Advanced Employee Permissions

August 7, 2019
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.

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc

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

Oracle may make available to Customer certain features that are labeled “beta” that are not yet generally available. To use such features, Customer acknowledges and agrees that such beta features are subject to the terms and conditions accepted by Customer upon activation of the feature, or in the absence of such terms, subject to the limitations for the feature described in the User Guide and as follows: The beta feature is a prototype or beta version only and is not error or bug free and Customer agrees that it will use the beta feature carefully and will not use it in any way which might result in any loss, corruption or unauthorized access of or to its or any third party's property or information. Customer must promptly report to Oracle any defects, errors or other problems in beta features to support@netsuite.com or other designated contact for the specific beta feature. Oracle cannot guarantee the continued availability of such beta features and may substantially modify or cease providing such beta features without entitling Customer to any refund, credit, or other compensation. Oracle makes no representations or warranties regarding functionality or use of beta features and Oracle shall have no liability for any lost data, incomplete data, re-run time, inaccurate input, work delay, lost profits or adverse effect on the performance of the Service resulting from the use of beta features. Oracle's standard service levels, warranties and related commitments regarding the Service shall not apply to beta features and they may not be fully supported by Oracle's customer support. These limitations and exclusions shall apply until the date that Oracle at its sole option makes a beta feature generally available to its customers and partners as part of the Service without a “beta” label.
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 .............................................................................................. 1
Before Enabling the Advanced Employee Permissions Feature ................................................. 1
Advanced Employee Permissions and Employee Searches ......................................................... 1
Advanced Employee Permissions and NetSuite Reports ........................................................ 6
Advanced Employee Permissions and Contact Records .......................................................... 6
Advanced Employee Permissions and SuiteScript ................................................................. 6
Advanced Employee Permissions and SuiteFlow ................................................................. 7
Advanced Employee Permissions and SuiteAnalytics Connect ............................................... 8
Advanced Employee Permissions and SOAP Web Services ................................................... 8
Advanced Employee Permissions and Customizations ......................................................... 8
Advanced Employee Permissions Overview ............................................................................. 10
Advanced Employee Permissions and Standard NetSuite Roles ............................................ 10
Employee Self Permission Overview ..................................................................................... 13
Employee Public Permission Overview ................................................................................... 16
Employee Confidential Permission Overview .......................................................................... 17
Employee Compensation Permission Overview ....................................................................... 19
Employee System Access Permission Overview ................................................................... 20
Employee Administration Permission Overview ..................................................................... 21
Advanced Employee Permissions Use Cases ........................................................................... 23
Setting Employee Access for Advanced Employee Permissions .......................................... 26
Creating Custom Advanced Employee Permissions ............................................................... 28
Advanced Employee Permissions

- Before Enabling the Advanced Employee Permissions Feature
- Advanced Employee Permissions Overview
- Setting Employee Access for Advanced Employee Permissions
- Creating Custom Advanced Employee Permissions

Before Enabling the Advanced Employee Permissions Feature

**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 NetSuite Reports
- Advanced Employee Permissions and Contact Records
- 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:** To avoid confusion, before you enable the Advanced Employee Permissions feature, review existing saved employee searches, and limit access to any searches that are not relevant to some users.

When using an account that does not have Advanced Employee Permissions enabled, it is only possible for employees to perform employee searches when they are assigned to a role that has the Lists > Employees, Lists > Employee Record, and Lists > Perform Search permissions.

However, when the Advanced Employee Permissions feature is enabled, many standard NetSuite roles are automatically given the Employee Public and Lists > Employee Record permissions, which gives them access to perform employee searches. Therefore, it is important that you review existing saved employee searches and limit access to any searches that are not relevant to some users.
Advanced Employee Permissions and Saved Searches

When Advanced Employee Permissions is enabled, based on the employee permissions assigned to the role, users will 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 not available to the employee permissions assigned to the role, the filter is not applied.

Saved Employee Search Results for Roles with Different Advanced Employee Permissions

The following section provides examples of what information is exposed to users when the same saved search is run using different Advanced Employee Permissions.

Example 1 — Employee Administration Permission: High Earning Employees in Toronto

When a user assigned to a role that has the Employee Administration permission runs a saved search that uses the filter criteria:

- Location — Toronto
- Base Wage — Greater than $100,000

Any employees that do not meet this criteria are filtered out. 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.

Example 2 — Employee Public Permission: High Earning Employees in Toronto

Now, when a user assigned to a role that has the Employee Public permission runs the same saved search that uses the filter criteria:

- Location — Toronto
- Base Wage — Greater than $100,000

The search shows different results, as you can see in the image below. This is because the Employee Public permission does not have access to see the base wage of employees, therefore this filter is not applied. Instead, this user sees all employee’s that meet the filter criteria of Location — Toronto.
Advanced Employee Permissions and Employee List View Results

The Employees List page generates the available columns, based on the fields the user has access to with the role they are using. All the employees, which they have permission to view all the fields for and which meet the set restrictions are displayed. 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:** NetSuite recommends that 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 will 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 — Employees List View Results with Employee Confidential and Employee Self Permissions.

Example 1 — Employees List Page Results with Employee Confidential Permission

For this example, the role assigned to the user has the Employee Confidential permission, which exposes the following fields:

- First Name
- Last Name
- Email
- Gender
- Job Title

With this permission, when the user selects **All** from the **View** dropdown list on the Employees List page, 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 are shown (First Name, Last Name, Email, Job Title, and Gender). This is because the Employee Confidential permission has the default restriction of Subordinates.
Example 2 — Employees List Page Results with Employee Self Permission

For this example, the role assigned to the user has the Employee Self permission, which exposes the following fields:

- First Name
- Last Name
- Email
- Job Title
- Birth Date

With this permission, when the user selects All from the View dropdown list on the Employees List page, the user sees the fields exposed with the Employee Self permission only for themselves. This is because the Employee Self permission has the default restriction of Own Only, meaning the user only has access to this information for themselves on their employee record.

Example 3 — Employees List View Results with Employee Confidential and Employee Self Permissions

For this last example, the role assigned to the user has a combination of the Employee Self and Employee Confidential permissions, which expose the following fields:

- Employee Confidential Permission
  - First Name
  - Last Name
  - Email
  - Gender
  - Job Title

- Employee Self Permission
  - First Name
  - Last Name
  - Email
Before Enabling the Advanced Employee Permissions Feature

- Job Title
- Birth Date

All View

With the Employee Confidential and Employee Self permission combination, when the user selects All from the View dropdown list on the Employees List page, the user sees an empty list. This is because the All view on the Employees List page generates the available columns, based on the fields the role has access to, across all roles, and displays all the employees that match all the fields that the user has access to. When fields are removed from the view, you will see the following message:

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.

Basic View

With Employee Confidential and Employee Self permission combination, when the user selects Basic from the View dropdown list on the Employees List page, the user sees themselves and their direct reports. This is because the field set contained in the Basic view is contained in most standard employee permissions.
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 details, see the help topic Access to Reports.

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 (), and any information specific to an employee's contact record can no longer be accessed.

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

Advanced Employee Permissions and SuiteScript

- 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 they attempt to access parts of the employee record that they are not permitted to access, with the role they are assigned.
  
  If needed, consider running these scripts as administrator, or revise the scripts to handle cases where some fields and subtabs are not accessible.

- A user could write or deploy a script that gains access to employee information that they would normally not be able to access. 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.

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

- 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.

Script Access

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

The fields and subtabs 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 a field or sublist exists before trying to do something with it. Simply calling functions and methods that interact with fields and sublists before checking whether they are there may result in inconsistent behavior.
For example, when the **Department** field is permitted on the employee record, and you check to see if this field exists and you do not have access, 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 are generated because whether the field exists, or whether you have access to the field is not checked.

```javascript
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.

```javascript
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.

```javascript
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](https://oracle-netSuite.com/docs/cp index) and [Client Script Best Practices](https://oracle-netSuite.com/docs/cp index).

### 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 be able to access. 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 subtabs 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. Scripts should be configured 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](https://oracle-netSuite.com/docs/cp index).
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:

- When a value for a field is set on the employee record in a SOAP web services program, and the current role does not have access to that field, the program completes without errors, but the field is not set or updated.
- For SOAP web services in accounts with Advanced Employee Permissions enabled, fields and subtabs that the current role does not have access to are not returned through search or filtering.

Advanced Employee Permissions and Customizations

Custom Roles

Custom roles created in your NetSuite account are not automatically updated with the employee permissions introduced by Advanced Employee Permissions. Custom roles will need to be manually updated to include any of the required employee permissions. For details, see Changing Access and Restrictions 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, when Advanced Employee Permissions is enabled, any customization created with NetSuite SuiteBuilder that are included with the standard Lists > Employees permission are preserved. However, customizations are not preserved when the Lists > Employees permission is customized. If required, you will need to manually add customizations to the custom Lists > Employees permission. For more information, see Creating Custom Advanced Employee Permissions.

Advanced Employee Permissions Overview

The Advanced Employee Permissions feature gives administrators more flexibility and control over which fields and subtabs on the employee record are available to the role, based on the assigned employee permissions.
This feature includes the following permissions: Employee Self, Employee Public, Employee Confidential, Employee Compensation, Employee System Access, and Employee Administration.

What happens when you enable the Advanced Employee Permissions Feature?

The following permissions are automatically assigned to a set of standard NetSuite roles, except where otherwise noted.

- **Employee Self** — Employees with this permission have access to relevant information about themselves on their employee record. This information can also be accessed by employees using their Employee Center role by clicking **My Profile** under **My Information**. For details, see [Employee Self Permission Overview](#).

- **Employee Public** — Employees with this permission have access to basic employee information, such as job title. For details, see [Employee Public Permission Overview](#).

- **Employee Confidential** — Employees with this permission have access to a set of fields and sublists, such as the **Billing Class** field, and the **Time-Off** subtab. For details, see [Employee Confidential Permission Overview](#).

- **Employee Compensation** — Employees with this permission have access to compensation information, such as base wage, and base wage type. For details, see [Employee Compensation Permission Overview](#).

- **Employee Administration** — This permission is not automatically assigned to any roles. For details, see [Employee Administration Permission Overview](#).

- **Employee System Access** — This permission is not automatically assigned to any roles. For details, see [Employee System Access Permission Overview](#).

With this feature, you can create custom employee permissions to include all or a set of standard fields and sublists from the employee record. You can also add custom fields and sublists to custom employee permissions. For more information, see [Creating Custom Advanced Employee Permissions](#).
**Note:** Inline editing is available only with the Lists > Employees permission at access level Edit or higher.

**Note:** When Advanced Employee Permissions is enabled, users who have access to effective dating logs will only see what they are permitted to see based on the permissions and restrictions assigned to their role. For example, roles with the Employee Confidential permission restricted to subordinates see effective dating logs only for their direct reports and below. For details, see the help topic Effective Dating for Employee Information.

### Advanced Employee Permissions Videos

- [View Advanced Employee Permissions Feature: Part 1 — Overview](#)
- [View Advanced Employee Permissions Feature: Part 2 — Creating Custom Advanced Employee Permissions](#)
- [View Advanced Employee Permissions Feature: Part 3 — Customizing a Role Using Advanced Employee Permissions](#)
- [View Advanced Employee Permissions Feature: Part 4 — Using Advanced Employee Permissions](#)

### Advanced Employee Permissions and Standard NetSuite Roles

The following table lists the standard NetSuite employee permissions, as well as the employee permissions introduced with the Advanced Employee Permissions feature that are automatically assigned to standard NetSuite roles. Also, listed are the default access levels and restrictions for each of the advanced employee permissions. Note that the Employee Administration and Employee System Access permissions are not automatically assigned to any standard roles. If required, these permissions can be manually added to a role.

- **Employee Self** permission:
  - If you change the access level of the Employee Self permission to level Edit, be aware that this will give employees the ability to make changes to the fields exposed with this permission, which includes their compensation information. It is recommended that you use the default access level View; however, if required, you can create a custom permission. For more information, see [Creating Custom Advanced Employee Permissions](#).
  - If you change the access level of the Employee Public, Employee Confidential, Employee Compensation, and Employee Administration permissions to level Edit, be aware that this will give users the ability to also create employees in NetSuite.
  - The standard NetSuite Lists > Employees permission gives access to all the 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 Lists > Employees permission, and add the Employee Administration permission. For details, see [Employee Administration Permission Overview](#).

<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Employee Permissions — Level of Access/Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>A/P Clerk</td>
<td>- Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>- Employee Record — View</td>
</tr>
<tr>
<td>A/R Clerk</td>
<td>- Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td>Standard Role</td>
<td>Employee Permissions — Level of Access/Restriction</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Accountant</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — Edit</td>
</tr>
<tr>
<td>Accountant (Reviewer)</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — View</td>
</tr>
<tr>
<td>Bookkeeper</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — Edit</td>
</tr>
<tr>
<td>Buyer</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full</td>
</tr>
<tr>
<td>CEO</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — Full</td>
</tr>
<tr>
<td>CEO (hands off)</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — View</td>
</tr>
<tr>
<td>CFO</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — Full</td>
</tr>
<tr>
<td>Chief People Officer (CPO)</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — Full</td>
</tr>
<tr>
<td>Employee Center</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Self — View/Own Only&lt;br&gt;■ Employee Confidential — View/Subordinates&lt;br&gt;■ Employee Compensation — View/Subordinates&lt;br&gt;■ Employee Record — Edit</td>
</tr>
<tr>
<td>Engineer</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — View</td>
</tr>
<tr>
<td>Engineering Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Confidential — View/Subordinates&lt;br&gt;■ Employee Compensation — View/Subordinates&lt;br&gt;■ Employee Record — View</td>
</tr>
<tr>
<td>Human Resources Generalist</td>
<td>■ Employee Public — View/Active and Non-Terminated&lt;br&gt;■ Employee Record — Full&lt;br&gt;■ Employees — Full</td>
</tr>
<tr>
<td>Standard Role</td>
<td>Employee Permissions — Level of Access/Restriction</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Intranet Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>Issue Administrator</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>Marketing Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>Payroll Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — Full</td>
</tr>
<tr>
<td>Payroll Setup</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — Full</td>
</tr>
<tr>
<td></td>
<td>■ Employees — Full</td>
</tr>
<tr>
<td>PM Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>Product Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>Support Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>QA Engineer</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>QA Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — View</td>
</tr>
<tr>
<td>Resource Manager</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>■ Employee Record — Full</td>
</tr>
<tr>
<td></td>
<td>■ Employees — View</td>
</tr>
<tr>
<td>Retail Clerk</td>
<td>■ Employee Public — View/Active and Non-Terminated</td>
</tr>
</tbody>
</table>
Advanced Employee Permissions Overview

<table>
<thead>
<tr>
<th>Standard Role</th>
<th>Employee Permissions — Level of Access/Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retail Clerk (Web Services Only)</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Record — Full</td>
</tr>
<tr>
<td></td>
<td>Employees — Full</td>
</tr>
<tr>
<td>Sales Administrator</td>
<td>Employee Public — View</td>
</tr>
<tr>
<td></td>
<td>Employee Record — Full</td>
</tr>
<tr>
<td></td>
<td>Employees — Full</td>
</tr>
<tr>
<td>Sales Manager</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>Employee Record — View</td>
</tr>
<tr>
<td>Sales Person</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Record — View</td>
</tr>
<tr>
<td>Sales Vice President</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Record — View</td>
</tr>
<tr>
<td>Store Manager</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>Employee Record — View</td>
</tr>
<tr>
<td>System Administrator</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Record — Full</td>
</tr>
<tr>
<td></td>
<td>Employees — Full</td>
</tr>
<tr>
<td>Warehouse Manager</td>
<td>Employee Public — View/Active and Non-Terminated</td>
</tr>
<tr>
<td></td>
<td>Employee Confidential — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>Employee Compensation — View/Subordinates</td>
</tr>
<tr>
<td></td>
<td>Employee Record — View</td>
</tr>
</tbody>
</table>

Employee Self Permission Overview

The Employee Self permission is intended for all employees. Users assigned to a role that has this permission can view basic personal information on the employee record. Basic personal information includes things such as home address, and passport information. This permission is automatically assigned to the Employee Center role when the Advanced Employee Permissions feature is enabled. By default, the access level for this permission it set to View, and the restriction is set to own only, but you can make changes. For details, 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 when assigned with a role that has 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 Creating Custom Advanced Employee Permissions.

### Employee Self Permission Fields

<table>
<thead>
<tr>
<th>Primary Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee ID</td>
</tr>
<tr>
<td>Mr./Ms</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Initials</td>
</tr>
<tr>
<td>Job</td>
</tr>
<tr>
<td>Supervisor</td>
</tr>
<tr>
<td>Image</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>Email</td>
</tr>
<tr>
<td>Phone</td>
</tr>
<tr>
<td>Office Phone</td>
</tr>
<tr>
<td>Mobile Phone</td>
</tr>
<tr>
<td>Home Phone</td>
</tr>
<tr>
<td>Fax</td>
</tr>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Classification:</td>
</tr>
<tr>
<td>Subsidiary</td>
</tr>
<tr>
<td>Department</td>
</tr>
<tr>
<td>Class</td>
</tr>
<tr>
<td>Location</td>
</tr>
</tbody>
</table>

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 Creating Custom Advanced Employee Permissions.

### Employee Self Permission SubLists

<table>
<thead>
<tr>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Shipping</td>
</tr>
<tr>
<td>Home</td>
</tr>
<tr>
<td>Label</td>
</tr>
<tr>
<td>Address</td>
</tr>
</tbody>
</table>
Employee Self Permission SubLists

- Edit

Human Resources

- Social Security
- Birth Date

Job Information:

- Job Description

Subordinates:

- Image
- Name
- Job Title
- Location
- Department
- Subsidiary
- Contact Info

Education:

- Level of Education
- Degree
- Date Conferred

Personal:

- Marital Status
- Ethnicity
- Gender

Time-Off

Available Now:

- Type
- Available this Year
- Used this Year
- Scheduled this Year
- Available Now

Balances:

- Type
- Carried Over
- Accrued
- Used
- Expired Carryover
- Balance

Compensation Tracking

- Compensation Currency
Employee Self Permission SubLists

- Base Wage Type
- Base Wage

Employee Public Permission Overview

The Employee Public permission is intended for all employees. Users assigned to a role that has this permission can view basic employee information. Basic information includes non-sensitive information, such as job title, and reporting relationships. This permission is automatically assigned to a set of standard roles when the Advanced Employee Permissions feature is enabled. By default, the access level for this permission is set to View, and the restriction is set to active and non-terminated, but you can make changes. For details, 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 Creating 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:**
  - 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 Creating Custom Advanced Employee Permissions.

**Employee Public Permission Sublist**

- **Subordinates**
Employee Confidential Permission Overview

The Employee Confidential permission is intended for manager roles. In addition to the employee public fields and sublists, users assigned to a role that has this permission also have access to 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. By default, the access level for this permission is set to View, and the restriction is set to subordinates, but you can make changes. For details, 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 Creating Custom Advanced Employee Permissions.

### Employee Confidential Permission Fields

<table>
<thead>
<tr>
<th>Primary Information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee ID</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Initials</td>
</tr>
<tr>
<td>Supervisor</td>
</tr>
<tr>
<td>Job</td>
</tr>
<tr>
<td>Image</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email</th>
<th>Phone</th>
<th>Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fax</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsidiary</td>
</tr>
<tr>
<td>Department</td>
</tr>
<tr>
<td>Class</td>
</tr>
<tr>
<td>Location</td>
</tr>
</tbody>
</table>
Employee Confidential Permission Fields

- 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 Creating 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
  - Purchase Approval Limit
  - Account

- Subordinates:
  - Image
  - Name
  - Job Title
  - Location
  - Department
  - Subsidiary
  - Contact Info

- Education:
  - Level of Education
### Employee Confidential Permission Sublists
- 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. Users assigned to a role that has 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. By default, the access level for this permission is set to View, and the restriction is set to subordinates, but you can make changes. For details, 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 Creating Custom Advanced Employee Permissions.

### Employee Compensation Permission Sublists

<table>
<thead>
<tr>
<th>Compensation Tracking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Wage</td>
</tr>
<tr>
<td>Base Wage Type</td>
</tr>
</tbody>
</table>
**Employee Compensation Permission Sublists**

| Compensation Currency
| Payroll
| Compensation Type

The **Base Wage**, **Base Wage Type**, and **Compensation Currency** fields are associated with the Compensation Tracking feature, and the **Compensation Type** field is part of SuitePeople US Payroll. For details, see the help topics Tracking an Employee’s Compensation and Including an Employee in Payroll.

**Employee System Access Permission Overview**

The Employee System Access permission is intended for IT administrators. Users assigned to a role that has this permission can 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 the Employee System Access permission can give access and assign roles to employees in their location only.

**Note:** The Employee System Access permission is not automatically assigned to standard roles when the Advanced Employee Permission feature is enabled.

**Employee System Access Permission Fields**

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

**Employee System Access Permission Fields**

Primary Information:

- Employee ID
- Name

Email | Phone | Address:

- Email

**Employee System Access Permission Sublist**

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

**Employee System Access Permission Sublist**

Access

- Give Access
- IP Address Restriction
- Inherit IP Rules from Company

Roles:

- Role

Global Permissions:
**Employee Administration Permission Overview**

The Employee Administration permission is intended for HR Generalists and HR Administrators. In addition to the employee public fields and sublists, users assigned to a role that has this permission have access to a limited set of fields and sublists based on the restrictions defined on the Role page.

**Note:** The Employee Administration permission is not automatically assigned to standard roles when the Advanced Employee Permissions feature is enabled.

**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 [Creating 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
Employee Administration Permission Fields

- Department

Employee Administration 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 Creating Custom Advanced Employee Permissions.

Employee Administration Permission Sublists

**Address**
- Default Shipping
- Home
- 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:
Employee Administration Permission Sublists

- Level of Education
- Degree
- Date Conferred
- Personal:
  - Marital Status
  - Ethnicity
  - Gender

Advanced Employee Permissions Use Cases

The following section provides examples of how standard NetSuite permissions and advanced employee permissions can be combined to expose 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 System Access Permission Overview
- Employee Administration Permission Overview

Note: These examples use the default advanced employee permissions, but you can customize these permissions. For details, see Creating Custom Advanced Employee Permissions and Setting Employee Access for Advanced Employee Permissions.

The Lists > Employee Record, Lists > Perform Search, and Lists > Employees permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to use Advanced Employee Permissions. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

Example 1: Employee Access for All Employees

<table>
<thead>
<tr>
<th>Permission</th>
<th>Access Level</th>
<th>Restriction</th>
<th>Gives Employees Access To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists &gt; Employee Record*</td>
<td>Edit</td>
<td>—</td>
<td>Access employee menus, for example List &gt; Employees.</td>
</tr>
</tbody>
</table>
### Advanced Employee Permissions Overview

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 use Advanced Employee Permissions. For more information about the standard permissions, see the help topic [NetSuite Permissions Overview](#).

#### Example 2: Employee Access for Managers

<table>
<thead>
<tr>
<th>Permission</th>
<th>Access Level</th>
<th>Restriction</th>
<th>Gives Managers Access To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists &gt; Employee Record*</td>
<td>View</td>
<td>—</td>
<td>Access employee menus, for example List &gt; Employees.</td>
</tr>
<tr>
<td>Lists &gt; Perform Search*</td>
<td>Full</td>
<td>—</td>
<td>Search for employees.</td>
</tr>
<tr>
<td>Employee Confidential</td>
<td>View</td>
<td>Subordinates</td>
<td>View and search confidential employee information, such as hire date and expense limit, for direct reports and below.</td>
</tr>
<tr>
<td>Employee Compensation</td>
<td>View</td>
<td>Subordinates</td>
<td>View compensation information for direct reports and below.</td>
</tr>
<tr>
<td>Employee Public</td>
<td>View</td>
<td>Active and Non-Terminated</td>
<td>View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.</td>
</tr>
<tr>
<td>Employee Self</td>
<td>View</td>
<td>Own Only</td>
<td>View relevant information about themselves on their employee record, such as job description and address.</td>
</tr>
</tbody>
</table>

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 use Advanced Employee Permissions. For more information about the standard permissions, see the help topic [NetSuite Permissions Overview](#).

#### Example 3: Employee Access for HR Generalists

<table>
<thead>
<tr>
<th>Permission</th>
<th>Access Level</th>
<th>Restriction</th>
<th>Gives HR Generalists Access To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists &gt; Employee Record*</td>
<td>Full</td>
<td>—</td>
<td>Access employee menus, for example List &gt; Employees.</td>
</tr>
<tr>
<td>Lists &gt; Perform Search*</td>
<td>Full</td>
<td>—</td>
<td>Search for employees.</td>
</tr>
</tbody>
</table>

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 use Advanced Employee Permissions. For more information about the standard permissions, see the help topic [NetSuite Permissions Overview](#).
### Advanced Employee Permissions Overview

#### Permission | Access Level | Restriction | Gives HR Generalists Access To
---|---|---|---
Employee Administration | Full | Inherit from Role | View, create, edit, and search for personal information, such as home phone and marital status, 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.

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 use Advanced Employee Permissions. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

### Example 4: Employee Access for HR Directors and Above

#### Permission | Access Level | Restriction | Gives HR Directors and Above Access To
---|---|---|---
Lists > Employee Record* | Full | — | Access employee menus, for example List > Employees.

Lists > Perform Search* | Full | — | Search for employees.

Lists > Employees* | Full | — | View, edit, and create employee record information for all employees who match the restrictions defined on the Role page. For example, if a location restriction is set, access is only for the employees in the set location or sublocation. If no restrictions are defined, access is given to all the information on the employee record for every employee.

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.

The Lists > Employee Record, Lists > Perform Search, and Lists > Employees permissions are standard NetSuite permissions, and are not part of Advanced Employee Permissions. However, these permissions are required to use Advanced Employee Permissions. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

### Example 5: Employee Access for IT Administrators

#### Permission | Access Level | Restriction | Gives IT Administrators Access To
---|---|---|---
Lists > Employee Record* | View | — | Access employee menus, for example List > Employees.
### Advanced Employee Permissions Overview

<table>
<thead>
<tr>
<th>Permission</th>
<th>Access Level</th>
<th>Restriction</th>
<th>Gives IT Administrators Access To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists &gt; Perform Search*</td>
<td>Full</td>
<td>—</td>
<td>Search for employees.</td>
</tr>
<tr>
<td>Employee System Access</td>
<td>Full</td>
<td>Inherit from Role</td>
<td>Give access and assign roles to employees who match the restrictions defined on the Role page.</td>
</tr>
<tr>
<td>Employee Public</td>
<td>View</td>
<td>Active and Non-Terminated</td>
<td>View and search basic employee information, such as email address and supervisor, for all active, non-terminated employees.</td>
</tr>
</tbody>
</table>

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 use Advanced Employee Permissions. For more information about the standard permissions, see the help topic NetSuite Permissions Overview.

### Setting Employee Access for Advanced Employee Permissions

Additional levels of restrictions and access to employee information can be specified on the Employee Access subtab of the Role page.

**To set employee access:**

1. Go to Setup > Users/Roles > Manage Roles.
2. From the list, click Customize or Edit beside the role you want to assign custom employee access to.
3. Click the Employee Access subtab.
4. From the Permission list, select the employee access you want to add to the role. Choose from the following:
   - **Employee System Access** — This permission is intended for IT Administrators. Users assigned to a role with this permission can give access and assign roles to employees. For details, see Employee System Access Permission Overview.
   - **Employee Administration** — This permission is intended for HR Generalists and HR Administrators. Users assigned to a role with this permission have access to HR related fields on the employee record. For details, see Employee Administration 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 details, see Employee Confidential 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 details, see Employee Compensation 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 details, see Employee Public 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 details, see Employee Self Permission Overview.
Setting Employee Access for Advanced Employee Permissions

- **Employees** — This permission is intended for HR Business Partners, CPOs, and HR Directors. Users assigned to a role with this permission have access to all information on the employee record.

  **Note:** When you select a permission, the default access level and restrictions are automatically selected, but you can change these.

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

  **Note:** When two employee permissions are included with a role, one at level view and another at level edit, 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.

6. If required, change the default restriction for the selected restriction from the **Restrictions** list. Choose from the following:

   - **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*.
   
   - **Subordinates** — Select this when you want the permission to be restricted by subordinates. For example, you could add this restriction to the Employee Confidential permission, so that users assigned to this role would have access to public and confidential employee information only for their subordinates.
   
   - **Active and Non-Terminated** — Select this when you want the permission to be restricted to active and non-terminated employees. For example, you could add this restriction to the Employee Public permission, so that users assigned to this role would have access to basic employee information for all active and non-terminated employees only.

   - **Own Only** — Select this when you want to restrict the permission to own only. This means, 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, so that users assigned to this role would only have access to basic personal employee information for themselves.

7. Click **Add**.

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

**Note:** If you assign an additional role to a user who is currently logged in to NetSuite, that user must log out and log back in to see the newly assigned role. The same is true if you add permissions to an existing role while a user is currently logged in to NetSuite. The user needs to log out and log back in to exercise the new permissions.

### Creating Custom Advanced Employee Permissions

**Important:** When creating a custom employee permission, be aware that some fields on the employee record have dependencies on other fields, and should not be added or removed individually. For example, when you customize the Employee System Access permission, having only a partial set of the fields that come standard with this permission will prevent the employee record from loading. The employee record will only load when it has either all or none of the access fields.

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 also customize a standard employee permission to only include a subset of the fields and sublists that are exposed, or customize it to include additional fields and sublists.

Standard employee permissions cannot be modified, so it is recommended that you use these permissions as templates to create your own custom employee permissions.

### Creating Custom Advanced Employee Permissions

**Important:** Before creating custom advanced employee permissions:

- By default, when the Advanced Employee Permissions feature is enabled, any customization's created with NetSuite SuiteBuilder that are included with the standard Lists > Employees permission are preserved. However, customization’s are not preserved when the Lists > Employees permission is customized. If required, customization’s need to be manually added to the custom Lists > Employees permission.
- 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 (including third-party scripts) may fail if they attempt to access parts of the employee record that they are not permitted to access, with the role and permissions they are assigned.

For more information, see [Before Enabling the Advanced Employee Permissions Feature](#).

**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.
   a. 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.
   b. To create a new employee permission that does not start with a list of associated fields and sublists, select **New Permission** from the Manage Permissions page.

3. If required, you can add standard and custom fields to the permission. For more information, see Adding Standard Fields and Sublists to Advanced Employee Permissions and Creating Custom Fields for Advanced Employee Permissions.

4. To finish, click **Save**.

To remove the permission, click **Actions > Delete**. When the permission is assigned to a role you will need to remove it from the role before it can be deleted.

Related Topics
- Before Enabling the Advanced Employee Permissions Feature
- Advanced Employee Permissions Overview
- Setting Employee Access for Advanced Employee Permissions

Adding Standard Fields and Sublists to Advanced Employee Permissions

⚠️ **Important:** When you add a sublist to a custom permission that is associated with another feature in NetSuite, the specific permission for the feature also needs to be added to the role. If the role does not have the required permission for the feature users will 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 you need to make sure that the Time-Off Administration permission is included. For more information, see the help topics SuitePeople Permission Requirements and Permissions Documentation.

To add standard fields and sublists to 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 > Standard Fields subtab.
   Or:
4. To add a standard sublist, select the Sublists > Standard Sublists subtab.
5. Click a line in the list.
6. From the **Record Type** list, select **Employee**.
7. From the **Field** list, select the field to add to the permission.
   Or:
8. From the **Sublist** list, select the sublist to add to the permission.
9. Click **Add**.
Creating Custom Advanced Employee Permissions

10. Repeat these steps for each field and sublist that you want to include.
11. To finish, click Save.

Alternatively, click +Insert, select the employee record and field, and click Add. To remove a field, select it from the list, and click Remove.

Related Topics
- Before Enabling the Advanced Employee Permissions Feature
- Advanced Employee Permissions Overview
- Setting Employee Access for Advanced Employee Permissions

Creating Custom Fields for Advanced Employee Permissions

**Important:** Permission access levels are set on the Role page, when the advanced employee permission is assigned to the role and not on the custom entity record. For example, if a 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:

2. In the Label field, enter a name or description for the field. You can enter up to 200 characters for the label.
3. From 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 that you want to associate this custom field with. 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. To remove a permission, select it from the list, and click Remove.
8. Repeat these steps 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. You can see a list of the custom fields associated with a permission from the Fields > 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 the Edit View button from the Employees List page and manually add the custom fields.

Related Topics
- Before Enabling the Advanced Employee Permissions Feature
- Advanced Employee Permissions Overview
- Setting Employee Access for Advanced Employee Permissions
Creating Custom Sublists for Advanced Employee Permissions

To create custom sublists for advanced employee permissions:

**Important:** Permission access levels are set on the Role page, when the advanced employee permission is assigned to the role and not on the custom entity record. For example, if a permission is assigned to a role at access level View, any custom fields that are added to the permission respect that access level.

1. To create a custom sublist, go to Customization > Forms > Sublists > New.
2. In the **Type** field, select **Entity**.
3. Check the **Employee** box.
4. In the **Search** field, 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. In the **Tab** field, select the subtab where 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.

Related Topics

- Before Enabling the Advanced Employee Permissions Feature
- Advanced Employee Permissions Overview
- Setting Employee Access for Advanced Employee Permissions

Adding Custom Fields and Sublists to Advanced Employee Permissions

To add custom fields and sublists to advanced employee permissions:

1. Go to Setup > Users/Roles > Manage Permissions.
2. Click **Customize** or **Edit** beside the permission you want to add a custom sublist to.
3. Click the **Sublists > Custom Sublists** subtab.
   Or:
4. Click the **Fields > Custom Fields** 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.
   Or:
8. From the **Field** list, select the custom field to add to the permission.
9. Click **Add**. Alternatively, click **+Insert**, select the record type and sublist, and click **Add**
10. Repeat these steps for each custom sublist and field you want to add to the permission.
11. To finish, click **Save**.

Related Topics
- Before Enabling the Advanced Employee Permissions Feature
- Advanced Employee Permissions Overview
- Setting Employee Access for Advanced Employee Permissions