigned to a role with this permission have access to all information on the employee record. For more information, see Employee Record Full Permission Overview.
- **Employee Self** – This permission is intended for employees. Users assigned to a role with this permission have access to basic personal information on the employee record. For more information, see Employee Self Permission Overview.
- **Employee Access Tab** – This permission is intended for IT Administrators. Users assigned to a role with this permission can give access and assign roles to employees. For more information, see Employee Access Tab Permission Overview.

5. If required, change the access level for the selected restriction from the **Level** list. For more information, see Setting Employee Access for Advanced Employee Permissions.
6. From the **Restrictions** list, select the custom restriction to apply to the permission.
7. Click **Add**.
8. Repeat steps 4 to 7 for each custom restriction you want to assign to the role.
9. To finish, click **Save**.

> **Note:** If you add a custom restriction to a role that a user who is currently logged in to NetSuite is using, note the following. That user must log out and log back in to see the newly-assigned restriction.