



# Security



2024.2

October 9, 2024



Copyright © 2013, 2024, Oracle and/or its affiliates.

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.

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

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.

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 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>

#### 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](http://www.netsuite.com/tos), where the term "Service" shall mean the OpenAir Service.

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.

# Table of Contents

Overview .....	1
Product Overview .....	1
Standard Features .....	2
Encryption .....	2
Masking .....	2
TLS Protocol and Cipher Suites .....	3
Availability .....	3
Data Control .....	4
Privacy Considerations .....	4
General Security Principles .....	9
Configuration .....	11
Initial OpenAir Configuration .....	11
Mail Domain and Firewall Configuration .....	11
DMARC Alignment and OpenAir Email .....	12
Setting Up DKIM for OpenAir Notifications .....	13
Custom Email Return Path .....	14
Automatic Backup Service .....	16
Security Features .....	19
The Security Model .....	19
Configuring and Using Authentication .....	21
Authentication by OpenAir .....	22
SAML Authentication .....	30
NetSuite Single Sign-On .....	31
OAuth 2.0 Token Based Authentication .....	31
Configuring and Using Access Control .....	41
Roles Overview .....	41
Filter Sets Overview .....	48
Form Permissions .....	53
Employee Access Control Settings .....	62
Guest Roles and Guests .....	69
Configuring and Using Auditing features .....	70
Reports Overview .....	70
Audit Trail Fields .....	76
Quick Audit Trail on Forms .....	80
Data Export for Auditing .....	82
Configuring and Using OpenAir Integrations and Add-on Services .....	88
Add-on Services — Security Considerations .....	89
Business Intelligence Connector — Security Considerations .....	93
NetSuite Connector — Security Considerations .....	93
Enabling and Controlling Access to OpenAir Platform Tools .....	95
Security Considerations for Developers .....	100

# Overview

This guide outlines the security features currently available for OpenAir and describes security-related controls and configuration settings.

This chapter gives an overview of the product, outlines some standard security features and explains the general principles of application security. It contains the following sections:

- [Product Overview](#)
- [Standard Features](#)
- [General Security Principles](#)

## Product Overview

From resource management and project management, to time and expense tracking, project accounting and advanced billing and invoicing, OpenAir supports the entire professional services delivery lifecycle with a powerful Cloud suite. The OpenAir platform is a comprehensive offering of configurability, cloud development tools and infrastructure that enables customers and software developers to maximize the benefits of cloud computing. OpenAir is architected as a multi-tenant cloud platform that provides the core infrastructure, including support, for industrial-strength standards of high availability, disaster recovery and security as well as an integrated scripting capability and a set of APIs to build and connect applications to the platform.

OpenAir was designed with industry standard security features:

- On the transport layer, all pages within the application are delivered using the HTTPS protocol. See [TLS Protocol and Cipher Suites](#).
- Different authentication methods, IP address restriction and session timeout features are available to protect your OpenAir environment from unauthorized access. See [Configuring and Using Authentication](#) under [Security Features](#).
- The backbone of the OpenAir security model is built on a roles and permissions model, in which users are given roles that define their access level to records, reports and add-on services. See [Configuring and Using Access Control](#) under [Security Features](#).
- OpenAir's auditing capabilities give you the flexibility to achieve your control objectives, including tracking data and configuration changes as well as user sign-in attempts. See [Configuring and Using Auditing features](#) under [Security Features](#).
- The access control and other security measures also apply to the OpenAir integrations and add-on services. See [Configuring and Using OpenAir Integrations and Add-on Services](#) and [Enabling and Controlling Access to OpenAir Platform Tools](#) under [Security Features](#).
- Constraints and limitations enforced on platform tools provide some safeguards for developers looking to extend OpenAir features and integrations. See [Security Considerations for Developers](#)

# Standard Features



**Important:** OpenAir is not intended to store personal information such as social security numbers or government ID numbers. The following security features are not natively supported as they fall out of OpenAir's intended scope:

- Anonymization
- Pseudonimization
- Truncation
- Tokenization

Customers are responsible for ensuring that their end users do not inappropriately store personal information in the OpenAir application.

This section reviews the following standard security features:

- [Encryption](#)
- [Masking](#)
- [TLS Protocol and Cipher Suites](#)
- [Availability](#)
- [Data Control](#)
- [Privacy Considerations](#)

These are inherent product security and privacy features that require little or no configuration. For security controls requiring configuration, see [Configuration](#) and [Security Features](#) chapters.

## Encryption

OpenAir uses the following cryptographic measures to ensure the security of your data.

- OpenAir web services are protected by HTTPS over TLS. All data is encrypted in transport.
- OpenAir Production and Disaster Recovery data centers use the Advanced Encryption Standard (AES) algorithm with 256-bit encryption to encrypt data at rest.
- The Automatic Backup Service (ABS) allows customers to set up a regular delivery of their OpenAir account data to an email address or SCP/SFTP server. The data is compressed as a ZIP file and can be PGP-encrypted for additional security. See [Automatic Backup Service](#).
- User passwords stored in the database are one-way hashed using BCrypt.

## Masking

Password values are masked as they are typed. This includes built-in password fields as well as password custom fields and script parameters.

Form permissions can be used to control what information is captured on many OpenAir entity forms. The information captured can be conditional on selected field values. This functionality can be applied to both standard fields and custom fields. See [Form Permissions](#) and [Permission Rules](#).

The Hide personal user information on reports internal feature can be used to hide information such as addresses and phone numbers in timesheet reports. To enable this feature, contact OpenAir Customer Support.

## TLS Protocol and Cipher Suites

The Transport Layer Security (TLS) protocol is an established method for ensuring private, trustworthy, and reliable communication between computer programs over a network. Computer programs use the HTTPS protocol to establish communication with each other using the TLS encryption protocol. After the computers have agreed on which cipher to use, authenticated each other, and selected a method to ensure reliable communication, they agree to communicate. This exchange is known as the TLS handshake.

Each new version of the TLS protocol enhances these qualities. TLS 1.2 is the version currently supported for use in OpenAir. All inbound and outbound secure communication must use TLS 1.2.

### Supported Cipher Suites

OpenAir currently supports the following cipher suites

- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384



**Important:** The list of supported ciphers is subject to change at any time. It is your responsibility to be aligned with the highest possible level of security available in the industry. This applies to:

- **Browser access** — Users should update to the latest browser versions and OS versions to ensure they are using up to date ciphers.
- **Integration client access** —IT/Technical teams need to be sure connections from any integration tools have supported ciphers enabled.

## Availability

OpenAir Service Level Commitment guarantees a 99.5% uptime (outside of scheduled service windows) for the OpenAir production applications for all customers.

The following site may be used to check the OpenAir system status at any time: <https://status.openair.com>. This site is available even if the OpenAir web application is experiencing a service interruption or downtime.

All OpenAir accounts in all environments are hosted in Oracle Cloud Infrastructure (OCI). For more information about OCI, see <https://cloud.oracle.com/iaas/architecture>. In OCI, data is backed up using the [OCI Gold policy](#).

A secondary data center in California provides disaster recovery and failover capabilities should the primary data center become non-operational. The secondary data center will eventually be replaced by another region in OCI.

OpenAir has an SSAE 18 (SOC1/SOC2)/ISAE 3402 Type II audit conducted annually and a report prepared by an accredited third-party external auditor. The report contains information about policies, procedures, and controls relevant to data backups, offsite storage, restore, system availability, and uptime. A copy of the report can be provided to customers on request.



**Tip:** You can use NetSuite Account Center to request the audit report. See the help topic [NetSuite Account Center](#).

For reference, see the [Service level commitment for the OpenAir Service](#), the [Terms of Services](#) and [Oracle Cloud Services Contracts](#).

## Data Control

Following the expiration or termination of the OpenAir Service, data is deleted from all live and non-live environments after six months of the account cancellation date.

OpenAir provides customers with the option to allow authorized support employees to access a backup copy of the customer account in a sandbox environment to investigate cases submitted by the customer. This is used for troubleshooting complex cases, and the related sandbox environment is deleted after 30 days of inactivity, if not sooner.

## Privacy Considerations

Personal data is protected under privacy and data protection laws, ordinances, and regulations in many countries around the world. Customers are responsible for assessing the legal and operational implications of any applicable privacy and data protection laws on their business. In particular, Customers are responsible for:

- The identification and subsequent redaction, anonymization or pseudonymization of any personally identifiable information (PII) or other data pertinent to the privacy regulations in their production account and in any sandboxes which they own.
- Considering any applicable cookies consent requirements when collecting and tracking personal data from end users.

OpenAir makes the following provisions to enable you to meet your regulatory obligations:

- [Data Minimization](#)
- [End-User Access](#)
- [Data Deletion](#)
- [Data Portability](#)
- [Tracking Technologies](#)
- [Notice and Consent](#)
- [Right to Erasure or Right to Be Forgotten](#)
- [Personally Identifiable Information \(PII\) Redaction](#)



- [Requesting Purge of Deleted Records or Audit Trail Data](#)

## Data Minimization

OpenAir provides a Role Based Access Control (RBAC) model to set up authorization policies for users. These policies control the functionality available to users and can be set up by customers to enforce separation of duties. Filter sets can be used to control what data the user can view or update. See [The Security Model](#) and [Roles Overview](#).

Form permissions can be used to control what information is captured on many OpenAir entity forms. This functionality can be applied to both built-in and custom fields. See [Form Permissions](#).


User scripts can also be used to ensure the data collected is sufficient and limited to what is necessary.

## End-User Access

End-user data is accessible through the web application, APIs, Automatic Backup Services (ABS) and user scripts. Data access, correction, and deletion can be performed by the end-users themselves or by authorized personnel with the correct permissions and restrictions. OpenAir end-users with access can also use the SOAP API or XML API or user scripts to programmatically access, modify, or delete their data.

## Data Deletion

Users with appropriate role permissions can delete transactions or records using the OpenAir web application or OpenAir API.

 **Note:** Only transactions or records which are not associated with another transaction or a child record can be deleted, unless those associated transactions or records themselves have been deleted.

A deleted transaction or record cannot be recovered. A new transaction or a record needs to be created to replace the deleted one.

API Access is a licensed add-on and must be purchased separately. To enable API Access for your account, contact your OpenAir account manager or OpenAir Professional Services.

When a user deletes a record in OpenAir, the record is flagged as deleted. The record is not removed immediately from the OpenAir database.

Deleted records are retained in the OpenAir database for a minimum of 180 days. Older deleted records, that is, records marked as deleted and last updated 180 or more days ago, are removed permanently from the database according to a routine schedule.

- Starting February 24, 2024 on sandbox accounts, and March 9, 2024 on production accounts, the removal process will run every week on the weekend. Each deleted record will remain available in the OpenAir database for a minimum of 180 days and up to one to two weeks after this minimum retention period.
- Previously, the removal process ran two times a year during major OpenAir release windows. Each deleted record remained available in the OpenAir database for a minimum of 180 days and up to one year after the record was marked as deleted.

Deleted records cannot be removed permanently or modified by your company's account administrators during the retention period.

Account administrators may request the expedited purge of specific records flagged as deleted for regulatory compliance. See [Requesting Purge of Deleted Records or Audit Trail Data](#).


Following the expiration or termination of the OpenAir Service, data is deleted from all live and non-live environments after six months of the account cancellation date. See also [Data Control](#).

## Data Portability

Users with appropriate permissions can export account, batch or list data.


OpenAir Automatic Backup Service (ABS) lets you set up a regular delivery of your OpenAir data. See [Automatic Backup Service](#).

Users with appropriate permissions can use the API to retrieve data.

 **Note:** The Automatic Backup Service (ABS) and API Access are licensed add-ons and must be purchased separately. To enable the Automatic Backup Service (ABS) or API Access for your account, contact your OpenAir account manager or OpenAir Professional Services.

## Tracking Technologies


The OpenAir website collects certain information about the user's computer and internet connection, such as the IP address, the date and time of access, actions, the computer technology which is being used, and movements and preferences on the website. The service only uses functional (not tracking) cookies for maintaining sign-in sessions and personalization, and no third-party cookies. Session ID cookies generated from regular OpenAir sign-ins are set to expire depending on the session timeout time set by the customer. For SAML sign-ins, the Session ID cookies are set to expire after 300 seconds of inactivity. For all other OpenAir cookies, they are removed after the browser is closed.

 **Important:** Customers are responsible for assessing the legal and operational implications of any regulation on their business, and for considering any applicable cookies consent requirements when collecting and tracking personal information from end users.

## Notice and Consent

Dashboard messages can be used to display notice information which can include your entire notice or provide an external URL to your privacy notice.

Custom fields can be used to create a mechanism for employees to give or withdraw consent.

Administrators can set up an automated email notification feature using the query builder to inform users and refresh consent if anything changes. For more information about dashboard messages and the query builder, see  [Administrator Guide](#).

## Right to Erasure or Right to Be Forgotten

OpenAir provides many options to delete personal data, either manually or automatically. These features are either available by default or require some configuration. See [Data Deletion](#) and [Requesting Purge of Deleted Records or Audit Trail Data](#).

Administrators and users with the appropriate role permissions can:

- Use the OpenAir web application or the API to permanently obfuscate personal information held for terminated or inactive employees.
- Use the Personal Information (PI) feature to redact personally identifiable information (PII) for employees, customers and contacts. See [Personally Identifiable Information \(PII\) Redaction](#).
- Delete expense report attachments using a wizard.
- Run maintenance tasks to delete script log entries.

## Personally Identifiable Information (PII) Redaction

Personally identifiable information (PII) is data that can be used to determine a person's identity. Rules and regulations about PII vary by country, but usually include strict guidelines covering personal information acquisition, storage, and removal. The right to be forgotten is one of the key requirements in recent privacy laws, including in General Data Protection Regulation (GDPR). Administrators can use the PI Removal feature to replace the data stored in OpenAir with a standard value depending on the field type.


The PI Removal optional feature:

- Remove personal information (PI) from relevant standard, custom, and audit trail fields.
- Improves compliance with privacy regulation.
- Permits an authorized user to create, submit, and approve individual PI removal requests from within OpenAir, or review all the requests that have been submitted, including who created the request, when it was created, and the current status of the request.

Submitted PI removal requests must be approved before they are queued for processing. OpenAir processes approved PI removal request automatically on a set day and time each week. PI removal requests approved in the last 72 hours at the time of processing are not processed immediately but the following week. This allows a minimum of 72 hours to cancel an approved PI removal request, should it be required.

After a PI removal request is processed, the PII is redacted permanently from OpenAir and the status of the PI removal request shows as completed. Users with the appropriate privileges can cancel the request at any time before its status shows as completed.

Email notifications are sent to all users with access privilege to use the PI Removal feature every time a request is submitted, approved, rejected, or canceled.

 **Note:** To enable this feature, contact OpenAir Customer Support.

For more information about using the feature, see .

## Requesting Purge of Deleted Records or Audit Trail Data

When a user deletes a record in OpenAir, the record is flagged as deleted. The record is not removed immediately from the OpenAir database. Deleted records are retained in the OpenAir database for a minimum of 180 days. Older deleted records, that is, records marked as deleted and last updated 180 or more days ago, are removed permanently from the database according to a routine schedule. See [Data Deletion](#).

Account administrators may request the expedited purge of specific data for regulatory compliance. The following information can be permanently removed from the OpenAir database:

- Specific records flagged as deleted which need to be purged before it is due to be purged as part of the regular data maintenance cycle.
- Specific audit trail data or any other specific data which cannot be modified by account administrators.

Valid requests are processed within 30 days.



**Important:** Do the following before requesting the purge of deleted record or audit trail data:

- Use the PI Removal feature to redact personally identifiable information (PII) from any contact, customer and employee records, including audit trail data. Redact PII from records before you delete them, where possible. For more information about the PI Removal feature, see [Personally Identifiable Information \(PII\) Redaction](#) and [PI Removal](#).
- Review the [Purge Request Guidelines](#).

### To request the purge of specific audit trail data or specific records flagged as deleted:

1. Make sure any data or personally identifiable information has been removed from the affected fields on the records.
2. Go to SuiteAnswers and create a support case. See the help topic [Creating a Support Case](#).
3. Specify your request fully and clearly. Provide all of the following information:
  - Business justification for the request — The request must proceed from regulatory obligations.
  - Name or dbid of any sandbox accounts from which the data also needs to be removed.
  - Required completion date — A minimum of twelve US business days is required.
  - Clear and detailed identification of the data to be removed — Include:
    - The internal IDs and table names of the records. Indicate whether internal IDs are different in your production and any sandbox accounts you may have, and provide the internal IDs for each account.
    - The specific names of fields needing audit trail data removed. Provide field names as they appear in the OpenAir database, and not in the OpenAir UI. Indicate whether the names and internal IDs of custom fields are different in your production and any sandbox accounts you may have, and provide the custom field names for each account. Reference custom fields using the custom\_<id> convention where <id> is the internal ID for the custom field.



**Tip:** Use the [OpenAir Data Dictionary](#) and other technical documentation to identify the table names and standard field in the OpenAir database.

## Purge Request Guidelines

Review the following guidelines before requesting the purge of deleted record or audit trail data:

- Any request to purge or delete data must be made by an account administrator and proceed from regulatory requirements.
- Any such request must be made in writing to OpenAir Customer Support and must include all the required information listed in the instructions for [Requesting Purge of Deleted Records or Audit Trail Data](#).
- Use the PI Removal feature to redact personally identifiable information (PII) from any contact, customer and employee records, including audit trail data. Redact PII from records before you delete them, where possible. For more information about the PI Removal feature, see [Personally Identifiable Information \(PII\) Redaction](#) and [PI Removal](#).
- OpenAir Engineering will only remove audit trail information if this information cannot be removed using the PI Removal feature.
- OpenAir Engineering will only purge deleted records. Make sure you delete the records in all your company's production and sandbox accounts before submitting the purge request.

- All data from the specified fields in the specified records will be removed or redacted by OpenAir engineering within twelve business days of receiving the request. OpenAir makes no assurances for timely removal of data by any required date fewer than twelve US business days notice.
- There will be no record of what specific data was removed other than the information you provide in the support case requesting the purge. You are entirely responsible for retaining any important information in another system or medium should you require it in the future for any reason.
- There is no restoration or rollback capability after the removal of deleted record and audit trail data. The information is deleted permanently and cannot be recovered.
- OpenAir Engineering will propagate those changes to all environments not owned by the customer (such as support sandboxes) or otherwise assure their removal.

## General Security Principles

The following principles are fundamental to using any application securely.

### Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. This applies to add-on services and other integration applications connecting to OpenAir as well as operating systems and browser technology.

In the specific case of Web Browser support, the following four browsers are supported in accordance with the vendor support policy: Google Chrome (most current major stable channel release), Mozilla Firefox (most current major ESR version and above, in production only), Apple Safari (most current major production release and one prior release), and Microsoft Edge (latest major version of Microsoft Edge Chromium). Other versions may continue to work with OpenAir but are not officially supported. Microsoft Explorer 11 is no longer supported.

Operating System	Chrome	Firefox	Microsoft Edge	Safari
macOS	Supported	Supported	—	Supported
Windows	Supported	Supported	Supported	Not Supported

See also [Oracle Software Web Browser Support Policy](#).

### Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, etc., especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

When an employee leaves, immediately remove their access to OpenAir.

### Separation of Duties

Beyond limiting user privilege level, you also limit user duties, or the specific jobs they can perform with OpenAir. No user should be given responsibility for more than one related function. This limits the ability

of a user to perform a malicious action and then cover up that action. For example, you may not want the same user or role to be responsible for both entering a transaction (timesheet, expense report, or invoice, for example) and approving that transaction.

## Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

## Keep Up To Date on Latest Security Information

OpenAir continually improves its software and documentation. Advance customer notifications will be sent by email regarding any changes impacting system infrastructure or security. These Announcements will also be posted to the [OpenAir User Group](#).

# Configuration

This chapter outlines some initial configuration required as part of deploying an OpenAir account. This includes:

- [Initial OpenAir Configuration](#)
- [Mail Domain and Firewall Configuration](#)
- [DMARC Alignment and OpenAir Email](#)
- [Automatic Backup Service](#)

## Initial OpenAir Configuration

OpenAir Professional Services discuss the unique needs of your business with you and perform the initial configuration of your OpenAir account during deployment. This initial set up includes security configuration changes that must be made after an account is provisioned:

- **Change default user passwords** — Administrative users will be required to change their password the first time they sign in. You should sign in to each administrative user account and set new passwords immediately.
- **Enforce password management** — The password policy for your OpenAir account is configured by OpenAir Professional Services during deployment and applies to all user passwords. The password policy parameters include the password length, complexity, history and lifetime. The password policy can only be configured by OpenAir Professional Services or by OpenAir Customer Support to ensure it meets the standard strength requirements for cloud services.
- **Convention for user IDs** — Typically, the convention for OpenAir user IDs will follow existing corporate standards as used in network user IDs or email addresses, for example.
- **Session expiration** — It is best practice to log user off if an open session is left idle for a certain period of time. The default and maximum period of time is 5 hours.
- **Proxy policy** — Optionally, selected users can be allowed to proxy or act on behalf of other users and proxy rights can be configured to have expiration dates.

## Mail Domain and Firewall Configuration

Account administrators need to take the following steps to ensure that emails sent from OpenAir are delivered successfully and to allow communication between OpenAir and add-on service applications.

- Create a Sender Policy Framework (SPF) record to provide a list of servers that are authorized to send mail on behalf of your domain and include emails sent from OpenAir — SPF is a Simple Mail Transfer Protocol (SMTP) validation system that verifies the host names or IP addresses emails can originate from for a domain name. An SPF record is a TXT record using the SPF format with your DNS provider. An SMTP server on the receiving end determines (based on the content of the DNS TXT record) whether the nameserver / IP address the email message is sent from is approved for that domain. Setting up a DNS TXT record for SPF might be required by the email infrastructure or services (as presented by email domains) that you send email to. For more information, see the OpenAir SuiteAnswers article “OpenAir’s Sender Policy Framework (SPF) Record” (Answer ID: 18737).

**Note:** OpenAir email does not comply with DMARC alignment rules by default. Additional action may be required to ensure that OpenAir email pass either DKIM or SPF checks if you use DMARC for email authentication. Depending on your DMARC policy, OpenAir email may be marked as junk mail or not be delivered at all if both DKIM and SPF sets of checks fail. For more information, see [DMARC Alignment and OpenAir Email](#).

- Allow the relevant OpenAir domains in the firewall settings of the servers and machines running add-on services or accepting communication with OpenAir. For example, this may be needed to allow OpenAir Automatic Backup Service files to be transferred to your SCP/SFTP server, or to allow the secure transfer of data between your OpenAir account and the OpenAir Integration Manager application.

Ensure the following domains are allowed:

- openair.com
- outbound1.openair.com
- outbound2.openair.com
- relay.openair.com
- system.openair.com
- Your account specific domain name (\*.app.openair.com).

The URL for OpenAir services includes the domain name for your OpenAir account <account-domain>. For more information about your account-specific domain name, see the help topic [Your Account URLs](#).

**Important:** The use of OpenAir IP addresses to access or manage access to any OpenAir services is no longer supported. You should allow domains instead of IP addresses. The IP addresses of OpenAir services may change at any time without notice.

## DMARC Alignment and OpenAir Email

If you use DMARC for email authentication and your DMARC policy quarantines or rejects email that is not DMARC compliant, you can take the following actions to ensure that OpenAir email pass either DKIM or SPF checks. OpenAir email does not comply with DMARC alignment rules by default. If both DKIM and SPF sets of checks fail, email may be marked as junk mail or not be delivered at all.

- To pass DKIM authentication and alignment, you can contact OpenAir Customer Support to set up DKIM for OpenAir notifications. See [Setting Up DKIM for OpenAir Notifications](#).

**Note:** If DKIM authentication and alignment fail after DKIM is set up, contact OpenAir Customer Support for further investigation.

- To pass SPF authentication, you can add the OpenAir email relay server domain (relay.openair.com) to your SPF DNS record.
- To pass SPF alignment, you can use the Custom Email Return Path feature to set a custom return path for your account. Review the best practice guidelines before enabling this feature. See [Custom Email Return Path](#).

## What is DMARC?

DMARC is an open email authentication protocol that provides domain-level protection of the email channel. DMARC authentication detects and prevents email spoofing techniques used in phishing, business email compromise (BEC) and other email-based attacks. Building on existing standards – SPF



and DKIM –, DMARC is the first and only widely deployed technology that can make the header From domain trustworthy. The domain owner can publish a DMARC record in the Domain Name System (DNS) and create a policy to tell receivers what to do with email messages that fail authentication. It is a set of rules that when validated will ensure the email message received comes from a trusted source.

To pass DMARC alignment, email must pass either SPF alignment and authentication checks or DKIM alignment and authentication checks.

- SPF Authentication checks whether the sender server is allowed to send email for this domain (domain part of the email address in the Return-Path header).
- SPF Alignment checks whether the email message originates from whom the From header says it did. It does so by checking that the email addresses in the From and Return-Path headers have matching domains.
- DKIM Authentication checks whether the email message includes a valid DKIM signature certifying that the message body, attachments and other parts of the email message have not been modified.
- DKIM Alignment checks whether the key used for signing the email message is correct for the domain of the sender. It does so by checking that the domain part of the address in the From header matches the source domain found in the DKIM signature.

## Setting Up DKIM for OpenAir Notifications

DKIM provides email authentication, which can be used to give the recipient server confidence that an email came from a given address and was not tampered with in transit. When DKIM is set up, the OpenAir email relay adds a DKIM signature to outbound notification email. The receiving email server verifies the signature on the email using the DKIM public key, which it retrieves from your DNS records. If the signature is verified successfully, the email pass DKIM checks, which in turn contribute to the DMARC policy check.

This process uses an RSA public/private key pair generated for a given domain name and unique selector name. The selector identifies the DKIM record, that is the TXT record you create in your DNS settings to store the DKIM public key.

DKIM keys do not expire, but you may want to rotate the DKIM key for OpenAir notifications from time to time. To do so, follow the steps below to have a new RSA key pair generated with a new selector. You should keep the old DNS TXT record for a few days after implementing the change to give the DNS time to update.

### To set up DKIM for OpenAir notifications:

1. Contact OpenAir Customer Support and request to apply or change the DKIM signature to OpenAir notification email. Provide the information listed in the following table:

Name	Required / Optional	Description
Domain	Required	A fully qualified domain name (FQDN) is the complete address of the internet host or computer. It provides its exact location within the domain name system (DNS) by specifying the hostname, domain name and top-level domain. mail.example.com and example.com are examples of FQDN with the hostname mail, the domain name example and the top-level domain com.
Selector	Required	The unique name of your DKIM record. The DNS TXT record you create must be named <selector>._domainkey.<domain> where <domain> is the FQDN and <selector> is a unique name for the DKIM signature on this domain.  For example, openair._domainkey.example.com can be used to find DKIM public key information for OpenAir notification email sent from an example.com email address. It is specified as an attribute for a DKIM signature, and is recorded in the DKIM-Signature header field.

Name	Required / Optional	Description
Key length	Optional	If you require the DKIM key to be a specific length, specify the key length.

OpenAir Customer Support will arrange for an RSA public/private key pair to be generated and will provide you with the DKIM signature you need to add to your DNS record.

**Note:** You should let OpenAir generate the RSA public/private key pair. However, you can generate the RSA public/private key yourself and supply it to OpenAir Customer Support if required. If you prefer to generate and supply the DKIM private key, make sure you use all necessary precautions to keep the DKIM private key secret. Anyone with access to it can stamp tokens could pretend to be you.

2. Add the DKIM signature to a TXT record in your DNS record. Use the selector you provided to make up the name of your record following the format <selector>.\_domainkey.<domain>. Use the content supplied by OpenAir Customer Support for the content of the DNS TXT record, which includes the version, type and the public key among other information.

Example of DNS TXT record:

- Name: openair.\_domainkey.example.com
- Content:

```
1 v=DKIM1; h=sha256; k=rsa; s=email; p=ABCDEFGHIJKLMN0PQRSTWXYZ+abcdefghijklmnopqrstuvwxyz/1234567890+ABCDE
FGHIJKLMN0PQRSTWXYZ/abcdefghijklmnopqrstuvwxyz+1234567890/ABCDEFGHIJKLMN0PQRSTWXYZ+abcdefghijklmnopqrstu
vwxyz/1234567890+ABCDEFGHIJKLMN0PQRSTWXYZ/abcdefghijklmnopqrstuvwxyz+1234567890/ABCDEFGHIJKLMN0PQRSTWXYZ+abcde
fghijklmnopqrstuvwxyz/1234567890+ABCDEFGHIJKLMN0PQRSTWXYZ/abcdefghijklmnopqrstuvwxyz+1234567890/BCDEFGHIJKLMNO
```

3. Contact OpenAir Customer Support to confirm the creation of the DNS record.

OpenAir engineers will confirm after the DKIM signature is enabled for notification email from your OpenAir account.

4. Test the DKIM set up. OpenAir notification email should include a DKIM signature in the email headers. The DKIM signature should look like the following example:

```
1 smtp.mailfrom=example.com; dkim=pass (signature was verified)
2 header.d=example.com; dmarc=pass action=none header.from=example.com; compauth=pass
3 reason=100
```

**Note:** After DKIM is correctly set up, DKIM authentication fails if the message is changed during transit. If the bounce message includes the header information dkim=fail("body hash did not verify"), the message was modified. This may be the case if you use an email security gateway that is configured to remove email attachments and replaced them with a string, for example. Make sure that services in your email delivery infrastructure are not altering messages.

## Custom Email Return Path

You can specify a custom return path for email sent by OpenAir.

To do so, go to Administration > Global Settings > Display > Email Settings and enter the custom return path in the **Set up email return path** box. Review the best practice guidelines before using this feature. See [Custom Return Path Best Practice Guidelines](#).

By default, the Return-Path header (sometimes referred to as "envelope address") is set to `www@openair.com` by the OpenAir email relay server for all email messages originating from OpenAir. If you have a DMARC policy for your domain, this results in failing SPF alignment when the OpenAir

application sends an email message with a user email address in the From header. See [DMARC Alignment and OpenAir Email](#).

The Custom Email Return Path feature allows the Return-Path to be changed to a custom value when appropriate, depending on the scenario. If a custom return path is specified for your account and the custom return path domain matches the email header in the From domain, the OpenAir application sets the Return-Path header to this custom return path and tells the OpenAir email relay not to modify the Return-Path header.

The following table summarizes the three possible scenarios for OpenAir email when a custom return path is specified for the account. The example custom return path for all three scenarios is pm-bounces@pm-bounces.example.com.

Scenario	From header	Return-Path header	SPF Alignment	Notes
Email coming from user email address. From and custom return path email addresses have matching domains.	Account user email address. <b>Example:</b> marc.collins@example.com	Set to custom return path by the OpenAir application. <b>Example:</b> pm-bounces@pm-bounces.example.com	Pass	The email addresses in the From and Return-Path headers must have matching domains but may have different subdomains.  If a forward email address is specified for undeliverable OpenAir email in Administration > Global Settings > Display > Email Settings, it has no impact in this scenario.
Email coming from www@openair.com.	www@openair.com	Set by the OpenAir email relay server. www@openair.com	Pass	The custom Return-Path is not used.
Email coming from user email address. From domain matches neither the custom return path domain nor openair.com.	Account user email address <b>Example:</b> marc.collins@domain-mismatch.net	Set by the OpenAir email relay server. www@openair.com	Fail	The email addresses in the From and Return-Path headers must have matching domains.

## Custom Return Path Best Practice Guidelines

Review the following guidelines:

- You should specify an email address for undeliverable OpenAir email to be forwarded to. To do so, go to Administration > Global Settings > Display > Email Settings and enter the email address in the **Forward undeliverable email to this email address** box. See the help topic [Email Settings](#).
- You should set a custom return path as a preventive measure if you send notification email from OpenAir with a custom From header such as the user email address. However, setting a custom return path is necessary only if email messages sent from OpenAir fail to be delivered – when Mimecast blocks email delivery with error 550 Envelope Blocked, for example. It offers little benefit over forwarding undeliverable email to a specific address otherwise.


**Note:** Mimecast DMARC tool is the only known tool that checks SPF alignment. Generic mailing services, such as Microsoft Exchange, Gmail, or Yahoo, for example, omit SPF alignment checks by default. When email is sent to such mailboxes and a custom return path is specified for the account, all three scenarios pass.

- Bounce (undelivered) notification messages are sent to the address in the Return-Path header. If you specify a custom return path for your account:

- In some scenarios, the custom return path bypasses the forward address for undeliverable OpenAir email as OpenAir no longer receives the bounce email notification.
- You should set both the custom return path and the forward address for undeliverable OpenAir email (**Forward undeliverable email to this email address**) to the same email address.
- The custom return path you enter **must** correspond to a valid email inbox on your email servers.
- Setting a custom return path does not provide a complete solution unless the From email domain is the same for all email sent with custom From header from your account. The feature has little to no use if you send OpenAir email from a wide range of email domains – Email messages would pass SPF alignment checks only for those custom From email addresses with a domain matching the Return-Path email domain; all other email with a custom From email address would fail SPF alignment.

## Automatic Backup Service


The Automatic Backup Service (ABS) lets you set up a regular delivery of your account data to an email address or SCP/SFTP server for safeguarding. Your data is compressed as a ZIP file and can be PGP encrypted for additional security. You can use this feature to download all of your data, workspace documents and attachments.

 **Note:** The Automatic Backup Service is a licensed add-on and must be purchased separately. To enable the Automatic Backup Service feature, contact your OpenAir account manager or OpenAir Professional Services.

## Setting up the Automatic Backup Service

When the Automatic Backup Service (ABS) is enabled, go to Administration > Global Settings > Account > Automatic backup service and configure your backup settings.

- **Data to include in the backup** — Select which data will be exported in each backup. You can include the OpenAir data dictionary, text files (either comma- or tab-delimited) and MySQL import file. You can set the default CHARSET for your MySQL import files to "UTF-8", and include table relationships in the MySQL import file.

 **Note:** If the **Apply relationships** box is checked, the MySQL import file contains statements to support table relationships:

- Change the storage engine to "InnoDB".
  - Change foreign key columns to allow null values.
  - Set foreign keys to null if the value is 0 (zero).
- **Documents and attachments** — Check the **Document and attachments** box to include them in the backup.
    - By default, the filename of each attachment and workspace document is the system-generated internal ID for the attachment (document). You can append the original names and extensions to documents and attachments in addition to the internal ID.
    - You can use a **Date range filter** to include only documents and attachments created or updated during a specific period. Using a date range filter can be useful to manage the size of the backup file. The form indicates the total file size of selected documents before compression.

- **When do you want the backup to run** — schedule when you would like the backup to run. You can set the schedule to particular days of the week or month, or every day. You can also set the time for the backup to run. You should run the backup in the evening for better performance.
- **How do you want the data sent** — Select how the data should be sent. Options include SCP, SFTP or Email. Emails will not be sent if the files are larger than 60 MB. You can also suspend the service.



**Important:** Support for the FTPS protocol in the Automatic Backup Service stopped on January 20, 2021.

- **SCP/SFTP settings**

- **Address** — Enter the IP address or DNS name for your SCP or SFTP connection.
- **Directory** — Specify a directory to place the exported file in.
- **User name** — Enter the user name used for your SCP or SFTP connection.
- **Password** — Enter and verify the password for the SCP or SFTP service.
- **Status email** — Enter an email address for status emails to be sent to.
- **Status notification** — Select which events are included in status emails. You can include all events or errors only.
- **Disable remote file attribute copy** — Try to check this box if you receive setstat errors during the ABS transfer.
- **Try to resume transfer when it fails** — Check this box to try and resume the transfer in case the connection to the SFTP server is interrupted. This is only available if you choose to send your data using SFTP.

If the SFTP connection is interrupted, OpenAir will attempt to retry the scheduled automatic backup transfer twice. After the third unsuccessful attempt, an error is logged and a status notification email is sent to advise that the automatic backup was unsuccessful. The status notification email also indicates if the connection is interrupted but the automatic backup completes successfully on the second or third attempt.

- **Seconds between retry attempts** — Enter the time interval (in seconds) between ABS transfer attempts. The interval can be between 5 seconds (default) and 5 minutes.



**Note:** After you change the transfer method to SFTP, click **Save** to see the **Try to resume transfer when it fails** box and **Seconds between retry attempts** field.



**Important:** Support for custom remote ports for SCP or FTPS in the Automatic Backup Service stopped on January 20, 2021.

- **SSH Security Information** — After you set up the ABS and OpenAir connects with the SCP or SFTP server, OpenAir stores the SSH public keys for all hosts ABS connected to (**Known hosts**). To clear the list, check the **clear list** box.

 **Note:** To replace an existing SSH public key with a new one:

1. Check the **clear list** box.
2. Click **Save**.
3. Click the Tips button then **Test ABS connection settings**. If the connection test is successful, the new SSH public key is added to **Known hosts**.

- **PGP Encryption** — If you want to use PGP encryption, copy and paste the PGP public key in the text box.
- **Other**
  - **Include the audit trail in the text backup** — By default, text files do not include audit trails. Check this box to include the audit trail. This can make the text files difficult to parse. MySQL import files always include the audit trail.
  - **Include all tables in the text and MySQL backups** — By default, the export excludes some tables with typically large datasets such as `assign_by_day`, `booking_by_day`, `schedule_by_day`, and `user_tag_by_day` for example. Check this box to include all tables in text and MySQL backups.
  - **Include status file with backup** — Check this box to include a small status file with data about the transfer. The status file contains the checksum of transferred file(s), file size, and the list of all tables.
  - **Tables to exclude** — You can exclude tables from a MySQL import file here. Enter the list of tables to exclude, separated by commas.

# Security Features

This chapter outlines the security mechanisms OpenAir offers. It includes the following sections:

- [The Security Model](#)
- [Configuring and Using Authentication](#)
- [Configuring and Using Access Control](#)
- [Configuring and Using Auditing features](#)
- [Configuring and Using OpenAir Integrations and Add-on Services](#)
- [Enabling and Controlling Access to OpenAir Platform Tools](#)

## The Security Model

This section gives a high level overview of the threats that OpenAir is designed to counter and how the individual security features combine to protect your OpenAir data and environment against unauthorized access and use.

Security requirements arise from the need to protect data: first, from accidental loss and corruption, and second, from deliberate unauthorized attempts to access or alter that data. Secondary concerns include protecting against undue delays in accessing or using data, or even against interference to the point of denial of service.

The critical security features that provide these protections are:

- **Authentication** – ensures that only authorized individuals get access to OpenAir and data.
- **Authorization** – controls access to system privileges and data. Authorization builds on authentication to ensure that individuals only get access to the functionality and specific data that are appropriate for their jobs.
- **Audit** – allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control. It also enables accountability for user's actions affecting specific content and, as a result, deters users from taking inappropriate actions.

Access to OpenAir data, to the OpenAir user interface and add-on services is based on users, roles and permissions, and filter sets.

## Users

A user is an individual who has access to an OpenAir account.

- Generally, most users are employees, but third party consultants, partners, and customers can also be users.
- Users need to be set up in the OpenAir system through the creation of employee records. For users to have access to OpenAir, their records must include a user ID, and a password, and the user must be marked as active.
- Users can be granted access to specific applications within the OpenAir user interface as well as specific add-on services.

## Roles

A role is a defined access configuration that can be assigned to users — it controls access to functionality, primarily.

- Each role includes a set of associated permissions that determine the type of data users can see and the tasks they can perform. For example, roles determine whether a user will be able to view and/or create a project or view and/or create a booking.
- Form permissions can be used to restrict the form data users can view or modify according to their role.
- A user may only be assigned a single role.

## Filter sets


A filter set is a defined access configuration that can be assigned to users — it controls the data set users have access to.

- Each filter set includes a set of associated permissions that determine the data set users can see. For example, filter sets may determine whether a user will be able to access all projects or only the projects they are booked for or assigned to.
- A user must be assigned at least one filter set, their primary filter set.
- A user may be assigned multiple filter sets.
- Filter set overrides can be set for each of the application the user has access to. This enables to give the user access to a different data set depending on the application they are currently using.

## OpenAir Account Access


When a new OpenAir account is deployed, customers must designate at least one employee who will have responsibility for administering the account. The administrator has full privileges to all aspects of OpenAir and usually is the person who sets up account access by assigning roles to users.

- The first step for setting up account access is to set up roles. See [Roles Overview](#).
  - Two roles are predefined. The Administrator role cannot be modified and grants all access privileges.
  - You can create roles to suit your business requirements. See [Typical Custom Roles](#).
  - OpenAir provides reports for managing roles and other access privileges such as filter sets and approvals. See [Privileges Overview](#).
- The next step is to set up filter sets. See [Filter Sets Overview](#) and [Filters Hierarchy Overview](#).
  - Two filter sets are predefined. The All access filter set cannot be modified and grants access to all data.
  - You can create filter sets to suit your business requirements.
  - You may create hierarchies to group employees, customers and projects under a hierarchical classification tree, e.g. geographical location. You can then create filter sets to grant users access to projects according to the hierarchy.
 

See the  [Administrator Guide](#) under Administration - Global Settings > Organization > Hierarchy.
- After roles and filter sets have been set up, users can be given access and assigned roles and filter sets.
  - Create employee records for your users and either:
    - Give them a temporary password and enforce password change on first sign-in.
    - Enable an alternative sign-on method for users to access OpenAir.


See [Configuring and Using Authentication](#).



- Remove access to OpenAir if a user is not an active employee. See [User Access Removal](#).
- Grant the relevant user privileges in the Employee Demographic form. See [Application Options Overview](#).
- Grant access permission to the relevant OpenAir application and add-on services. See [Access Control Overview](#).
- Assign users a role and a primary filter set. Set up any filter set overrides for the different module as appropriate. See [Filters Hierarchy Overview](#).
- OpenAir provides a report enabling you to monitor users' sign-in activity. See [User Access Log](#).
- You can define form permissions to further restrict what data users can view and/or modify according to their role. See [Form Permissions](#).
- Consider the security implications and where relevant, grant access selectively to the OpenAir integration and add-on services or to the OpenAir platform tools. See [Configuring and Using OpenAir Integrations and Add-on Services](#) and [Enabling and Controlling Access to OpenAir Platform Tools](#).
- Form scripts could also be used to implement custom rules determining user restrictions and privileges for specific processes and establish segregation of duties. See the  [User Scripting](#) for information about User Scripting features.

## Internal Controls for OpenAir Access

To achieve effective internal controls, you will need a combination of both automated and manual controls that both prevent and detect misstatements or misappropriation of assets. Companies have several responsibilities for establishing good general controls for OpenAir applications.

- Ensure logical access and application security. Users should have only the information that they need to do their jobs.
- Segregate duties.
- Ensure that your organization has user administration controls in place, including:
  - Process for requesting and approving access. If possible, the request, approval, and granting of access should be segregated among different individuals to ensure appropriate application of the process.
  - Access should be reviewed periodically for changes in responsibilities, assurance that terminated employees have had their access revoked, assurance that sensitive/critical access permissions are granted to the appropriate individuals and to them only.
  - Process access termination in a timely manner.
- Maintain a mapping of role assignment to job function, and map role assignment to job title.
- Periodically audit the permissions that make up each role to ensure they are appropriate.
- The administrator role is very powerful, and access to this role should be extremely limited. Ideally your organization should have at least one administrator and one back-up administrator.
- Audit configuration options, changes to data, record deletions, web services and script deployment logs either periodically or as and when required. See [Configuring and Using Auditing features](#).
- User scripts could also be used to trigger notifications based on certain criteria or user action. See the  [User Scripting](#) for information about User Scripting features.


## Configuring and Using Authentication

OpenAir can authenticate users internally, by using information stored in the OpenAir database. OpenAir also supports external authentication methods: an external Identity provider can be used to manage

authentication using the Security Assertion Markup Language (SAML) protocol, SAML can also be used to integrate with Active Directory, or the NetSuite Single Sign-On feature can be used to access applications in OpenAir from within NetSuite. OpenAir uses the Transport Layer Security (TLS) protocol to ensure the security of network authentication — all passwords are encrypted during transmission.

The following authentication mechanisms may be configured and used for your OpenAir account.

- [Authentication by OpenAir](#)
- [SAML Authentication](#)
- [NetSuite Single Sign-On](#)
- [OAuth 2.0 Token Based Authentication](#)

 **Note:** OpenAir stopped supporting Secure Lightweight Directory Access Protocol (LDAPS) service for authentication with the OpenAir 2020.1 release in April 2020. The **Active Directory integration** optional feature allowing to use Active Directory user authentication with Secure Lightweight Directory Access Protocol (LDAPS) can no longer be enabled. You can use your existing LDAPS service with a SAML 2.0 service instead.

## Authentication by OpenAir

OpenAir can authenticate users attempting to connect to the application, by using information stored in the OpenAir database itself. This is the default authentication mechanism for new accounts. Each user must be given a user name with an associated password as well as the Company ID for the OpenAir account. The user must provide this company ID, user name and password when attempting to access or connect to the application. This process prevents unauthorized use of the application, because the access or connection will be denied if the user provides an incorrect password. OpenAir stores user passwords in a hashed format and applies restrictions to prevent unauthorized alteration. Users can change their own passwords at any time.

OpenAir authentication includes the following features:

- [Password Encryption](#)
- [Minimum Password Policy Requirements](#)
- [Password Options](#)
- [Two-Factor Authentication](#)
- [Employee Lockout](#)
- [Session Timeout](#)
- [IP Restriction](#)

## Password Encryption

Passwords are always automatically and transparently encrypted during network (client/server and server/server) connections before sending them across the network. This protection is always enforced, by default.

## Minimum Password Policy Requirements

OpenAir enforces the following minimum policy requirements:

- **Password History** — Users cannot reuse the last two passwords in their password history.

- **Password Complexity Verification** — Complexity verification checks that each password is complex enough to provide reasonable protection against intruders who try to break into the system by guessing passwords.
  - Minimum length of 8 characters.
  - Must contain at least 3 of the following types of characters: uppercase letters , lowercase letters, numbers, or [special characters](#).
  - Not equal to user ID.
- **Password Lifetime and Expiration** — The maximum lifetime of a password is three months, after which they expire and must be changed on the next successful logging.
- **Verify password before change** — Users must enter their current password correctly when attempting to change their password. This also applies when users are prompted to change password when their password has expired or does not meet the password policy requirements. Any failed attempt at changing password counts toward the number of failed sign-in attempts allowed before locking the user account.

## Password Options

Password policy options can be configured for the account.

To obtain information about password policy options currently set for your account, to increase the strength of your current password policy, or to enable any of the optional password features, contact OpenAir Customer Support.

Passwords created by account administrators for new users or users who have never signed in must respect the password policies for your OpenAir account. In addition, an option on the Employee Demographic form allows account administrators to force users to change their passwords the next time they sign in.

The password policy for your account is subject to minimum requirements. See [Minimum Password Policy Requirements](#).

The following password options can be configured:

- **Password Lifetime and Expiration** — A lifetime can be specified for passwords, after which they expire and must be changed on the next successful logging.
- **Password Expiration Notifications** — An expiration notification email is sent automatically 14 days before the password expires, and 3 days before the password expires, unless the password is changed in the meantime. Notices include the date the password will expire and instructions for changing your OpenAir password.
- **Password History** — The password history option checks each newly specified password to ensure that a password is not reused for a specified number of password changes. The specified number of password changes must be at least 2.
- **Password Complexity Verification** — The minimum password length can be changed. The minimum password length must be at least 8 characters.
- **Password Validation Against Known Compromised Passwords** — When this optional feature is enabled for your account, OpenAir validates new passwords against a list of compromised passwords and will require users to enter a different password if the new password is on a regularly updated list of known compromised passwords. This validation does not apply to temporary passwords set by administrators.
- **Password Expiration Rule Exception** — Enables account administrators to override the password lifetime and expiration rule for individual users. OpenAir will not enforce the password expiration rule for the user if the option "**Do not enforce password expiration rule for this user**" is checked on the Employee Demographic form.

**Important:** Passwords created or updated using the API, NetSuite integration and other integrations must respect the password policies for your OpenAir account.

## Two-Factor Authentication

Add more security to OpenAir with an extra verification step during sign-in.

Two-factor authentication (2FA) adds a second level of security when you sign in to the OpenAir user interface. To sign in using 2FA, you must first enter your OpenAir user credentials (company ID, user ID and password) and then enter a time-based verification code generated by an authenticator app for each sign-in.

**Note:** Currently, OpenAir supports only time-based verification code from an authenticator app as second factor.

The authenticator app must comply with the OATH TOTP standard. OATH stands for the Initiative for Open Authentication. TOTP stands for time-based one-time password.

To enable 2FA for your account, go to Administration > Global Settings > Account > Security, check the **Two-factor authentication** box, and click **Save**.


After you enable 2FA for your account:

- Account administrators can control 2FA settings for the OpenAir account and enroll users to sign in using 2FA. See [Managing two-factor authentication in OpenAir](#).
- Enrolled users must setup 2FA within a set number of days or sign-ins. For more information, see the help topic [Signing In Using Two-Factor Authentication \(2FA\)](#).

## Managing two-factor authentication in OpenAir

After you enable 2FA for your company's OpenAir account, you can:


- Control 2FA settings. To do so, go to Administration > Global Settings > Account > Two-factor authentication.
  - When you enroll a user to sign-in using 2FA, this user can skip the 2FA setup for a limited number of days and sign-ins. You can control the number of **Days until 2FA setup is required** and the number of **Sign-ins until 2FA setup is required**.
  - Check the **Trust devices** box to allow users to add the device they sign in from as a trusted device. This will let the same user sign in to OpenAir on the same device without being asked to enter a verification code every time. Each device is trusted for a limited number of days, after which it is removed automatically from the list of trusted devices for your company's OpenAir account. You can specify the number of **Days until a trusted device is removed**. A user's trusted devices are removed automatically when the user changes password.

 **Important:** Clearing the **Trust devices** box removes all trusted devices for all users.

- [Enroll or disenroll users to sign in using 2FA](#).
- Add the following columns to the employees list for auditing purposes:
  - **2FA required** – The column indicates whether a user is enrolled to sign in using 2FA (Required), not enrolled (Not required), or accessing OpenAir using single sign-on (empty value).
  - **2FA status** – The column indicates whether a user has completed the 2FA setup (Setup), not completed it yet (Required), or is not enrolled to sign in using 2FA (empty value).
  - **Complete 2FA setup by** – The column shows the deadline when the user must set up 2FA by.
- Reset two-factor authentication or remove trusted devices for one user from Administration > Global Settings > Users > Employees > [Select an employee] > Two-factor authentication.

When you reset 2FA settings for a user, OpenAir sends an email notification automatically to inform the user.

- Disable 2FA temporarily for your account. To disable 2FA, go to Administration > Global Settings > Account > Security, clear the **Enable two-factor authentication** box, and click **Save**.

 **Note:** Disabling 2FA temporarily for your account does not remove 2FA setup-related information for users. After you enable 2FA again, users will not need to set up 2FA again.

### Enroll or disenroll users to sign in using 2FA

Use the following steps to enroll or disenroll users to sign in to your company's OpenAir account using 2FA.

When you disenroll a user, all 2FA setup-related information for this user is removed. If you enroll that same user again, the user will need to setup 2FA again and will be able to skip 2FA setup up to the number of times and days specified in the two-factor authentication settings for your company's account.

### To enroll or disenroll users to sign in using 2FA:

1. In OpenAir, go to Administration > Global Settings > Users > Employees > [Select an employee] > Demographic.
2. Check the **Two-factor authentication required** box to enroll the user. Clear the box to disenroll the user.
3. Click **Save**.  
After you enroll a user, the demographic form shows "User must complete 2FA setup by <date>" under the **Two-factor authentication required** box.  
OpenAir sends an email notification automatically to inform the enrolled user of the requirement to setup 2FA.
4. Repeat for each user you want to enroll to sign in using 2FA.

**Note:** Two-factor authentication is not available for users accessing OpenAir using single sign-on. Saving the form returns an error if both the **Two-factor authentication required** and `saml_auth` boxes are checked.

You can use the bulk employee change wizard to copy the value of the **Two-factor authentication required** box to other user records in your company's OpenAir account. See the help topic [Making Changes to Multiple Employee Records at the Same Time](#).

You can use the XML API and SOAP API, or the Integration Manager to modify the value of the **Two-factor authentication required** [`mfa_status`] box for multiple users.

## Employee Lockout

Employee lockout is a security feature that ensures employees have an active account and have knowledge of the password to access OpenAir.

**Important:** OpenAir Customer Support cannot act as an administrator for company specific data-related items such as unlocking employee accounts or resetting passwords. As an account administrator, you perform these tasks for your company.

Account administrators can control the following Employee lockout options. To do so, go to Administration > Global Settings > Account > Security, and use the instructions for each of the following setting on the Security form.

- **Failed logins to allow before locking employee** — Select a value from the dropdown list. This is the number of times an employee can attempt to sign in using an incorrect password.


**Note:** Locked employees see the same on-screen error message on the OpenAir sign-in page whether the employee credentials are invalid or the employee is locked out of OpenAir.

By default, OpenAir sends a lockout notification email to the employee when the employee exceeds the number of sign-in attempts permitted.


Lockout notification email can be disabled for your account. To stop OpenAir sending lockout notification email to employees being locked, contact OpenAir Customer Support.

- **Send employee lockout notifications to this email address** — Enter an email address. When a user reaches the maximum number of sign-in attempts and is locked out, an email notification is sent

automatically to the address supplied in this field. The email includes the name of the employee so account administrators within your company can follow the appropriate password reset procedure. Typically, administrators unlock the user account and send an email notification to the employee or reset their password and notify them verbally or by email. OpenAir Customer Support is not allowed to unlock employees — you should include the email address of one of the administrators for your company's OpenAir account.


 **Note:** You can specify multiple email addresses separated by semi-colons. However, depending on how long your email addresses are within your company, you may be able to enter only one to three. A better option would be to set up an email distribution list and use this in the notification field. Then your distribution list can be expanded as your list of contact employees grows or modified as your organization changes.

- **Employee log in support email address** — Enter an email address or the alias for an email distribution list. Typically, this should include the email address for your company's Help Desk. If an email address is specified, OpenAir Customer Support will direct employees to the email address provided in this field for any access issue such as unlocking employee accounts or resetting passwords.

 **Tip:** Create an email distribution list if you have more than one office location or department using OpenAir. Appoint ownership of various general employees to specific employees on this distribution list or allow a primary and backup support structure within your environment.

Users have the following recourse if they forget their password or need help with unlocking their user account:

- Users can click the **Forgot your password or ID?** link on the OpenAir sign-in page and enter the email address associated with their user account. If the email address supplied is associated with an active OpenAir employee record, OpenAir sends an email to that address containing the Company ID, the User ID as well as the password hint entered by the user when setting their password. For more information, see the help topic [Signing In Using Your OpenAir Sign-In Details](#).
- Users may contact any of their account administrators to request a password reset or to obtain help with unlocking their account. Account administrators can then set a temporary password from the Demographic settings form on the employee record. See the help topic [Demographic](#).

 **Note:** Administrators who need help with resetting their password or unlocking their user account should obtain help from other account administrators, or contact OpenAir Customer Support if there is only one administrator for the OpenAir account.

- If the Password Security Questions optional feature is enabled for your account, users can click the **Reset password or unlock account** link on the OpenAir sign-in page and regain access to OpenAir by answering a security challenge.

To enable the Password Security Questions feature, contact OpenAir Customer Support.

**Note:** Review the following guidelines:

- If the Password Security Questions feature is not enabled and a user attempts to regain access to OpenAir using this method, an error message appears. To specify a custom error message, go to Administration > Global Settings > Account > Security. and enter the custom message in the **Custom error message for password questions** box. You can use this custom message to provide the user some information about opening a ticket with your company's internal help desk, for example.
- If you require answers to the security questions to have a minimum lengths, contact OpenAir Customer Support and request to change the minimum number of characters each answer must contain to a specific value.
- System emails are disabled by default on sandbox accounts. The **Forgot your password or ID?** and **Reset password or unlock account** links can therefore only be used for production accounts.

For more information about the Password Security Questions feature, see the help topics [Password Security Questions](#), [Setting Up Security Questions](#) and [Resetting Your OpenAir Password](#).

## Session Timeout

The session timeout features requires users to re-enter either their passwords or their full credentials after a given period without user interaction.

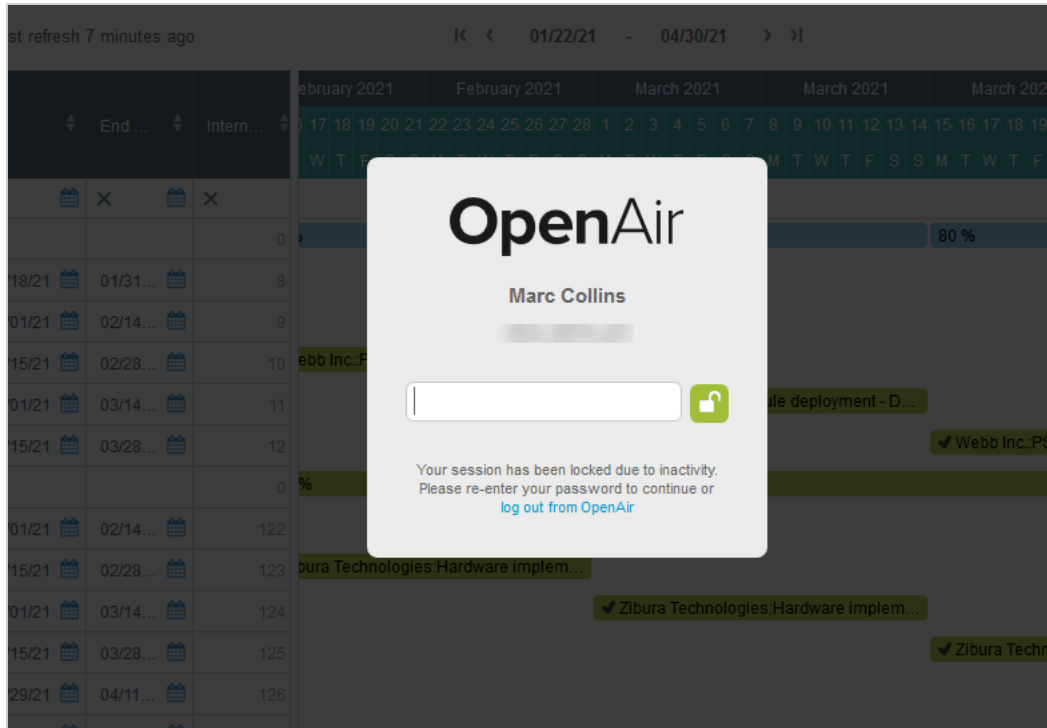
Account administrators can set the **Session timeout** and **Redirect user's page after timeout** periods in Administration > Global Settings > Account > Security Options:

- **Session timeout:** This option controls the time a session may be inactive before the employee is automatically locked out and prompted to re-enter their password. Session timeout avoids OpenAir sessions from being used by others on a shared machine. Session timeouts should be set according to the data security policies your company has in place. The default and maximum period for the session timeout is 5 hours.

**Note:** You may have different categories of OpenAir users in your company, such as power users who use OpenAir all the time, and time and expenses users who use OpenAir one time a week or less. You should select a session timeout value that does not inhibit power users. This is generally a 30 minute to 1 hour window.

- **Redirect user's page after timeout:** This option controls the time a session may be locked out before the user is automatically signed out and redirected. The user will be redirected either to the OpenAir sign-in page or to the alternate URL configured in Administration > Global Settings > Account > Integration: SAML Single Sign-On, if this feature is enabled on your account. This option can be set to "On timeout" or to a finite period up to a maximum of 6 hours. It should be set according to the data security policies your company has in place.






## IP Restriction

An optional feature can be used to restrict access to the OpenAir account to specific IP addresses. This includes access to your OpenAir account using the OpenAir UI, OpenAir API, or any client application utilizing the API to exchange information with your OpenAir account.

This optional feature lets you store authorized IP addresses on the employee record for each user. You can allow single IP addresses or network ranges, using an explicit range or subnet mask. The IP Restriction feature may be used to ensure users can only access your OpenAir account if they are connected to your company's physical network or VPN, for example.

You can extend the IP Restriction feature to check for IP address changes with every API request. In this case, if the IP address of the authenticated user's device changes and the new IP address is not in the IP address allowlist for this user, API requests return an error, and client applications utilizing the API can no longer exchange information with your OpenAir account.

 **Note:** Client applications utilizing OpenAir API include:

- OpenAir Mobile.
- Other add-on services supplied by OpenAir (Integration Manager, Exchange Integration Manager, Projects Connector, Outlook Connector, OffLine).
- Any bespoke integration utilizing the REST API, SOAP API, or XML API.

If the IP address of the authenticated user's device changes and the new IP address is not in the IP address allowlist for this user, the user can continue using the OpenAir UI normally until the user signs out or the session times out. This is true whether the user is accessing the OpenAir UI as a standalone application, or within NetSuite using the Single Sign-On integration feature.

Contact OpenAir Customer Support to enable the IP Restriction feature or the IP Restriction Check for IP Change feature extension.


After the feature is enabled, you will need to create a custom field **login\_ip\_address** associated with the **Employee** record to store the authorized IP addresses for individual users.


### To restrict access to specific IP addresses for an employee:

1. Create a text area custom field for Employee records. See the help topic [Creating and Modifying Custom Fields](#).

Use the following details:

- **Add a custom field to:** Employee
  - **Type of field to add:** Text area
  - **Field name:** login\_ip\_address
  - **Display name:** Authorized IP Addresses (you can use any appropriate display name )
2. Go to Administration > Global Settings > Employee > [Select an Employee] > Demographic.
  3. Locate the **Authorized IP Addresses** custom field. If you used a different display name for the custom field, locate the display name on the form.
  4. Enter one or more IP address(es) separated by commas in the text field. The following address descriptions are accepted:
    - A single IP address — Example: 209.202.151.4
    - A network range using a netmask — Example: 209.202.151.0/24
    - An explicit network range — Example: 209.202.151.4 - 209.202.151.10
  5. Click **Save**.

 **Tip:** You can use the bulk employee change wizard to copy the value of the login\_ip\_address field to other user records in your OpenAir account.


See  [Administrator Guide](#) under Home > Home > Wizards > Making Changes to Multiple Employee Records at the Same Time.

## SAML Authentication

Companies wishing to use an external Identity provider to manage authentication to OpenAir can validate User IDs using the Security Assertion Markup Language (SAML) protocol. This interface allows users to

log in once to a single site account, and access OpenAir services without the need to provide credentials again. It provides a method of secure integration with existing, on-site authentication infrastructures without exposing these services to direct public access, and enables federation of user identity across any number of additional services.

Contact OpenAir Customer Support to enable Single Sign-on using SAML 2.0 Authentication for your account.

 [OpenAir SAML 2.0 Quick Start Guide](#) describes the steps required to set up and deploy SAML Single Sign-on on your OpenAir account. The guide includes deployment best practice guidelines and instructions for configuring OpenAir as a Service Provider with your Identity Provider solution.

## NetSuite Single Sign-On

If you are using the OpenAir <> NetSuite integration, you can use the OpenAir Within NetSuite (NetSuite Single Sign-On Integration) feature and enable your users to access OpenAir from within NetSuite. With the NetSuite Single Sign-On Integration feature, you can:

- Deploy Suitelet scripts that bring OpenAir applications into NetSuite under a PSA Center tab.
- Use a Portlet on the Dashboard to perform OpenAir functions.
- Use a Subtab to launch OpenAir applications from within the NetSuite application.


Contact OpenAir Customer Support to request information about the OpenAir/NetSuite integration. After the feature is enabled, you can enable NetSuite Single Sign-on integration for individual users by checking the **Allow NetSuite Single Sign-On** box on the Employee Demographic form in OpenAir.


Refer to  [NetSuite Integration](#) for information about configuring and using the OpenAir <> NetSuite integration.

## OAuth 2.0 Token Based Authentication

OpenAir supports OAuth 2.0, a robust authorization framework. This authorization framework enables client applications to use a token to access OpenAir through the XML API, SOAP API, or REST API. The application accesses the protected resources on behalf of a user who gave an explicit permission for the access. This method eliminates the need for API integrations to store user credentials.

This feature is available if API Access is enabled for your account. It includes the following elements:

- **Administrators** can register up to 20 integration applications with OpenAir and enable or disable these applications in the Administration module. For more information, see [Managing API Integration Applications](#).
- **Administrators** can use web services reports to audit and revoke authorizations granted by OpenAir users to integration applications. For more information, see [Auditing and Managing OAuth 2.0 Authorizations](#) under  [Security](#).
- **Application Developers** can use the OAuth 2.0 authorization code flow to get an access token then use the access token to access your OpenAir data using the API. For more information, see the help topic [OAuth 2.0 for Integration Applications Developers](#) (Help topic under API).

 **Note:** OpenAir only supports the OAuth 2.0 authorization code grant type.

- **End-users** can give applications explicit permission to access OpenAir on their behalf and they can revoke this permission at any time. For more information, see [Authorizing Applications to Access OpenAir on Your Behalf](#).



**Note:** The first time a registered application attempts to access OpenAir on their behalf, users must sign in using the same trusted sign-in page they normally use to sign in to OpenAir then give the application explicit permission. The OAuth 2.0 feature supports the following user authentication mechanisms:

- Password authentication by OpenAir — Users enter their Company ID, User ID and Password on the OpenAir sign-in page.
- SAML authentication:
  - Service Provider initiated Single Sign-on — Users enter their sign-in details on your company Single Sign-on form.
  - Identity Provider initiated Single Sign-on — Users must sign in using their Identity Provider Single Sign-on form before the application attempts to access OpenAir on their behalf. When the application attempts to access OpenAir, the authorization page appears automatically. Users do not need to enter their sign-in details again if the Single Sign-on session has not expired.

## Managing API Integration Applications

Integration applications using OAuth 2.0 to obtain access to your OpenAir data must be registered and enabled by an account administrator. To register and manage your integration applications, go to Administration > Global Settings > Account > API Integration Applications.

**Note:** API Access must be enabled in your account to connect tools and services to OpenAir using the API. The Business Intelligence (BI) Connector feature must be enabled in your account to connect tools and services to your published reports using the REST API. The API Integration Application page is not available unless API Access or BI Connector is enabled. To enable API Access or BI Connector in your account, contact OpenAir Customer Support or your OpenAir account manager.

1. All your registered applications are listed in a grid. Details include the name of the application and the date and time when it was last updated.
2. To register a new application, click **ADD NEW APP**. This button is disabled if you reach the limit of 20 registered applications. See [Adding a New Application](#).
3. To enable or disable an application, click **ENABLE** or **DISABLE** in the top right corner of the corresponding box. See [Enabling, Disabling, or Removing Registered Applications](#)
4. To edit an application configuration, click the edit icon  in the bottom right corner of the corresponding box. See [Application Configuration](#).
5. To remove an application configuration from the list of registered applications, click the delete icon  in the bottom right corner of the corresponding box. See [Enabling, Disabling, or Removing Registered Applications](#).
6. To select one or more applications, check the box next to each application you want to select. You can only select multiple applications if they are either all enabled, or all disabled. You can then enable, disable or remove the selected applications. See [Enabling, Disabling, or Removing Registered Applications](#).

**Note:** All times are given as Eastern Standard Time (EST).

Global Settings **API Integration Applications**

## API Integration Applications 2 [ADD NEW APP](#)

Applications can help you connect tools and services to OpenAir using OpenAir APIs. Applications can be built by OpenAir, by third parties or by your own team.

Use this screen to add, enable or disable applications and manage their configuration. You can have a maximum of 20 applications.

Employees will be able to use an application if all the following conditions are met:

- The application must be enabled
- The employee must have the relevant permission
- The employee must allow the application to access your OpenAir data

If you disable an application, all employee authorizations related to this application will be deleted. Your employees will not be able to use the application.

**Your applications** 1 DISABLE ENABLE REMOVE

<input type="checkbox"/>	<b>C</b>	<b>CRM Integration</b> <span>3</span> <span>DISABLE</span>	Updated (EST): 2020-03-20 04:19:15
<input type="checkbox"/>	<b>E</b>	<b>Example Application</b> <span>3</span> <span>ENABLE</span>	Updated (EST): 2020-03-20 05:29:16
<input type="checkbox"/>	<b>O</b>	<b>OAuth2 Connector ...</b> <span>5</span> <span>ENABLE</span>	Updated (EST): 2020-09-12 18:23:28
<input type="checkbox"/>	<b>S</b>	<b>Some New Integration</b> <span>6</span> <span>DISABLE</span>	Updated (EST): 2020-09-12 18:23:00

4 [Edit configuration](#)

## Adding a New Application

You can register up to 20 applications. Each application needs a Client ID and Client Secret to obtain access to OpenAir using OAuth 2.0. The Client ID and Client Secret are generated by OpenAir as part of the registration process and are unique to each application.

**Important:** The Client Secret is a **private** key the application uses to request an authorization code from OpenAir. It should not be shared or stored in public code repositories.

The Client Secret is displayed only one time. You will not be able to retrieve it after you close the Application Credentials dialog.

If you misplace the Client Secret, you can edit the application configuration and generate a new Client Secret for the application.

**To register a new application with OpenAir:**

- Do one of the following:
  - Go to Administration > Global settings > Account > API Integration Applications, and click **ADD NEW APP**.
  - From any page in OpenAir, click the Create button and click API integration application.

The Add New Application popup window appears.

- Enter the following information:
  - Application name** (Required) — Enter a display name for your application in OpenAir. The name must be unique to the application. You will not be able to use a name already used by another registered application.
  - Description** — Enter a few sentences to tell your employees what the application and how it will help them. Your employees will use this information to decide whether they allow this application to access OpenAir on their behalf.
  - Redirect URI** (Required) — Enter a link users should be redirected to after granting or denying the application permission to access OpenAir on their behalf.

**Important:** Client applications use the redirect URI when requesting access to OpenAir. Ensure you enter the redirect URI supplied by the application developers.

**Add New Application**

APPLICATION NAME \*  
**Example Application** CLEAR 19/255  
 Choose a name for this application. This name will appear in the application lists and relevant dialogs in OpenAir.

DESCRIPTION  
 This app was created to demonstrate the new OAuth 2.0 support features in OpenAir. A description is not required but it is good practice to tell your end-users what the application does. You have up to 600 characters to do so. CLEAR 226/600  
 Provide a few sentences to tell your employees what this application does and how it will help them. Your employees will use this information to decide whether they allow this application to access OpenAir on their behalf.

REDIRECT URI \*  
**https://example-app.com/redirect** CLEAR 32  
 Provide a link employees should be redirected to after granting or denying the application permission to access OpenAir on their behalf.

CANCEL SAVE

- Click **Save**. The Application Credentials popup window appears.
- Copy the **Client Secret** and store it in a safe place. The Client Secret is displayed only one time. You will not be able to retrieve it after you close this window.

### Application Credentials

The application will need the following credentials to gain access to OpenAir Web API using OAuth 2.0. The Client ID and Client Secret are generated by OpenAir and are unique to each application.

CLIENT ID COPY TO CLIPBOARD

174\_h1FiXfWsJtLJG0DG

CLIENT SECRET COPY TO CLIPBOARD

vcFTaNE3nUXRuJ29jhEIXSH7LpXwbxTGdmJHoQMvo\_jz4vldOPITFJ-ZFToYR2G6gnl0dqXeeiFUloKnRGSfQ

- The client secret should not be shared or stored in public code repositories.
- The client secret is displayed only once. You will not be able to retrieve it after you close this window. You can generate a new client secret at any time.

Copy the client secret and store it in a safe place.  
To close this window, check the box to confirm you have stored the client secret in a safe place and click Close.

I have stored the client secret in a safe place
 CLOSE

5. Check the box to confirm you have copied and stored the Client Secret in a safe place then Click **Close**.

## Enabling, Disabling, or Removing Registered Applications

You must enable an application to allow this application to obtain access to OpenAir using OAuth 2.0.


You can disable an application to prevent this application from obtaining access to OpenAir using OAuth 2.0. If you disable an application, OpenAir automatically revokes all permissions given by users for the application to access OpenAir on their behalf. Employees will not be able to use the disabled application.

You can remove a disabled application from the list of registered applications. All permissions, authorizations and application credentials associated with the application configuration will be deleted. This action cannot be undone.

### To enable or disable a registered application:

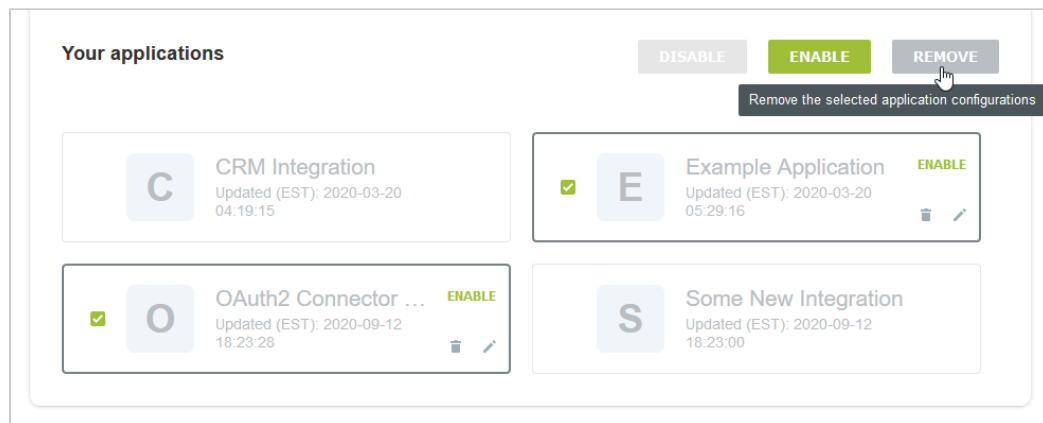
1. Go to Administration > Global settings > Account > API Integration Applications.
2. Click **ENABLE** or **DISABLE** in the top right corner of the corresponding box. A confirmation popup window appears.
3. Click **ENABLE** or **DISABLE** to enable or disable the application. Click **Cancel** to cancel the operation and return to the API Integration Applications page.

### To remove a registered application:

1. Go to Administration > Global settings > Account > API Integration Applications.
2. Click the delete icon  in the bottom right corner of the corresponding box. A confirmation popup window appears.
3. Click **REMOVE** to remove the application. Click **Cancel** to cancel the operation and return to the API Integration Applications page.

### To enable, disable, or remove multiple applications at the same time:


1. Go to Administration > Global settings > Account > API Integration Applications.
2. Check the box for each application you want to enable, disable, or remove. Notice that you can only select multiple applications if they are either all enabled, or all disabled. After you select the first application, the application that are not available for selection appear in light gray color. Notice also that some of the buttons in the top right corner of the list of registered applications become available and change from light gray color to dark gray or green.




3. Click **ENABLE**, **DISABLE**, or **REMOVE** to perform the corresponding action on all selected applications. A confirmation popup window appears. Click **ENABLE**, **DISABLE**, or **REMOVE** to confirm. Click **Cancel** to cancel the operation and return to the API Integration Applications page.

## Application Configuration

You can view the configuration details of your registered applications, including their unique Client ID from the Application Configuration form. You can change the application name, description or Redirect URI or generate a new Client Secret for the application.

To open the Application Configuration page for a registered application, go to Administration > Global Settings > Account > API Integration Applications and click the edit icon  in the bottom right corner of the corresponding box.

1. The **General** section of the form lists the main application detail:
  - You can change the **Application name**, **Description** and **Redirect URI**.

 **Important:** Client applications use the redirect URI when requesting access to OpenAir. Ensure you enter the redirect URI supplied by the application developers. If you need to change the redirect URI, disable the application, change the redirect URI and enable the application again.

- You can view when the application was registered under **Created**.



**Note:** All times are given as Eastern Standard Time (EST).

2. You can view the **Client ID** — the unique identifier a client application needs to send to OpenAir along with a client secret as part of the OAuth 2.0 authorization code flow.
3. Use the **Tokens Lifetime** section to configure the validity period of the access and refresh tokens:
  - **Access token lifetime** — Select the expiration time of access tokens. Available values go from 5 to 60 minutes in 5-minute increments. The default access token lifetime is 15 minutes.

**Note:** The validity period of access tokens cannot be greater than the session timeout set for your account. If the **Access token lifetime** value is greater than the session timeout value, the session timeout value is used for the access token validity period. The application configuration form shows the current values for the session timeout and access token validity period for reference.

To change the session timeout value, go to Administration > Global settings > Account > Security.

- **Refresh token lifetime** — Select the expiration time of refresh tokens. Available values go from 1 to 31 days in one-day increments. The default access token lifetime is 1 day.

**Note:** Before the OpenAir 2021.2 release, you could set the refresh token lifetime to values from 1 to 24 hours in one-hour increments. Values for the refresh token lifetime set before the OpenAir 2021.2 release show in days (decimal values) instead of hours

As part of the OAuth 2.0 authorization code flow, authorized applications need to exchange an authorization code for an access token and refresh token to obtain access to OpenAir. The access token has a short expiration time. When the access token expires, the client application can use the refresh token to obtain a new access token without user interaction until the refresh token expires or the authorization is revoked.

**Note:** Access tokens normally remain valid for their entire lifetime. However, the access token becomes invalid before it is due to expire if any of the OpenAir business rules have changed and the access token is refreshed. Business rule changes may include any changes to your company's OpenAir account configuration, or to the access privileges or role permissions of the employee who authorized the client application.

Each refresh token can be used one time only. Refresh in an access token generates a new access token and a new refresh token.

4. To generate a new Client Secret, click **Regenerate Secret** — You may need to generate a new client secret if you misplace or delete the client secret accidentally or if your client secret becomes compromised.

The new client secret will be valid immediately. The old client secret will continue to be valid for 24 hours after you generate a new one. This allows time to update any enabled application with the new client secret.

5. If you made any changes to the configuration details in the General section, the **Save** button is enabled. Click **Save** to save changes and return to the API Integration Applications page or click **Cancel** to close the configuration form without saving.

API Integration Applications

CANCEL
SAVE
5

## Example Application

**General** 1

APPLICATION NAME \*  
Example Application
CLEAR  
13/255

CREATED (EST)  
2020-03-06 12:03:40

Choose a name for this application. This name will appear in the application lists and relevant dialogs in OpenAir.

DESCRIPTION

This app was created to demonstrate the new OAuth 2.0 support features in OpenAir. A description is not required but it is good practice to tell your end-users what the application

CLEAR 228/600

CLIENT ID  
147\_64j8bj8YMB7wL9 2

Provide a few sentences to tell your employees what this application does and how it will help them. Your employees will use this information to decide whether they allow this application to access OpenAir on their behalf.

REDIRECT URI \*  
https://example-app.com/redirect
CLEAR  
32

Provide a link employees should be redirected to after granting or denying the application permission to access OpenAir on their behalf.

---

**Tokens Lifetime** 3

After the employee authenticates successfully and authorizes access, the application receives an Access tokens and a Refresh token. Access tokens have a short expiration time. When the Access token expires, the application can use the Refresh token to obtain a new Access token without employee interaction until the Refresh token expires or the authorization is revoked.

ACCESS TOKEN LIFETIME  
45 minutes

Select the validity period of the Access token in minutes.

i The validity period of access tokens cannot be greater than the session timeout set for your account. If the access token lifetime value is greater than the session timeout value, the session timeout value is used for the access token validity period.

The current session timeout value is: 30 minutes  
The current access token validity period is: 30 minutes

To change the session timeout value, go to Administration > Global settings > Account > Security.

REFRESH TOKEN LIFETIME  
31 days

Select the validity period of the Refresh token in days.

---

**Client Secret**

You can generate a new Client Secret at any time by clicking **Regenerate Secret**. Copy the new Client Secret and store it in a safe place. It should not be shared or stored in public code repositories. This Client Secret is displayed only once. You will not be able to retrieve it after you close this window.

REGENERATE SECRET
4

Last generated (EST): 2020-03-06 12:03:40

## Authorizing Applications to Access OpenAir on Your Behalf

Integration applications let you connect OpenAir with other applications and they extend what you can do with OpenAir. Integration applications may use the OAuth 2.0 authorization protocol to gain access to your company's OpenAir account.

The first time an application using the OAuth 2.0 protocol attempts to access OpenAir on your behalf, you will need to give this application your explicit permission.

To authorize an application, you will typically use the following steps:

1. The application opens a browser and directs you to the same trusted sign-in page you normally use to sign in to OpenAir — the OpenAir sign-in page or your company Single Sign-on form appears.
2. Enter your sign-in details and click **Log in**.

An authorization page will appear indicating that the application <application name> would like to access your OpenAir data.

3. Read the content of the authorization page attentively. It should describe what the application does and how it will help you. It should also say what the application can do, for example:
  - The application will be able to access all data you have access to.
  - The application will be able to perform all actions permitted by your role and user privileges.



**Important: For Administrators** — Business rules configured for your company's OpenAir account are applied when an integration application interacts with your OpenAir data through the REST API. However, they are not applied when an integration application interacts with your OpenAir data through the SOAP API or XML API — application developers must enforce business rules within their integration application if required. Business rules include OpenAir account configuration settings and access control mechanisms, as well as any user scripts deployed on your company's OpenAir account.

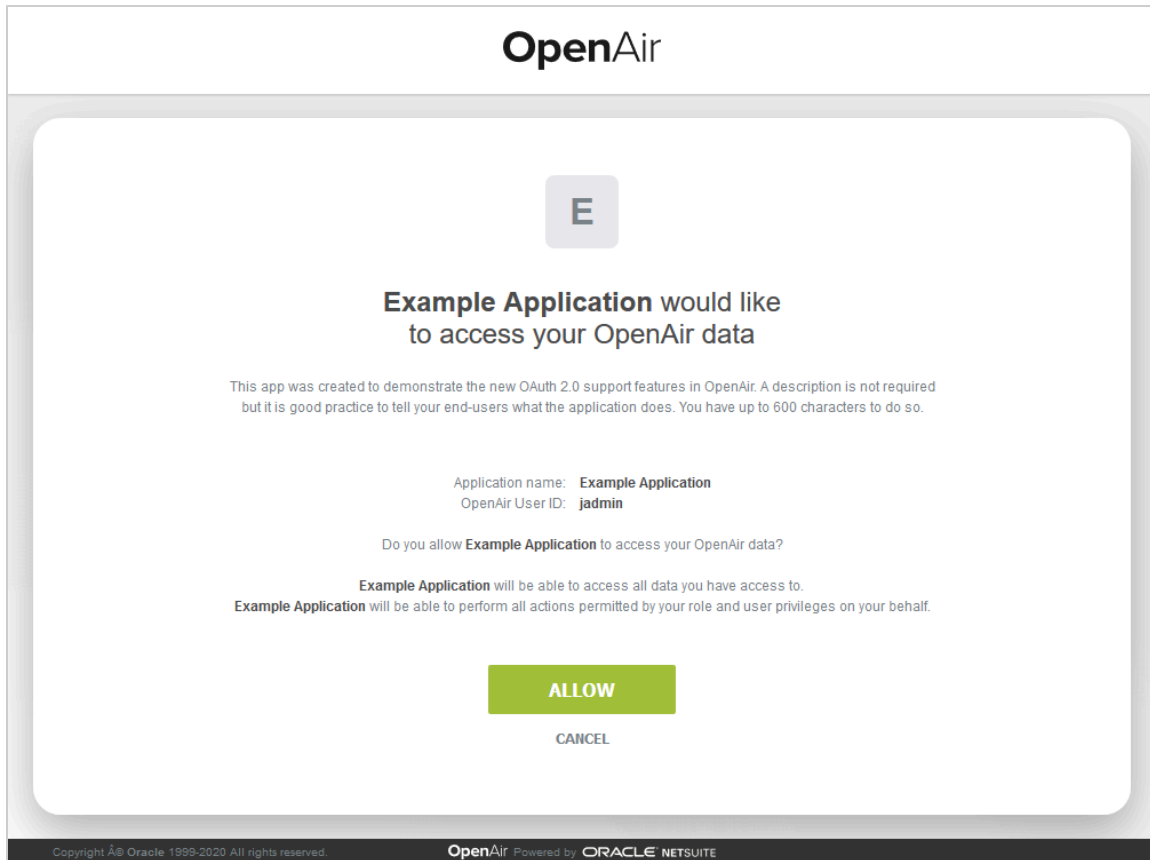
4. Click **ALLOW** to authorize the application or click **CANCEL** if you do not want the application to access OpenAir on your behalf.



**Note:** The steps may vary depending on the method you use to sign in to OpenAir:

- If you normally enter your company ID, user ID and password on the OpenAir sign-in page, or if you enter your company ID on the OpenAir sign-in page and then your password on your company single sign-on page, the above steps apply.
- If you normally need to enter all sign-in details on your company single sign-on page to access OpenAir without going to the OpenAir sign-in page first (Identity Provider initiated Single Sign-on), you must sign in and launch OpenAir before the application attempts to access OpenAir on your behalf. The authorization page appears automatically. Follow steps 3 and 4 above. You do not need to re-enter your sign-in details.

Integration applications are registered and managed by your account administrator. They need to be enabled on your account before they can attempt to connect to OpenAir and request your permission.



**Note:** Integration applications are registered and managed by your account administrator. They need to be enabled on your company's OpenAir account before they can attempt to connect to OpenAir and request your permission.

Account administrators can disable an application at any time.

- If you have authorized an application and this application is disabled by an administrator, the application will no longer be able to interact with OpenAir.
- If an administrator enables this application again, you will need to give this application your explicit permission again before you can continue to work with it in connection with OpenAir.

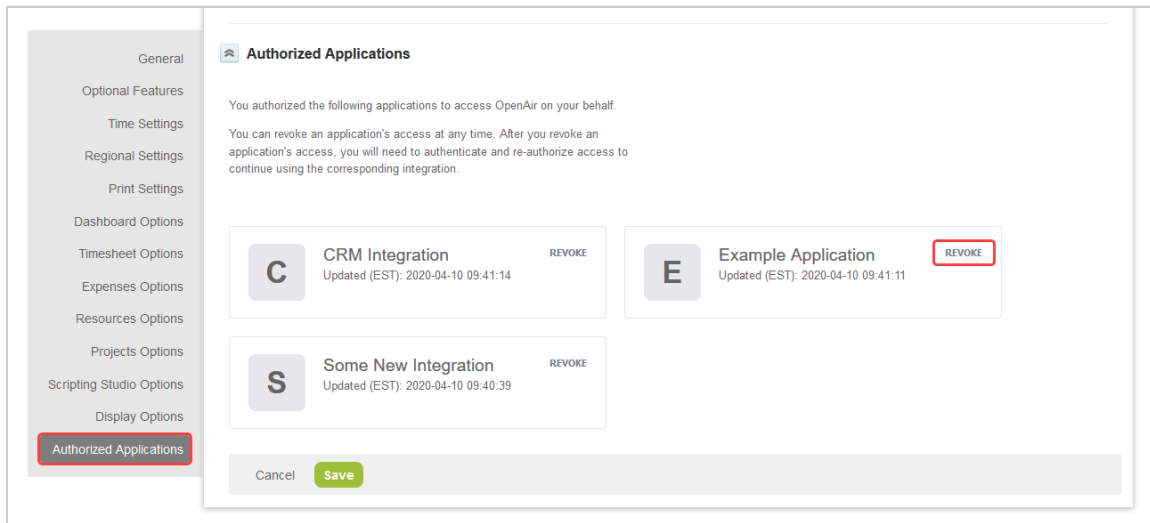
After you authorize an application, it will be able to interact with OpenAir on your behalf until you revoke the authorization.

To view the application you have authorized, go to User Menu > Personal Settings > Authorized Applications. All your authorized applications are listed in a grid. Details include the name of the application and the date and time when it was last updated.

**Note:** All times are given as Eastern Standard Time (EST).

To revoke an application, click **REVOKE** in the top right corner of the corresponding box, then click **REVOKE** in the confirmation message. The application no longer shows in the authorized applications

list. If a revoked application attempts to access OpenAir on your behalf, you will be prompted to give this application your explicit permission again.



## Configuring and Using Access Control

OpenAir provides a Role Based Access Control (RBAC) model to set up authorization policies for users. These policies control the functionality available to users and can be set up by customers to enforce separation of duties.

Authorization includes primarily two processes:

- Permitting only certain users to access, process, alter data or perform certain actions such as approval and data export.
- Applying varying limitations on user access or actions.

Account administrators can create an unlimited number of roles and assign roles to users.

This section introduces the basic concepts and mechanisms for placing or removing such limitations on users, individually or in groups. The following levels of permission are discussed:

- **Roles** — Managing and controlling user privileges is made easier by using roles, which are named groups of related privileges that you grant as a group to users. See [Roles Overview](#).
- **Filter Sets** — Filter sets define what data the employee has permission to view or update. Roles and Filter Sets may overlay to provide a feature/data matrix of capabilities for the employee. See [Filter Sets Overview](#).
- **Form Permissions** — Form Permissions can be used to control specific field level access on forms for each role. See [Form Permissions](#).
- **User Settings** — All users must be assigned one and only one role and at least one filter set. Privileges and access rights can also be set for users on an individual basis. See [Employee Access Control Settings](#).
- **Guest Roles and Guests** — Guests are customers who are able to sign in to OpenAir and view the application data that is associated with them. See [Guest Roles and Guests](#).

## Roles Overview

Roles define what an employee can do in your company's OpenAir account. The role setup designates what rights and privileges are available to employees with a specific role. This includes what applications

the employee can access as well as whether they can view, modify, or create various records. For example, you may create a Project Manager role which lets project managers modify projects but does not allow them to change the project stage.

Employees are assigned the default role when created. An employee must have a role assigned to them and can be assigned to only one role. You can change the employee's role at any time in the Employee Demographic form.

You can create or edit and grant or revoke rights and privileges for general and application-based entities and items. There are separate sections for General Settings, My Account, Workspaces, Opportunities, Resources, Projects, Timesheets, Expenses, Purchases, Invoices, Integration, Proxy restrictions, and Scripting. See [Role Permissions](#).

You can also create Guest roles to give customers a restricted access to OpenAir and enable to view only relevant project information. See [Guest Roles and Guests](#)

The screenshot shows the Oracle NetSuite interface for 'Global Settings - Users'. The table lists predefined roles with their default settings and assigned users.

Role	Default new user role	Full access role	Assigned users
- All -	- All -	- All -	
Finance			2
Guest Role			1
Operations			2
Project manager			3
Resource manager			2
System Administrator		✓	2
User	✓		17

## Predefined Roles

There are two predefined Roles within the application:

- **Administrator role** — cannot be modified. The Administrator's primary OpenAir usage is maintaining your account configuration, adjusting for company needs, data audits, report creation, release management, process enforcement, and general administration.
- **Employee role** — can be modified as needed. Typically, the Employee role has few rights and privileges.

## Typical Custom Roles

Here are some examples of typical roles that you may want to create:

**Employee (default)** — Primary OpenAir usage is time and expense entry. There is no edit or create capability on any other object.

**Project manager** — Primary OpenAir usage is budget and schedule management of projects. This may include project creation, financial review (no create-edit access to financial data), and resource management permissions (submit booking requests, create bookings, etc.).

**Finance** — Primary OpenAir usage is invoicing and billing-revenue financial management of projects. It also may include project setup and customer setup.

**Human Resources** — Primary OpenAir usage is employee maintenance as well as vacation and sick time (HR benefits) reporting. Typically, employees with this role can also create and edit employees as well as view all timesheets and expense reports.

**Project Administrator** — Primary OpenAir usage is project setup, including billing and recognition rules, and customer creation. This role does not usually have invoicing capability or the ability to create or edit financial information regarding billing and revenue.

**Resource Manager** — Primary OpenAir usage is for resource bookings and the management of resource schedules. This may also include project and task assignments within the Projects application.

**Super User** — Primary OpenAir usage is managing localized account configuration items such as invoice layouts, employee maintenance, and company calendars. This role has limited impact to global account configuration changes, although shares some account administration responsibilities.

### To create a new role:

1. Go to Administration > Global Settings > Users > Roles.
2. Click the **Create Button** and select **New Role**. The New Role form appears.
3. Enter the Role name.
4. Check the **Make this the default role for new and imported employees** box to assign this role to all new and imported employees by default.
5. Check the boxes for all permissions you want to grant employees with this role. The role form contains sections covering the permissions for the different functional areas and applications in OpenAir. See [Role Permissions](#).

### To edit an existing role:


1. Go to Administration > Global Settings > Users > Roles.
2. Click the role you want to edit. The Edit Role form appears.
3. Check the **Make this the default role for new and imported employees** box to assign this role to all new and imported employees by default.
4. Check the boxes for all permissions you want to grant employees with this role. The role form contains sections covering the permissions for the different functional areas and applications in OpenAir. See [Role Permissions](#).

### To assign a role to an employee:

1. Go to Administration > Global Settings > Users > Employees.
2. Click on the Employee ID for the employee whose role you want to change. The Employee Demographic form opens.
3. Click on the **Role** dropdown at the top of the form, next to the Employee ID, and select the employee's role.
4. Click **Save**.



**Tip:** You can use the bulk employee change wizard to copy the Role to other user records in your company's OpenAir account.

See  [Administrator Guide](#) under Home > Home > Wizards > Making Changes to Multiple Employee Records at the Same Time.

## Role Permissions

The role form contains sections covering the permissions for the functional areas and applications in OpenAir.

## Roles – General Settings

The General Settings section lets you specify general role permissions. For example: View Customers, View and modify Customers, and View and Modify Customers (except name). In this example, by selecting View and Modify Customers, View Customers is included and does NOT need to be checked. You can select the check boxes to turn options **on** or **off** based on the role requirements.

Most of the following options include either simply View or View and modify: Customers, Customer locations, Prospects, Contacts, Projects, Employees, Generic employees, Departments, Attribute sets, Roles, Services, Service 1 lines, Payroll types, Expense items, Vehicles, Approval processes, Vendors, Employee costs, Loaded costs, Generic employee costs, Employee job codes, Generic resource job codes, Filter sets, Custom time ranges, Account-wide reports, Employee login detail report, Auto-billing rules, Hierarchies, Tax locations, Job codes, Rate cards, Cost centers, External IDs, Snap shots, Calendars for others, Audit trails, Internal IDs, Dashboard graphs, Email templates, Calculated fields, Built in summary fields, Tag groups, Target utilization, Download lists, Download reports.

Also within the General Settings section are the following role options:

- **View and modify existing employees** — lets employees with this role view and update existing employees. This is useful for roles that may need to modify employees but who should not have the ability to create new employees.
- **See billing rates and budget amounts** — This is useful for project managers or others so that they are aware of project financial information.
- **Customize forms and Customize lists** — Customize forms option permits employees to modify certain forms within the application such as Receipts or the Timesheet. You, as the account administrator, are generally the employee who customizes forms, although some companies also use a super employee account. Customize lists permits employees to change the order and selection of fields in the list (for example, Projects or Employees).
- **Restrict data viewed on reports** — Share saved reports with other employees, Specify report usage designations, and Specify report filter sets.
- **Download lists and reports into Microsoft Excel or PDF files** — Download lists and Download reports.
- **Employee Unlock** — Allow employees to unlock the account of other employees who have failed the security requirements set for your company's OpenAir account. Many companies restrict this option to you, the account administrator, and to a backup employee for times when you are unavailable.
- **View and modify all list views** — Enables users to access and manage all list layouts in an account from the Administration module or from within lists. This role permission is available only if the Custom List Layouts feature is enabled for your account. To enable this feature contact OpenAir Customer Support.
- **Change owner on list views** — Enables users to change the owner for list layouts they have access to. This role permission is available only if the Custom List Layouts feature is enabled for your account. To enable this feature contact OpenAir Customer Support.

## Roles – My Account

Options in the My Account section relate to Administration > Global Settings. You can select the check boxes to turn options **on** or **off** based on the role requirements. You should not grant most of these options to roles other than the account administrator role.

The View and Modify options include: Dashboard, Company demographics, Company schedules, Company logos, Company settings, Terminology, Custom fields, Currency rates, Base currencies, My charges, Automated back-up service, Company status on dashboard, and Employee status on dashboard.

Also within the My Account section are the following role options:



- **Exchange information** — Import Customers from outside sources as well as Export data to other applications including Microsoft Excel.
- **Use of the following wizards** — Bulk employee change wizard, Expense report attachment wizard, American Express receipt import wizard, and Bulk task change wizard. The wizards allow you to make bulk changes to certain aspects of related records. For example, if you were going to change the department across a large set of employees, you would use the Bulk employee change wizard.
- **Administration** — Perform company maintenance functions and Create own proxies.

## Roles – Expenses

Options in the Expenses section relate to the Expenses application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Expense report alerts, Payment types, Expense reports, expense report layout, expense grid, reports, authorizations, and expense report reimbursements.

Also within the Expenses section are the following role options:


- **Create charges from approved expense reports** — This option permits charges to be created after an expense report has been approved. You must have enabled the following internal switch: Automatically bill expense items assigned to a customer when an Expense report is approved. To enable this internal switch, [Creating a Support Case](#).
- **Book approved authorizations** — This option permits employees to book (that is, create a financial transaction) for the item when the authorization is approved.
- **Allow employee to delete (individually or in bulk) open, submitted or rejected envelopes** — This option permits employees to delete any open, submitted or rejected expense reports either individually or in bulk. This features requires the following internal switch to be enabled: Administrators can delete employees envelope. To enable this internal switch, [Creating a Support Case](#).

## Roles – Timesheets

Options in the Timesheets section relate to the Timesheet application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Time types, Timesheet alerts, Ceridian payroll integration, Approved timesheets, Archived timesheets, Time off requests, Timebills from approved timesheets, Timesheet layout and rules, Reports, Adjust approved timesheets, Leave accrual transactions, Accrual rules, Run leave accrual, and View the time entry tab.

Also within the Timesheets section are the following role options:

- **Create charges from approved timesheets** — This option permits charges to be created after a timesheet has been approved. You must have enabled the following internal switch: Automatically bill time assigned to a customer when a timesheet is approved. To enable this internal switch, [Creating a Support Case](#).

 **Note:** Most customers use Billing Rules to generate charges. If you use Billing Rules, this role permission is not applicable.

- **Run leave accrual** — This option permits employees to run the leave accrual and update leave balances. You should restrict access to this option to account administrators and run leave accrual at a specified day and time.
- **Allow employee to delete (individually or in bulk) open, submitted or rejected timesheets** — This option permits employees to delete any open, submitted or rejected timesheets either individually

or in bulk. This feature requires the following internal switch to be enabled: Administrators can delete employees timesheets. To enable this internal switch, [Creating a Support Case](#).

## Roles – Projects

Options in the Projects section relate to the Projects application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Dashboards, Project locations, Tasks and Phases, Task types, Gantt chart layout, Reports, Project analysis, Project overview, Recognition rules, Transfers, Task cost and Billing projections, Project stages, Assignment groups, Project pricing, Baselines, Booking grid, Project alerts, Issues, Issue statuses, Issue severities, Issue sources, Issue stages, Budgets, and Unlock projects (locked by OpenAir Projects Connector).

Also within the Projects section are the following role options:

- Hide the profitability section in the project overview.
- Create and modify project billing rules and Run project billing. You should restrict access to these options to roles of employees who control the financial aspects of projects.
- Change the project stage of a project. This option can be useful when the employee who manages a project is not the one to change the stage of the project.
- Enable the advanced booking worksheet functionality.

## Roles – Workspaces

The options in the Workspace section relate to the Workspace application. You can select the check boxes to turn options **on** or **off** based on the role requirements. The options include: create, view, and modify workspaces, view account storage usage, view and modify document categories; copy, move and download documents; view reports; and view and modify workspace alerts.

## Roles – Invoices

Options in the Invoices section relate to the Invoices application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Charges, Invoices, Invoice payments, Invoice layouts, Reports, Charge stages, Agreements, and Customer POs, and Change the customer PO of a charge.

Also within the Invoices section are the following role options:

- **Change the charge stage of a charge** — This option permits employees to change the charge stage of a previously created charge (timebill). You should restrict this option to those personnel with billing responsibilities.
- **Change the agreement of a charge and Change the customer PO of a charge** — This option permits employees to adjust the agreement or customer PO on a charge. You should restrict this option to those personnel with billing responsibilities.

## Roles – Resources

Options in the Resources section relate to the Resources application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Skills, Booking types, Industries, Job roles, Locations, Education, Custom profiles (1-35), Profiles, Bookings, Booking grid, Booking requests, Deal booking requests, Customer engagement

history, Reports, Resource options, Optional resource detail in Custom search and quick search, and Resource alerts.

Also within the Resources section are the following role options:

- **Enable profile worksheet** — This option permits employees to modify a profile. When enabled, a **Worksheet** link displays in the Resources application for any resource that the employee has access to through their Filter Sets.
- **Create bookings** and **Customize the form used to create multiple bookings** — These options allow employees to schedule a resource on a project. You should restrict this option to those in a resource or project management function within your company to avoid resource scheduling conflicts. OpenAir lets you book multiple resources at the same time as well as customize this form to meet your needs.
- **Create booking requests** and **Create deal booking requests** — These options allow employees to request resource bookings for projects or on deals in the Opportunities application is available.
- **Customize the Custom Search form** — This option permits employees to customize the Custom Search form to include or exclude skills, education, custom profiles in the custom search. See the help topics [Search - Resources Application](#) and [Custom Search](#).

## Roles – Purchases

Options in the Purchases section relate to the Purchases application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Manufacturers, Purchasers, Carriers, Accounts payable locations, Receiving locations, Products, Shipping terms, Payment terms, Purchase requests, POs, Quick PO items, Fulfillments, PO layout, Reports, Reduce purchase item quantity payable, and F.O.B. locations.

Also within the Purchases section are the following role options:

- **Create POs** — This option permits employees to create purchase orders directly without having to submit a purchase order request.
- **Create and modify non-PO purchase items** — This option permits an employee to create or modify purchase items that have not been previously identified as products on purchase orders.
- **Create fulfillments** — This option permits employees to record fulfillments against purchase orders.
- **Can reduce purchase item quantity payable** — This option permits employees to adjust the quantity to be paid on a PO.

## Roles – Opportunities

Options in the Opportunities section relate to the Opportunities application. You can select the check boxes to turn options **on** or **off** based on the role requirements. Most of the following options include either simply View or View and modify: Create, view, and modify Deals; Estimates; Proposals; To Dos; Events; Territories; Employee locations; Business types; Customer sources; Customer sizes; Templates; Proposal layout; Reports; and Deal stages.

Also within the Opportunities section are the following role options:

- **Assignments** — Assign to dos to all employees, Assign events to all employees, and Assign deals to all employees
- **Create charges from accepted proposals** — This option permits employees to convert charges to time entries when a customer or prospect has accepted the proposal. If this is a Prospect, the prospect must be converted to a customer for the charges to be billable.

- Change the deal stage of a deal

## Roles – Proxy Restrictions

Options in the Proxy Restrictions relate to proxy permissions. You can select the check boxes to turn options **on** or **off** based on the role requirements. Proxy permissions allow an employee to proxy or, in other words, log-in as another employee and perform actions as that employee. OpenAir can distinguish between a direct sign-in and a sign-in done by proxy. In addition, OpenAir can distinguish the actions performed directly within a particular account and one done by a proxy.

Proxy restrictions under the **Roles settings** restrict what a proxied-in employee can do. Examples of proxy restrictions include: A proxy employee cannot approve timesheets, A proxy employee cannot approve their own timesheets, A proxy employee cannot approve booking requests, or A proxy employee cannot approve invoices.

## Roles - Integration

Options in the Integration section relate to the QuickBooks integration functionality in the OpenAir Integration Manager, which is no longer supported.



**Important:** As announced in the October 8, 2022 OpenAir Release Notes and through Proactive Feature Change Notification (PFCN), support for the QuickBooks integration functionality in OpenAir Integration Manager ended with the OpenAir 2023.1 Release on April 15, 2023. Previous versions of OpenAir Integration Manager, including any shortcuts created using Integration Manager 6.6 or earlier version, can no longer be used to exchange information between OpenAir and QuickBooks.

There are a variety of integrations with OpenAir. Employees can download some of them from the OpenAir UI under Add-on services. As an account administrator, you provide an employee with Exchange Access. See [Employee Access Control Settings](#).

Other integrations are enabled through an internal switch. You may need to discuss integration availability with your OpenAir account manager or OpenAir Professional Services. As an account administrator, when an integration is enabled, you generally provide employees access to it. You may want to speak with OpenAir Professional Services to understand other integration options and how to implement them in your company's account. See the help topic [Account](#).

## Filter Sets Overview

Filter sets define what data the employee has permission to view or update. The following entities are identified within the filter sets: Customers, Projects, Services, Employees, Expense Items, Charge stages, and Project stages. Roles and Filter Sets may overlay to provide a feature/data matrix of capabilities for the employee. By setting up appropriate Filter Sets, an administrator can provide multiple roles with access to the same record but can customize what users can see or do in those records.

Two filter sets are predefined for new accounts:

- All access — allows access to all data in your company's OpenAir account
- Booked/Assigned — the default configuration of this filter set limits Employees access to the authenticated user only, and limits Project access to either Projects that are owned by the user or Projects that the user has been booked or assigned to.

**Filter sets**

New filter set

Cancel Save

Filter set name \*

Notes

Make this the default filter set for new and imported users

Duplicate access control settings from this filter set

Select...

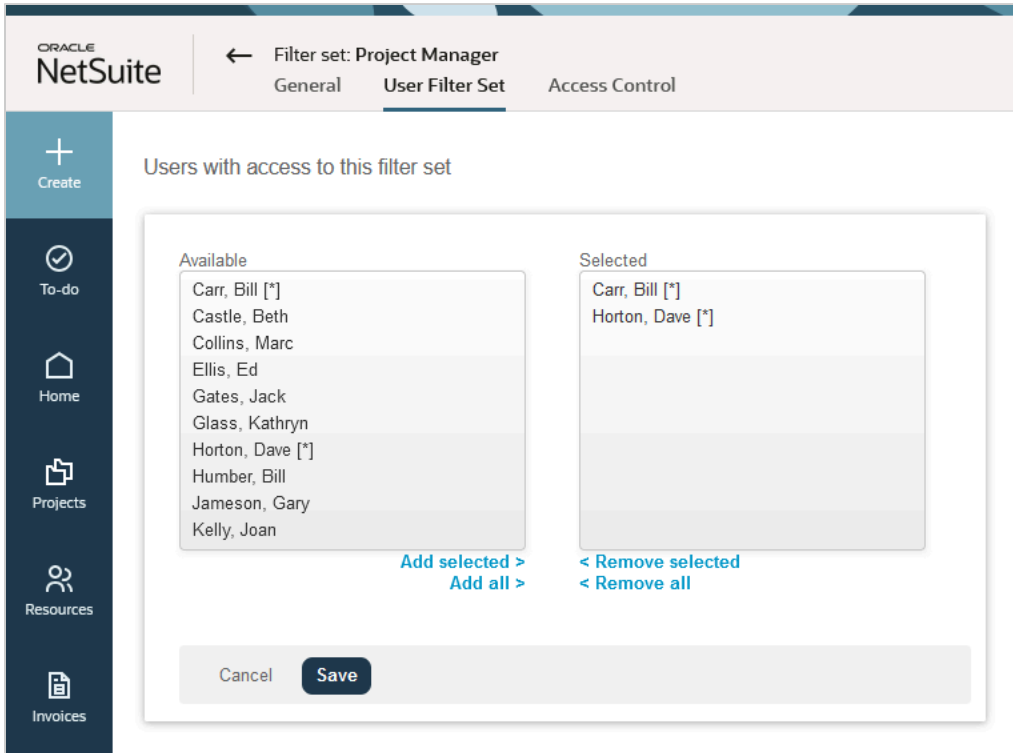
Cancel Save

### To create filter sets:

1. Go to Administration > Global Settings > Users > Filter Sets.
2. Click the Create button and select **New Filter set**. The New Filter Set form appears.
3. Enter the filter set name, Notes and check the Make this the default filter set for new and imported employees (if applicable).
4. Click Save.
5. After the filter set has been created and saved, additional options become available on the form, including the following links:
  - **General** — the Name and Notes about the filter set.
  - **Employee filter set** — identifies who has this filter set assigned to them in the filter set link of the employee record. See [Employee Filter Set](#).
  - **Access Control**— identifies what types of data employees with this filter set can view. See [Filter Set Access Control](#).

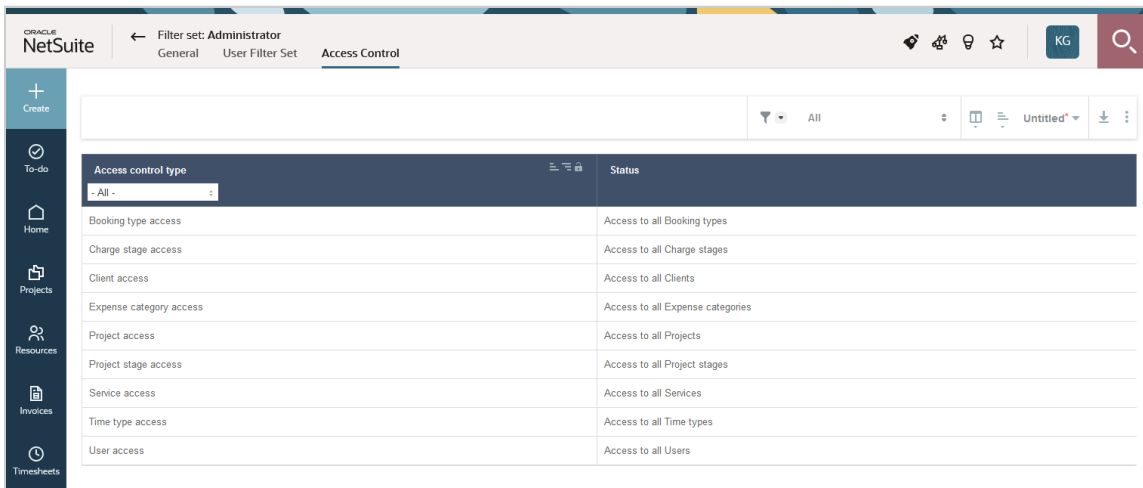
## Employee Filter Set

After the filter set has been created, you can choose which employees will have this filter set available to be added to their employee record. It is added to the Filter sets link within the employee record. Employees with an asterisk (\*) after their name cannot be removed from the assignment as this is their primary and only filter set. Employees must have at least one filter set assigned to their employee record. Employees with more than one filter set can switch filter sets to view different types of data.



## Filter Set Access Control

Access Control defines the level of access that is granted to the assigned employees. Access Control can be set for the following entities: Customers, Projects, Project stages, Services, Employees, Expense Items, Charge stages, and Booking types. The filter sets provide the access relationship of those entities to a specific employee through discrete selections or with a meta value relationship description. For example, employees may have access to Project XYZ or to all projects they directly own.



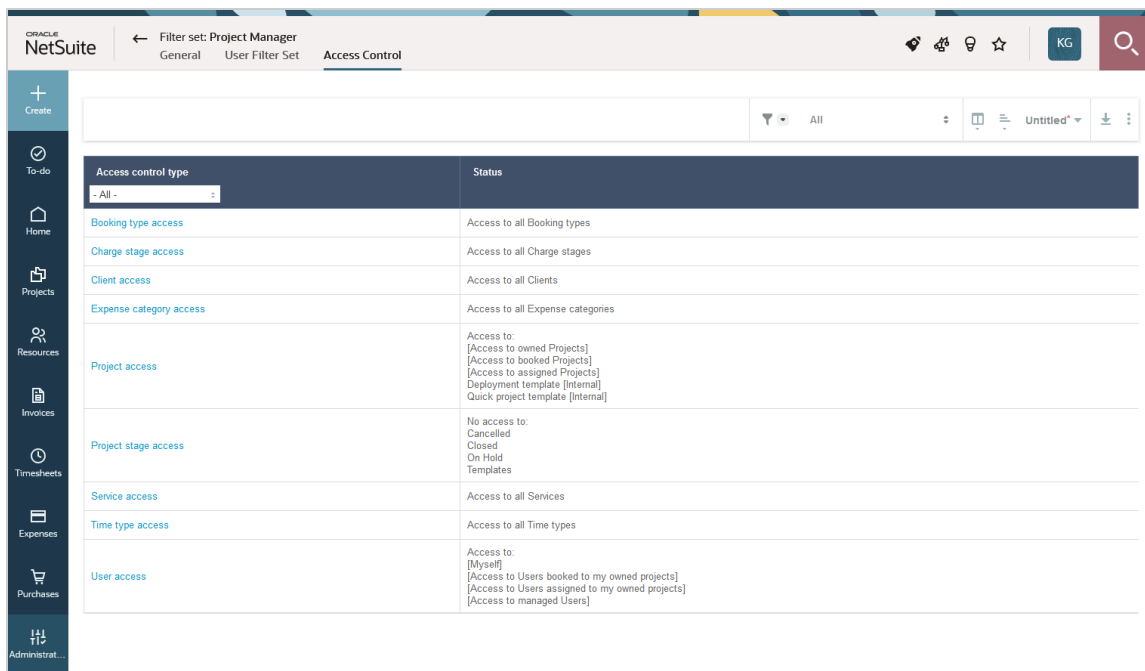
### To view or modify the Access Control for a filter set:

1. Go to Administration > Global Settings > Users > Filter Sets.

2. Click a Filter set name to display the Filter set form.
3. Click the **Access Control** link.
4. To modify Access Control, click the Access control type you would like to modify for this filter set.
5. Include or exclude items by adding or removing the items from the Available or Selected areas, respectively.
6. Click **Save**.

## Customer/Project/Project Stages

Filter sets can limit the view of customers, projects and project stages. For example, you could set a project manager filter set to be able to access only owned projects, booked projects, or assigned projects as well as only projects in a certain project stage.



Access control type	Status
- All -	
Booking type access	Access to all Booking types
Charge stage access	Access to all Charge stages
Client access	Access to all Clients
Expense category access	Access to all Expense categories
Project access	Access to: [Access to owned Projects] [Access to booked Projects] [Access to assigned Projects] Deployment template [Internal] Quick project template [Internal]
Project stage access	No access to: Cancelled Closed On Hold Templates
Service access	Access to all Services
Time type access	Access to all Time types
User access	Access to: [Myself] [Access to Users booked to my owned projects] [Access to Users assigned to my owned projects] [Access to managed Users]

## Expense Items/Booking Types/Charge Stages

Filter Sets can limit the view of Expense Items, Booking Types and Charge Stages. For example, you could prevent an employee from accessing the Miscellaneous Expenses item or the Overage charge stage by modifying the filter sets.

## Employees/Services/Time Types

Filter sets can limit the view of employees, services, and time types. For example, you could set an employee filter set to be able to access only their own timesheets or choose only internal time types on their timesheet.

## Filter Sets Options at the Employee Level


See also [Filters Hierarchy Overview](#).

## Switching Filter Sets

If an employee has been assigned more than one filter set, the employee can select which filter set is currently active by using either of the following paths, depending on their Employee setup configuration.

### To select a filter set as active:


1. Go to User Menu > Change filter set to display the list of available filter sets. Click **Choose** on one of the rows to set that filter set as your active filter set for the current session.
2. Go to Employees and select the Employee ID. On the Employee Demographic form, scroll down the Primary filter set field and select the desired value.

 **Note:** This is only available if the Employee has been assigned more than one filter set.

## Primary Filter Sets Application Overrides

### To assign multiple filter sets at the Employee level:

1. Go to Employees and select the Employee ID. On the Employee Demographic form, scroll down the Filter set module overrides. Use the create or edit link to add or remove filter sets for the employee record.

 **Note:** If you are using the Filter set module overrides, changing the primary/active filter set does not impact the application overrides, unless the override setting is Active filter set.

## Frequently Asked Questions (FAQs)

### Why would an employee have more than one filter set assigned to them?

There may be instances where an employee is playing two or more role in the company. For example, a manager may be primarily responsible for the Eastern Region. But due to a vacancy in the company, they may also need to take over the responsibility for the Central Region. Using filter sets would allow the manager to view each of the regions individually. Remember that filter sets determine what data the employee has access to in your company's OpenAir account.

Administrators and users with a "All Access " filter set can experience slow performance in accounts with large amounts of data, especially when loading lists. Assigning multiple filter sets allows these users to change the active filter set to view only the data they need. Lists will load quicker if the filter set combination returns significantly less data than the "All Access" option.

### Can I delete a filter set?

You cannot delete a filter set if there are employees assigned to it. To delete a filter set, you must remove all assigned employees first. You can run a detail report for the filter set which can show what employees are assigned to it. You can delete the filter set when no employees are assigned to it.

When considering the Access Control in filter sets, you should consider using the meta value relationships as much as possible. The values provided in employee and project access are the discrete lists of all the employees and projects in your company's OpenAir account, which can be cumbersome to manage.



For example, employee access for managers would typically need to see their direct reports. If you assign the meta value **[Access to Managed Employees]**, it automatically lets the employee see all direct reports who have that employee as their manager in your company's OpenAir account.

## Form Permissions

You can use Form Permissions to control users' access and permission rights according to their role. You can control several elements of the form.

Some of the form permissions settings can be used for access control:

- **General permissions** — Control users' ability to save and delete records. See [General Permissions](#).
- **Field settings** — Control users' permission rights for each field on the form. See [Field Settings](#).
- **Hidden divider sections** — Control users access to specific groups of fields. See [Hidden Divider Sections](#).
- **Permission rules** — Control users' permission right dynamically when certain conditions are met. See [Permission Rules](#).

Other settings control usability, input validation and display options:

- **Field order** — Control the order fields appear on the form if the record type supports this feature. See [Field Order](#).
- **Text field length** — Control the maximum length of text fields on a form. See [Text Field Length](#).
- **Form options** — Control general form display options. See [Form options](#).
- **Form message** — Add a custom message to the form. See [Form message](#).

There are two ways to access form permissions:

- Go to a record form, such as the Project Properties form, for example, click the Tips button, and click **Modify the form permissions**.

The following page appears. Scroll down or use the quick links on the left-hand side to configure the permission settings for this form.

- Go to Administration > Customization.

The following page appears. You can select a form on the left-hand side, then click on the **Field Access** tab to set the general permissions, field settings and hidden divider sections and on the **Rules** tab to set the permission rules.

**Note:** Form permission settings apply throughout the OpenAir web application as well as the OpenAir Mobile applications and the OpenAir OffLine desktop application.

## General Permissions

General permissions control users’ ability to save and delete records. You may check the **Disable the Delete button** and **Disable the Save button** boxes for each role. General permissions settings are universal for the entity associated with the form.

## Field Settings

Field settings allow you to set users permission rights for each field on the form and for each role. On the form permission page, each row corresponds to a field and each column corresponds to a role. You can select the permission rights given to a specific role over a specific field by selecting one of the following dropdown options:

- **REQ** — Required on form. Employee must enter a value.
- **RO** — Read Only on form. Entry is not allowed.
- **Hide** — Hide from form. Field does not display on form.
- **R-RO** — Read Only for system required fields.
- **R-Hide** — Hide from form for system required fields.

Field Settings are universal for the entity associated with the form.

**Note:** Field settings and switches override Permission Rules. If field settings or switch-based **field is required** options are used to control a set of fields, you cannot control those fields using permission rules.

The "Ready for Recognition" box on Projects> Tasks (Pending/ Completed/ All) does not support form permissions as standard. To enable form permission support for the "Ready for Recognition" box, contact OpenAir Customer Support.

**Field settings**  
 A field will not be made read-only or hidden if it is required and does not have a value.  
 Keys: [REQ] = Required, [RO] = Read-only, [HIDE] = Hidden

	Admin	Consultant	Project mana...	Resource m...	Controller	Contractor
Project name	REQ	REQ	REQ	REQ	REQ	REQ
Client	REQ	REQ	REQ	REQ	REQ	REQ
Project manager						RO
Project stage						RO
Start date	REQ	REQ	REQ	REQ	REQ	REQ
Budget (hours)						HIDE

## Hidden Divider Sections

Hidden divider sections control users' access to specific groups of fields. Check the box to hide a section of the entity form for users with a specific role. Sections are defined as a grouping of fields with a section title. Both the fields and the section title are hidden from users when the box is checked.

**Note:** The Hidden divider sections settings are only available if the feature is enabled on your account. Contact OpenAir Customer Support and ask for the following feature: **Hide divider sections on Forms.**

**Hidden divider sections**  
 Check the box to make a section hidden for a role.

	Admin	Consultant	Project mana...	Resource m...	Controller	Contractor
Notifications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Message board enabled/disabled according to:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Loaded hourly cost	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Expense policy	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Additional information	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Filter set	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Attachments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

## Permission Rules

**Note:** Form permission rules are available only if the feature is enabled on your account. Contact OpenAir Customer Support and ask for the following feature: **Form Permission Rules.**


Permission rules control permission rights dynamically when certain conditions are met. You can create new rules or edit existing rules and select the access permission for selected fields when one or all the

conditions defined are met. The conditions can apply to any of the standard and custom fields on the entity form or to the user role. You can choose the access permission applicable to selected field from the following dropdown options.


- **Show** — Displays selected fields when the conditions are met.
- **Hide** — Hides selected fields when the conditions are met.
- **Read Only** — Marks selected fields as Read Only so that users cannot edit them when the conditions are met.
- **Required** — Marks the selected fields as required when the conditions are met.
- **Hide and Clear** — Hides the selected fields and clears any values in them when the conditions are met.
- **Limit values** — Allows you to limit which values are available to select in a field when the conditions are met. Selecting this rule displays the **Limit values** pick lists.
- **Hide buttons** — Hides selected buttons, such as “Save”, “Delete” or “Cancel”, when the conditions are met.

### To create permission rules:

1. Access the **Create a new rule** form using either of the following methods:
  - Go to Administration > Customization, select an entity form, click the **Rules** tab and click the **Create** link.
  - Go to an “Edit entity” form (for example, the Project Properties form), click the **Modify the form permissions** link from the Tips menu, scroll down to **Permission rules** and click the **Create** link.
2. Enter a rule name.
3. Define the conditions for the rule. Multiple conditions may be required to create the rule.

 **Note:** Standard fields, custom fields, and employee roles are options within the conditions.

4. Click **Perform action** and select one of the dropdown options.
5. Select the fields or the button the action will apply to. Multiple fields or buttons may be selected.
6. If you selected the **Limit values** action, for each field selected:
  - a. Click one of the selected fields.
  - b. Select the values using the **Limit values** pick list to restrict the values displayed for this field.
7. Set a **Custom message** and the **Severity of custom message** as required. The severity setting determines the color scheme for the message to be displayed at the top of the form.
8. Click **Save**.

 **Note:** Field settings and switches override Permission Rules. If field settings or switch-based **field is required** options are used to control a set of fields, you cannot control those fields using permission rules. However, those fields can be included in any of the rule conditions.

Create a new rule

Cancel Save Save & create another

Rule name

Define conditions:

Any of the following  All of the following

Client equal to Global Information OR

[Add rows]

Perform action \*

Limit values

Available

Project budgets approved by  
Message board enabled/disabled  
Resource  
Sales Rep  
Radio Group

Selected

Employee  
Resource

Add selected >  
Add all >

< Remove selected  
< Remove all

Limit values

Available

Collins, Marc  
Collins, Marc  
Consultant [Generic]  
Cox, Brian  
Davis, Judy

Selected

Carr, Bill  
Carter, Tom  
Collins, Marc  
Davis, Judy

Add selected >  
Add all >

< Remove selected  
< Remove all

To choose limit values, click on one of the selected fields

Custom message will be displayed

Severity of custom message

error

Custom message

Cancel Save Save & create another

## Field Order

You can create different form layout, and change the order in which standard and custom fields and standard and custom section dividers appear for each form layout, and apply the form layout to selected user roles. Depending on their role, users will see a different form layout when they view, add or modify a record, for record types that support this feature.

**Note:** You can also set the position of custom fields to appear after any standard or custom field or add a custom form section when creating or modifying custom fields. See the help topics [Custom Field Position](#) and [Custom Field Position](#).

### To create a form layout and assign it to specific roles

1. Access the **Field order** form using either of the following methods:
  - Go to Administration > Customization, select an entity form, click the **Field order** tab.

- Go to a record form (for example, the Project Properties form), click the **Modify the form permissions** link from the Tips menu, and scroll down to **Field order**.
2. Click **Create**.

**Note:** To modify an existing layout, click **Edit** next to the layout name.

3. Enter a **Name** for the custom layout.
4. In the **Field order** list, click the field or section divider you want to move, and use the arrows pointing up or down to move the field or section divider up or down.

You can move multiple fields and section dividers at the same time. To do so, hold Ctrl or Shift and click the fields and section dividers you want to select, then use the arrows to move the fields and section dividers.

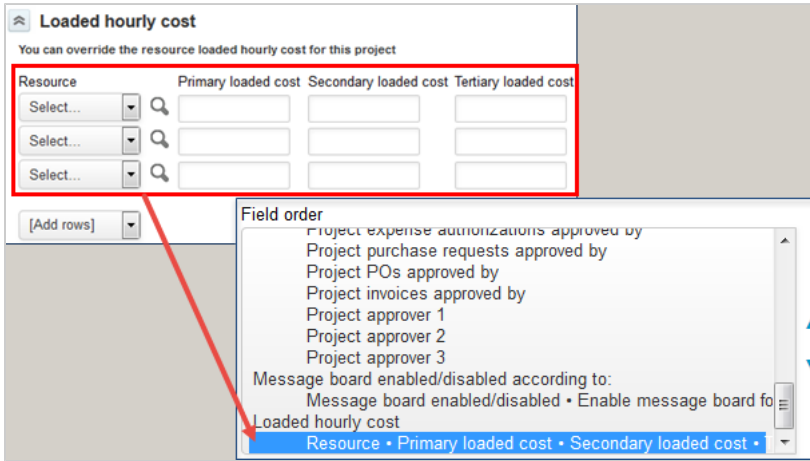
5. Under Assigned to roles, select the roles you want to assign this form layout to.
6. Click **Save**.

The screenshot shows the 'Set up field order' dialog for 'Quick Project'. The dialog has a 'Name' field containing 'Quick Project'. Below it is a 'Field order' list with the following items: Project stage, Project name, Customer, Project owner, Project location, Start date (YY-Month-DD), Budget (hours), Currency, Revenue • Cost, and Cost center • Billing code. There are up and down arrows next to this list. Below the field order list are two 'Assigned to roles' lists. The left list contains: Admin, Client, Consultant, Contractor, Controller, Project manager, Resource manager, and View the script deployment log report. The right list contains: Admin and Consultant. There are 'Add selected >' and '< Remove selected' buttons between the role lists, and 'Add all >' and '< Remove all' buttons below them. The dialog has 'Cancel', 'Delete', and 'Save' buttons at the top and bottom.

Note that some fields can only be moved together as a group, for example:

- Project Task
  - "ID" and "Task name"
  - "Priority", "Part of Phase", and "Project task type"
  - "Planned hours" and "Percent complete"
  - "Start date" and "End date"
  - "Employee", "Hours remaining", and "Override (hours)"
- Expense Report
  - "Tracking number" and "Currency"
  - "Date" and "Accounting date"

Compound objects with individual access settings are moved together as a block.



## Text Field Length

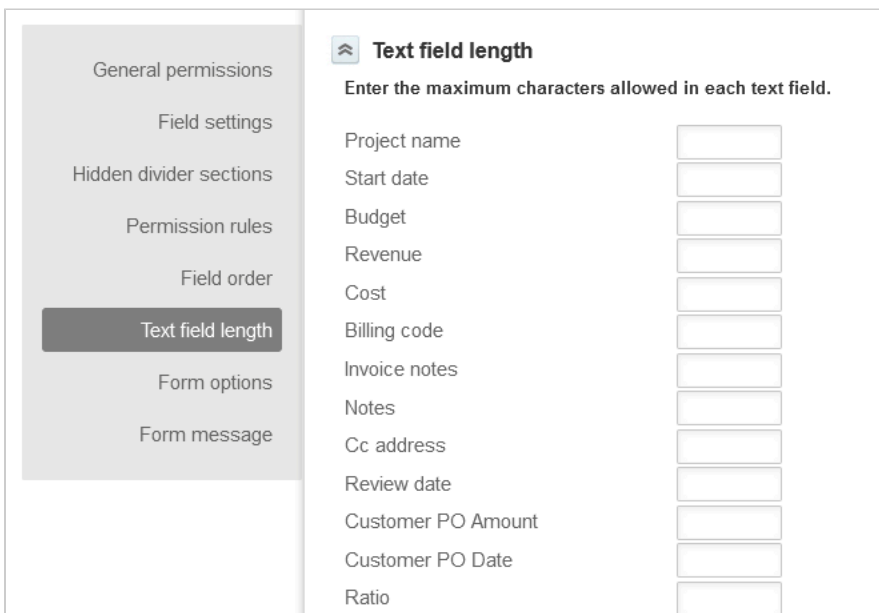
This feature shows you the list of fields that can have a maximum character length set, and lets you to set the maximum lengths. If you leave a field blank then the maximum database length for the field is applied.

**Note:** If you specify a maximum length greater than the length allowed in the database then your maximum value will be ignored and the database maximum for the field applied.

The new text field length maximum is applied when creating a new form and modifying an existing form.

**Note:** If you have an existing value that is longer than the new **Text field length** then the existing length of the value will be treated as the maximum length while the form is being modified.

**Note:** The Text field length sections settings are only available if the feature is enabled on your account. Contact OpenAir Customer Support and ask for the following feature: **Maximum Text Field Length Form Permission Settings**.



## Form options

The following form level permissions can be set:

- **Display "Save & create another" button at top** — Select this option to display the **SAVE & CREATE ANOTHER** button when create a new entity.

**Note:** This behavior can be overridden by the **Add "Save & create another" button to the top right of forms** company switch under Administration > Global Settings > [Display] Interface : Display.


- **Display Custom Fields before form field** — This option determines where on the form the custom fields will be positioned in relation to the standard form fields. The **[Default]** setting will place the custom fields at the bottom of the form. You can also select **[Top]** or specify a field to position the custom fields after.
- **Disable divider before Custom Fields** — This option will disable the displaying of the divider.
- **Fields which maintain value on "Save & create another"** — This option allows you to select the fields that will be copied forward when using the "Save & create another" feature.

## Form message

You can define messages to be shown on the form whenever users go to the form.



**Note:** You can also show:

- Custom messages on forms depending on certain conditions using permission rules on Modify form permissions. See [Permission Rules](#) for details.
- Confirmation, warning and error messages on forms using form scripts. See the help topics [NSOA.form.confirmation\(message\)](#) and [NSOA.form.error\(field, message\)](#) under  [User Scripting](#).

Form messages can be displayed either at the top of the form or to the right of the form at the top.

The message can be simple text or may use HTML formatting.

- Example of HTML formatting

**This project must be closed by year end.**

```
1 | <p style="font-family:arial;color:green;font-size:20px;">This project must be closed by year end.</p>
```

- Example of an information message box

This project must be closed by year end.

```
1 | <span class="message blockMessage informationMessage">This project must be closed by year end.</span>
```

- Example of a warning message box


This project must be closed by year end.


```
1 | <span class="message blockMessage warningMessage">This project must be closed by year end.</span>
```

- Example of an error message box

This project must be closed by year end.

```
1 | <span class="message blockMessage errorMessage">This project must be closed by year end.</span>
```

 **Note:** This will format the text to look like an error message. It will not stop the form from being saved.

 **Important:** You should not use this feature to run client side script to modify form behavior.

## Employee Access Control Settings

All users must be assigned one and only one role and at least one filter set. You can also set rights and privileges for users on an individual basis when creating or editing user records for your company's employees, subcontractors or guests.

This section gives an overview of the available settings relevant to configuring access control. Go to Administration > Global Settings > Users > Employees > [*select an Employee*] to review the available settings. For example:

- **User Access Removal** — Only employees marked as active employees have access to OpenAir. See [User Access Removal](#).
- **Application Options** — Options in the **Demographic** tab control certain user privileges for the different OpenAir applications. See [Application Options Overview](#).
- **Application Access** — The **Access Control** tab can be used to control user access to specific applications. See [Access Control Overview](#).
- **Filter Hierarchy** — The **Primary Filter Set** and **Filter set** fields on the Demographic form as well as the **Filter sets** tab define what the user can see in OpenAir. See [Filters Hierarchy Overview](#).
- **User Proxy** — User proxy enables an authorized employee to use OpenAir as another employee with no knowledge of that other employee's password. See [User Proxy Overview](#).


### User Access Removal

Only employees marked as active employees have access to OpenAir. To remove access to OpenAir for a particular user, either temporarily or indefinitely, clear the Active employee box on the Demographic form for this employee.

### Application Options Overview

Certain user privileges can be granted or revoked from the Employee Demographic form. Scroll through the Employee Demographic form to review the options available.

In particular, you may enable users to un-approve or un-export items within OpenAir such as timesheets, expense reports, invoices, booking requests, project recognition transactions, and proposals. If the item follows the approval process functionality, an additional setting in the Demographic form lets you grant un-approve as well as un-export permission to an employee for the item. These permissions are controlled at the employee level only on the Employee Demographic form. They cannot be granted to a role.

 **Note:** These settings control approval and data export capabilities. They are sensitive and are used to support integration in many cases.

### Access Control Overview

Access Control settings are available in the employee record for existing employees. When adding a new employee, the access control tab becomes available after the Employee Demographic form has been saved.

Access control type	Status
Application access	Access to all applications
Exchange access	Access to all optional Data Exchange items

2 rows

There are two main access control settings:

- **Application access** lets you control which modules (applications) are available to the employee from the main navigation menu.

You should grant access to application on a needs basis. For example, if an employee does not have responsibility for invoicing or permissions to view invoicing data, remove Invoices from their application access. This helps minimize confusion for users.

Application access determines which type of user license is taken up by the employee. An employee with any combination of Account, Timesheets and Expenses application access takes up a Timesheets and Expenses (T&E) only license. An employee with any other application access takes up a Full user license. For more information, see the help topic [Licenses](#).

Granting application access does not automatically grant feature permission. This is controlled by the role assigned to the employee. See [Role Permissions](#).

Check the **Default set of applications for new employees** to grant the same application access for the new employee records you create.

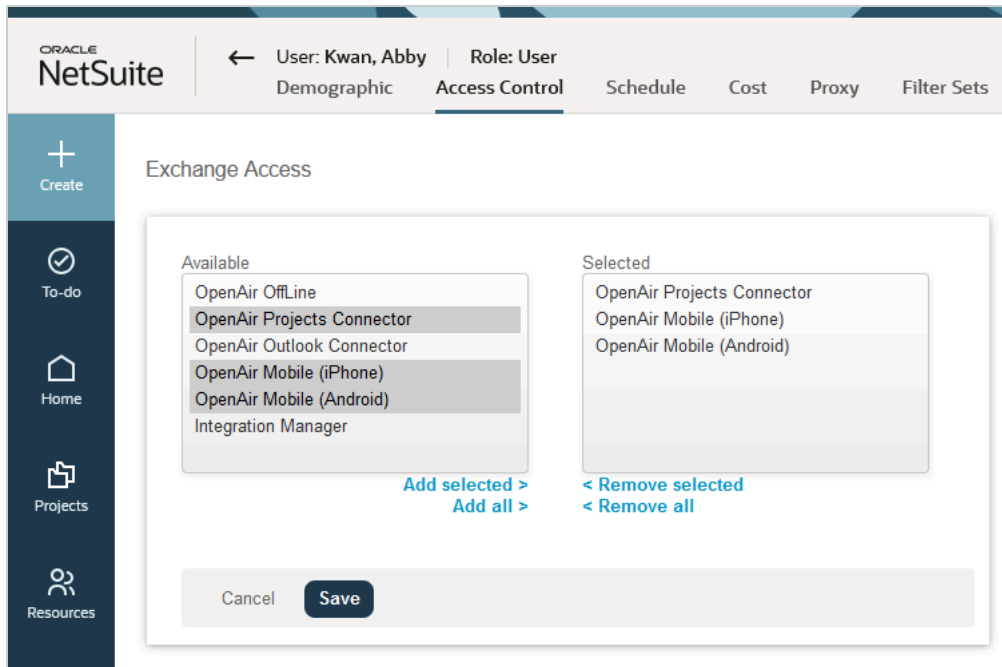
**Note:** Default application access typically includes Account and Timesheets. You should not grant application access other than Account, Timesheets and Expenses to avoid taking up Full user licenses unnecessarily.

**Tip:** The All Item Types in Calendar optional feature lets employees see their task assignments and bookings in the calendar even if they do not have access to the Projects and Resources module. See the help topic [All Item Types in Calendar](#).

The screenshot displays the 'Application access' configuration interface in Oracle NetSuite. At the top, the user is identified as 'User: Kwan, Abby' with the role 'User'. The navigation menu includes 'Demographic', 'Access Control' (which is active), 'Schedule', 'Cost', 'Proxy', and 'Filter Sets'. The main content area is titled 'Application access' and contains two columns: 'Available' and 'Selected'. The 'Available' column lists: Account, Workspaces, Resources, Projects, Timesheets, Expenses, Purchases, and Invoices. The 'Selected' column lists: Account, Timesheets, and Expenses. Below the columns are four buttons: 'Add selected >', 'Add all >', '< Remove selected', and '< Remove all'. At the bottom of the configuration area, there is a checkbox labeled 'Make this the default application access for new users' which is currently unchecked. At the very bottom are 'Cancel' and 'Save' buttons.

- **Exchange access** lets you control which Add-on services the employee is allowed to download and use. An employee must have exchange access for the add-on service to be able to work with OpenAir data using the application.

**Note:** Removing access to an add-on service application does not eliminate the ability to download the application. The mention “Not approved for download” appears above the download link if the user has not been granted access to that application. All add-on service applications require authentication to connect with OpenAir. Authentication fails if the employee does not have the appropriate exchange access.



## Filters Hierarchy Overview

Assigned filter sets determine what data users have access to. All users must be assigned at least one filter set — their primary filter set. Other filter sets can be assigned to the employee. Any filter sets may be used to override the primary filter set for a given application. You can also include an employee into the employee access definition of certain filter sets — users with any of these filter sets assigned would then have access to this particular employee.

**Important:** When assigning filter sets to an employee, you should assign only the filter sets that show the data the employee need to access in the course of their current work. If the employee's responsibilities change over time you should change the filter sets assigned to this employee accordingly.

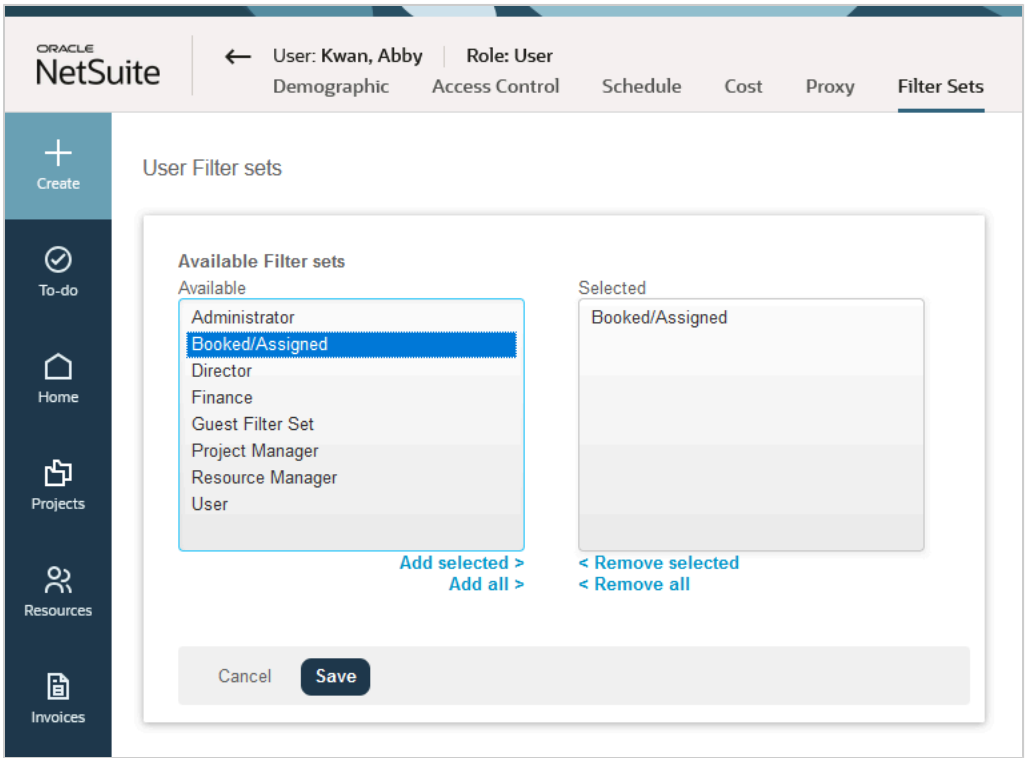
The following settings are available on the employee record:

- **Filter Sets tab** — Use the **Filter sets** tab to assign multiple filter sets to the employee. To do so:
  1. Go to Administration > Global Settings > Users > Employees > [Select an employee] > Filter Sets.
  2. Select filter sets from the **Available Filter sets** list and click **Add selected**.
  3. Click **Save**.

Users only have one of their assigned filter sets active at a given time and can switch between assigned filter sets to access different types of data.

**Tip:** When the All Access filter set is assigned to an employee, you should assign multiple filter sets and include filter sets that return significantly less data when viewing transaction lists such as a booking list, for example. This enables the employee to change filter set and limit the amount of records on lists to speed up loading times and improve the performance of lists.

**Note:** You can also assign filter sets to employees when creating or editing filter sets. See [Filter Sets Overview](#).



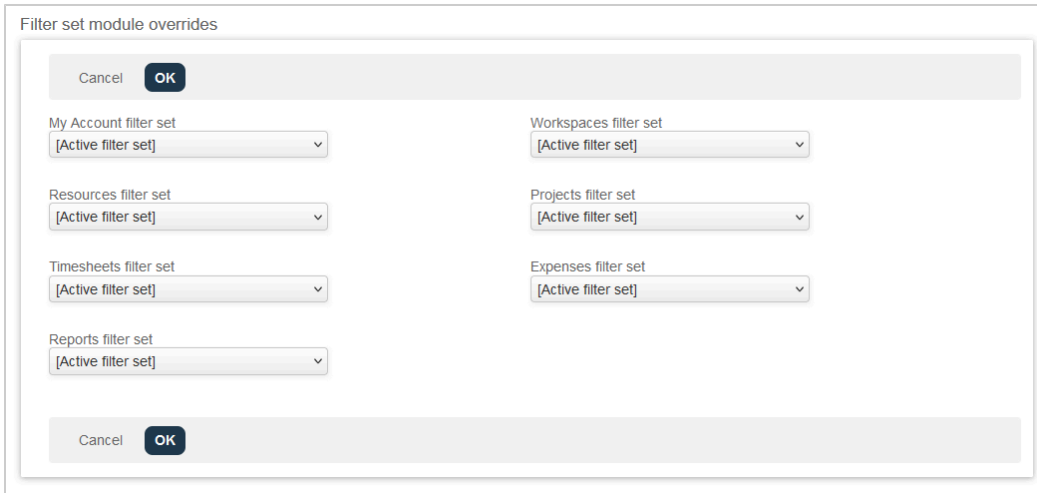
- Primary Filter Set** — All users must be assigned at least one filter set — their primary filter set. This is set to the default filter set when creating or importing users. You can select a primary filter using a dropdown in the top section of the Employee Demographic form. If the primary filter set was not already assigned to the user, it is added to the list of assigned filter sets on the **Filter Sets** tab.

Manager Collins, Marc	Department London
Job code PM	Cost center 04-London
Primary filter set Owned Projects	Filter set module overrides <a href="#">&gt; Create</a>

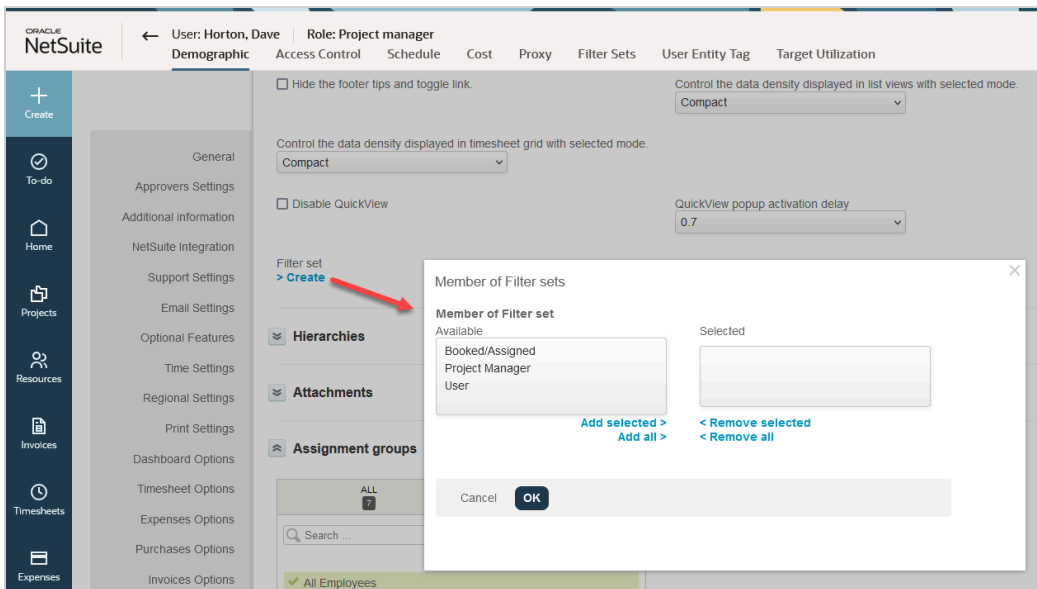
- Filter set modules overrides** — This optional application overrides feature allows you to grant or restrict access to data depending on the OpenAir application the employee is using. Contact OpenAir Customer Support to enable this feature.

The optional override may be used to control items such as projects available when users fill a timesheet or review resource booking, for example, while allowing a general view in other applications.

When the feature is enabled, an additional setting becomes available on the Employee Demographic form next to **Primary filter set**. Click the **Create** link to define filter set overrides. Any of the available filter sets can be selected for each application. Changing the primary filter set or changing the active filter set does not impact the application overrides, unless the override setting is **[Active filter set]**.




- Filter set** — You can include an employee into the employee access definition of certain filter sets if the filter set restricts employee access. Users with any of these filter sets assigned would then have access to this particular employee. Use the **Filter set** setting, normally found in the Display Options section at the bottom of the Employee Demographic form to ensure the employee is included in the employee access definition of selected filter sets. Depending on your configuration, this setting may need to be a required field.



## Project level access

An optional feature enables to restrict project access according to a defined project hierarchy. With this feature enabled, the **Use to determine filter set access for projects** box becomes available on the Edit hierarchy form. If you check this box, a **Project level access** section becomes available on the Employee Demographic form and you can assign a node in that project hierarchy to the user. You can restrict access to project information relevant to the assigned project hierarchy by creating a filter set and

configuring project access to **[Access to Projects in my hierarchy node]**. Contact OpenAir Customer Support and ask for the following feature to be enabled: **Enable ability to define project hierarchy for filter sets**.

For more information about configuring and using hierarchies, see  [Administrator Guide](#) under Global Settings > Company > Hierarchy.

## User Proxy Overview

User proxy enables an authorized employee to use OpenAir as another employee with no knowledge of the other employee's password. If users are granted the right to proxy in as other users, they can click **Log in as** from the **User Menu** menu and select an employee from a list of available proxies to sign in on their behalf. A new instance of OpenAir opens allowing the employee to perform a function for the proxied employee.

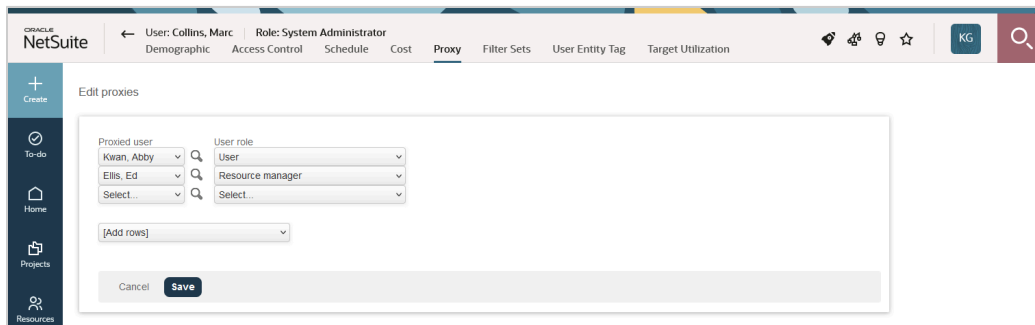
Users with the role permission **Create own proxies** enabled are permitted to designate proxies who will be able to sign in and perform a function on their behalf. **Proxy restrictions** may also be set for the role.

The role permissions a user will have when proxying in as another employee is specified in the proxy configuration.

The user proxy feature is helpful for delegating certain processes when employees are out of the office or do not have access to OpenAir. However, it can have security implications. Account administrator should exercise control over users ability to proxy and set expiration dates for user proxies to ensure that proxying rights are granted only when required and to authorized users only.

### To enable an employee to proxy in as another employee:

1. Go to Administration > Global Settings > Users > Employees and click the Employee ID of the employee you want to grant the proxying rights to.
2. Click the **Proxy** tab.
3. Select the **Proxied employee** and **User role**. This will determine the role permissions the user will have when proxying in as the proxied employee. Use the role assigned to the proxied employee on their Demographic form to ensure the proxying user has the same permissions as the proxied employee.
4. Set an **Expiration date** if required by the Proxy Expirations configuration settings. This ensures the proxy expires automatically on the specified date. See [Enabling Proxy Expirations](#).
5. Click **Save**.



Proxied user	User role
Kwan, Abby	User
Ellis, Ed	Resource manager
Select...	Select...

[Add rows]


Cancel Save

Users with the role permission **Create own proxies** enabled are permitted to designate proxies who will be able to sign in and perform a function on their behalf.

If the Proxy Approver Notifications feature is enabled for your company's OpenAir account, and if the designated proxy employees can approve transactions on their behalf, proxy approvers receive



notification email messages about transactions awaiting the proxied employee's approval. See the help topic [Proxy Approver Notifications](#).

 **Note:** Account administrators cannot create their own proxies for security reasons. It is not possible for any employees to sign in on behalf of an employee with an account administrator role.

### To enable another employee to proxy in as oneself:


1. Go to the **User Menu** menu and click **Proxies**.
2. Select a user who may proxy.
3. Click **Save**.

## Enabling Proxy Expirations

After the proxy expiration is activated you will be able to set expiration date when editing user proxies.

### To enable expiration dates for proxies:

1. Go to Administration > Global Settings > Account > Proxy Expirations.
2. Check the **Proxies have expiration dates** checkbox.
3. Select a **Default proxy expiration** period from the dropdown options.
4. Click **Save**

 **Tip:** You can configure OpenAir to send an email notification whenever an item is submitted or approved by a proxy. For example, you can go to Administration > Application Settings > Timesheets and configure OpenAir to notify the **[Approver]** whenever a timesheet **Was approved by proxy**.

## Guest Roles and Guests

You can provide guest access to your customers if you want to share some project information with them such as project Gantt charts, project outlines, or invoices, for example. Guests are customers who are able to sign in to OpenAir and view the application data that is associated with them.

Guests are stored as employees [users] in the OpenAir database. The Demographic form for guests is similar to the Demographic form for employees — many of the fields and settings are the same. However, guests must be assigned a guest role. You will need to create a guest role before you can add a guest user. You must also select the appropriate Customer in the **Employee is this Customer** dropdown when adding a guest user.

Guest role settings include the following: Guest can view Project Gantt charts, Guest can view Project outlines, Guest can view task details in Gantt/outline views, Guest can view Invoices, Guest can view Workspaces, and Guest can customize lists.


### To create a guest role:

1. Go to Administration > Global Settings > Users > Guest Roles.
2. Click the **Create Button** and select **New Guest role**. The New Guest Role form appears.
3. Enter the **Role** name. Check the boxes for all permissions you want to grant guest users with this role.
4. Enter any **Notes**, if desired.

5. Click **Save**.

### To add a guest user:

1. Go to Administration > Global Settings > Users > Guests.
2. Click the **Create Button** and select **New Guest**. The New Guest form appears.
3. Enter the Employee ID. Select a role and a customer from the **Role** and **Employee is this Customer** dropdowns, respectively.
4. Enter and confirm a password for the user. Check the **Force a password change** box to ensure the guest user changes password when signing in to OpenAir for the first time.
5. Click **Save**.
6. Go to the **Filter sets** tab.
7. Select any applicable filter sets.
8. Click **Save**.



 **Note:** You need to create at least one guest role before you can add a guest user. You will not be able to save the New Guest form if you are not able to assign a role to the user.

## Configuring and Using Auditing features


The audit information available in OpenAir and the different options to access this information give you the flexibility to implement an auditing scheme that suits your specific business needs.

This section introduces the basic concepts and mechanisms available for auditing purposes in OpenAir:

- **Reports** — The OpenAir Reports application allows you to configure and run reports for auditing purposes, including access logs. See [Reports Overview](#).
- **Audit trail fields** — The audit trail fields allow you to report on changes made at a record or a field level, identifying what was changed, when and by whom. See [Audit Trail Fields](#).
- **Audit trail for custom fields and company switches** — For custom fields and company switches, you can access a log of changes directly on the form. See [Quick Audit Trail on Forms](#).
- **Data export** — OpenAir data export feature can be used to access the auditing information available from reports and audit trail fields. See [Data Export for Auditing](#).

 **Tip:** You can use the User Scripting feature to extend the existing auditing capabilities. For example, a form script could be used to record additional audit information in a custom field on submit when certain conditions are met. See  [User Scripting](#).

## Reports Overview

The OpenAir reports application allows account administrators and users with the appropriate privileges to create and run reports for auditing and other purposes. For a description of the Reports application, see  [Administrator Guide](#). This section describes some of the reports you may use for auditing purposes:

- [User Access Log](#).
- [Module Access Overview](#).
- [Privileges Overview](#).
- [Auditing and Managing OAuth 2.0 Authorizations](#).

Reports can also be used for audit trails at a record or field level using the Audit trail fields feature. See [Audit Trail Fields](#).

## User Access Log

OpenAir records information about sign-in attempts including information such as the users attempting to sign in, their IP addresses, or the times and outcomes (successful / failed) of sign-in attempts. Account administrators and employees with the **View the employee login detail report** role permission can run an account-wide **Employee logins** reports to access this information in OpenAir.

**Note:** The following steps assume the Report Management and Editor Interface feature is not enabled. If you have the Report Management and Editor Interface feature enabled on your account and on your Employee Demographic form, go to Report > Management and use the search functionality to find the report template.

### To view a user access log:

1. Go to Reports > Detail.
2. Click the **Employee logins** link under **Account-wide**. The “Employee login detail report options” form displays.
3. **Employee login time** — Select a **Date Range** and a **Start** and **End** date if setting a **Custom** date range.
4. Click **Edit** next to Report layout, use the pick list to select the information you want to include in the report and click **OK**. In the example below, **Employee** is the full name of the employee, **Source** is the IP address the employee attempted to access OpenAir from and the **Status** of the sign-in attempt (successful / password incorrect / inactive user / locked user / restricted IP address).

**Tip:** Select **API** to show whether the sign-in was performed using an API call.

The screenshot shows the 'Employee logins detail report options' form. The 'General' section includes a 'Date range' dropdown set to 'Custom =>', with 'Start (MM/DD/YY)' and 'End (MM/DD/YY)' date pickers set to 02/01/11 and 02/28/11 respectively. The 'Options' section has a 'Report layout' dropdown set to 'Employee logins detail report layout' and an 'Edit' link. A modal window titled 'Employee logins detail report layout' is open, showing two columns: 'Available' and 'Selected'. The 'Available' column lists various fields, including 'API', 'Employee', 'Employee - Account access', 'Employee - Active', 'Employee - Address line one', 'Employee - Address line two', 'Employee - Allow NetSuite Single Sign-On', 'Employee - Allow support log in', 'Employee - Allowance reports approver', and 'Employee - Allowance reports approver for'. The 'Selected' column contains 'Employee', 'Source', 'Login time', and 'Status'. There are 'Add selected >' and '< Remove selected' buttons between the columns, and '< Remove all' and '< Remove all' buttons at the bottom of the modal. The modal also has 'Cancel' and 'OK' buttons.

- Click **Create** or **Edit** next to Employee, use the pick list to select the employees you want to include or exclude from the report, and click **OK**.

✓ **Tip:** If your OpenAir account has many active users and you want to find specific employees, you may search for these employees using the find utility instead of the pick list. Click the List and Find links at the top to switch between the two employee selection utilities.

- Change any other settings as required.
- Click **Run** to run and view the report.

## Module Access Overview

Account administrators and employees with the **View account-wide reports** role permission can create an account-wide employee detail (tabular) report to audit which modules users have access to.

This report may be used to:

- Review which users have access to modules other than the Account, Timesheets and Expenses modules and take up one full user license.
- Determine for which users module access should be changed so they take up one Timesheets and Expenses (T&E) only user license instead.

For more information about licensing and user types, see the help topic [Licenses](#).

**Note:** The following steps assume the Report Management and Editor Interface feature is not enabled. If you have the Report Management and Editor Interface feature enabled on your account and on your Employee Demographic form, go to Report > Management and use the search functionality to find the report template.

### To view a module access overview:

1. Go to Reports > Detail.
2. Click the **Employee** link under **Account-wide**. The “Employee detail report options” form displays.
3. Click **Edit** next to Report layout, use the pick list to select the information you want to include in the report and click **OK**. You can include some basic information about the employee such as **Employee ID, Name**, whether the employee is **Active**, and whether the employee has access to each OpenAir module.

The screenshot shows the 'Employees detail report options' form. The 'General' tab is active, showing fields for 'Employee created date' and 'Employee updated date', each with a 'Date range' dropdown set to 'All' and 'Start (MM/DD/YY)' and 'End (MM/DD/YY)' date pickers. The 'Options' dialog box is open, displaying a list of available fields on the left and a list of selected fields on the right. The 'Available' list includes: Account access, Active, Address line one, Address line two, Allow NetSuite Single Sign-On, Allow support log in, Allowance reports approver, Allowance reports approver for, Appears in Filter sets, and Approval process participation. The 'Selected' list includes: Employee ID, Name, Active, Account access, Expenses access, Timesheets access, Invoices access, Opportunities access, Projects access, and Purchases access. Below the lists are buttons for 'Add selected >', '< Remove selected', and '< Remove all'. The 'OK' button is highlighted in green. Below the dialog box, there are checkboxes for 'Exclude transactions associated with inactive entities', 'Make this report available in project-specific situations', and 'Run the report in the background'. At the bottom, there is a checkbox for 'Save this report as' which is checked, and a text field containing 'Module Access Overview'.

4. Change any other settings as required.
5. Click **Run** to run and view the report.

Employee detail report - Module Access Overview

mostly report re-run report Clear sort

Employee ID	Name	Active	Account access	Expenses access	Timesheets access	Invoices access	Opportunities access	Projects access	Purchases access	Resources access	Workspaces access
JAdmin	Admin, Jim	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
MCollins	Collins, Marc	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
JKwan	Kwan, Jane	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No	Yes
JPinn	Pinn, Joe	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
MAdams	Adams, Mary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
MPorter	Porter, Marie	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TCarter	Carter, Tom	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
JDavis	Davis, Judy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
EEllis	Ellis, Ed	Yes	Yes	No	No	No	Yes	Yes	No	Yes	Yes
TFoster	Foster, Tim	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
JGates	Gates, Jack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SHuff	Huff, Sue	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
JKelly	Kelly, Joan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LMorse	Morse, Lia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
THugent	Nugent, Tara	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
BCates	Cates, Brian	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
DHorton	Horton, Dave	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TQuinn	Quinn, Teddy	Yes	Yes	No	No	No	Yes	No	No	No	No
SVila	Vila, Sally	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
GJameson	Jameson, Gary	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

20 rows on page  
71 total rows

1 2 3 Next

## Privileges Overview

The following account-wide reports can be used to review the access control mechanisms configured on your account. Configuring and running these reports follows a procedure similar to the procedure given above. See [User Access Log](#).

Only account administrators and employees with the **View account-wide reports** role permission can access these reports.

**Note:** The following list assumes the Report Management and Editor Interface feature is not enabled. If you have the Report Management and Editor Interface feature enabled on your account and on your Employee Demographic form, go to Report > Management and use the search functionality to find the report template.

- Under Reports > Detail > Account-wide:
  - **Roles** — to list the employees or the privileges assigned to each role.
  - **Approval processes** — to review rules associated with each approval process.
  - **Filter sets** — to review the employees assigned to each filter set, including filter set application overrides.
  - **Proxies** — to review user proxies configured on your account, including expiration dates.
- Under Reports > Advanced > Account-wide:
  - **Role privileges** — to review the privileges assigned to each role in a matrix format.

Role privileges - 6.4 Security Role Differences

modify report re-run report

Group	Privilege	Administrator	Consultant	Project manager	Resource manager	Controller	Contractor	View
All	All							
Timesheet Options	Disable overlapping timesheets	◆						
Expenses Options	Disable overlapping Expense reports	◆						
User roles - General settings	View clients	◆		◆		◆		
User roles - General settings	View and modify clients	◆		◆		◆		
User roles - General settings	View and modify existing clients (except name)	◆		◆				
User roles - General settings	View client locations	◆						
User roles - General settings	View and modify client locations	◆						
User roles - General settings	View prospects	◆						
User roles - General settings	View and modify prospects	◆						
User roles - General settings	View contacts	◆				◆		
10 rows on page								
625 total rows								

## Auditing and Managing OAuth 2.0 Authorizations

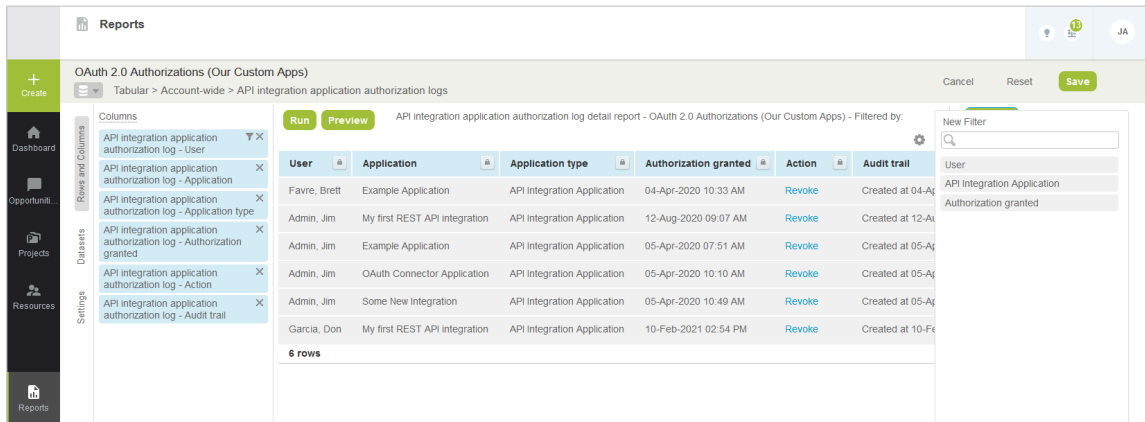
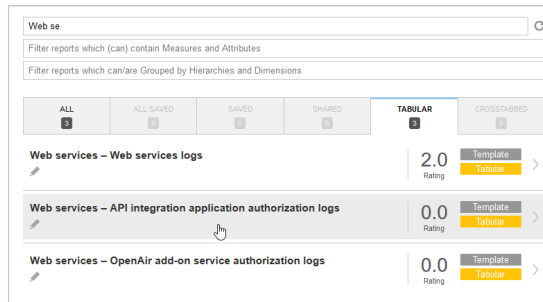
Account administrators can use web services reports to audit and revoke authorizations granted by OpenAir users to integration applications utilizing OAuth 2.0 to connect to OpenAir data.

- **API integration application authorization logs** — User authorizations granted to custom or third party applications registered with your OpenAir account in Administration > Account > API integration applications.
- **OpenAir add-on service authorization logs** — User authorizations granted to OpenAir add-on services (OpenAir Mobile and other add-on service applications).

The reports include information about which integration applications were authorized, when, and by which users. The reports also include a link to revoke the authorization given for an integration application by a user.

### To access the OAuth 2.0 authorizations logs (if the Report Management feature is enabled):

1. In OpenAir, go to Reports > Management.
2. Enter “web services” in the **Search saved reports by name** box. The Report Management UI shows the list of web-services tabular reports.
3. Click the report name, then click **New** to create a new report.
4. Add columns and define filters as required.
5. (Optional) Click Untitled in the top bar and enter a name for your report.
6. (Optional) Click **Save** to save the report you created for later use. The Report Management UI will list the report under on Saved reports tab.
7. Click **Run** to run the report.



## To access the OAuth 2.0 authorizations logs (if the Report Management feature is not enabled):

1. In OpenAir, go to Reports > Detail.
2. Click the report name under the Web services heading. The report options form appears.
3. (Optional) Set a date range for the **Authorization granted** filter. Defaults to All.
4. Click **Report layout** and select the columns to include, or keep the default layout.
5. (Optional) Click **Employee** and select the employees to include in the report.
6. (Optional) Click **API integration application** and select the applications to include in the report.
7. (Optional) Check the **Save this report as** box and enter a name for the report
8. (Optional) Click **Save** to save the report. The report will be accessible in Reports > Saved reports.
9. Click **Run** to run the report.

## Audit Trail Fields

OpenAir lets you include audit information in reports and to access a log of changes made to OpenAir data. This information is recorded in the Audit trail field in the OpenAir database. The information recorded includes: the change made to the record (created / updated / deleted), when, by whom, what fields were changed and the values before and after the change. Changes to custom fields are also included. Moreover, if a user proxied in to make changes to a record, the audit trail identifies the actual user who made the changes, rather than the proxied user.

This section describes two ways to include audit information in reports:

- [Viewing full audit trail in detail reports](#)





- Viewing audit trail values in summary reports

Audit trail fields can also be included when exporting OpenAir data. See [Data Export for Auditing](#).

## Viewing full audit trail in detail reports

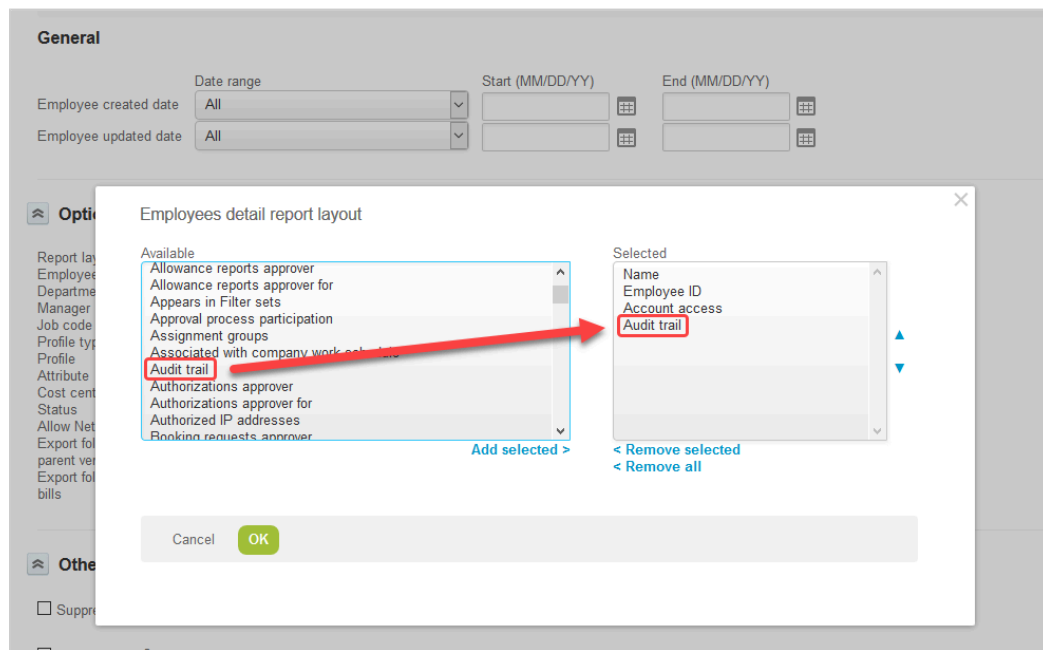
The full audit trail can be included in detail reports to provide a complete log of changes made to OpenAir records.

 **Tip:** Add the Audit trail field to the [Privileges Overview](#) detail reports to monitor any changes made to the access control mechanisms on your account.

 **Note:** To view the audit trail, a user must either be an administrator or have appropriate role permissions. The role must allow access to detail reports and have **View audit trail** enabled under the general settings section.

### To include the audit trail in detail reports:

1. Go to Reports > Detail.
2. Click the entity for which you would like to view an audit trail. The “Detail report options” form displays.
3. Set the **Date Range** for all date fields under General.
4. Click **Edit** next to Report layout, add **Audit trail** and any other information required to the list of **Selected** fields, and click **OK**.



5. Change any other settings as required.
6. Click **Run** to run and display the report.

**Note:** You can select the audit trail field in the account-wide employees detail report to track any changes to the filter set application overrides. Two letters acronyms are used to denote each application — e.g. “Pm Filter set” refers to the filter set override for the Project module or application. Refer to the list below for a list of acronyms and corresponding applications:

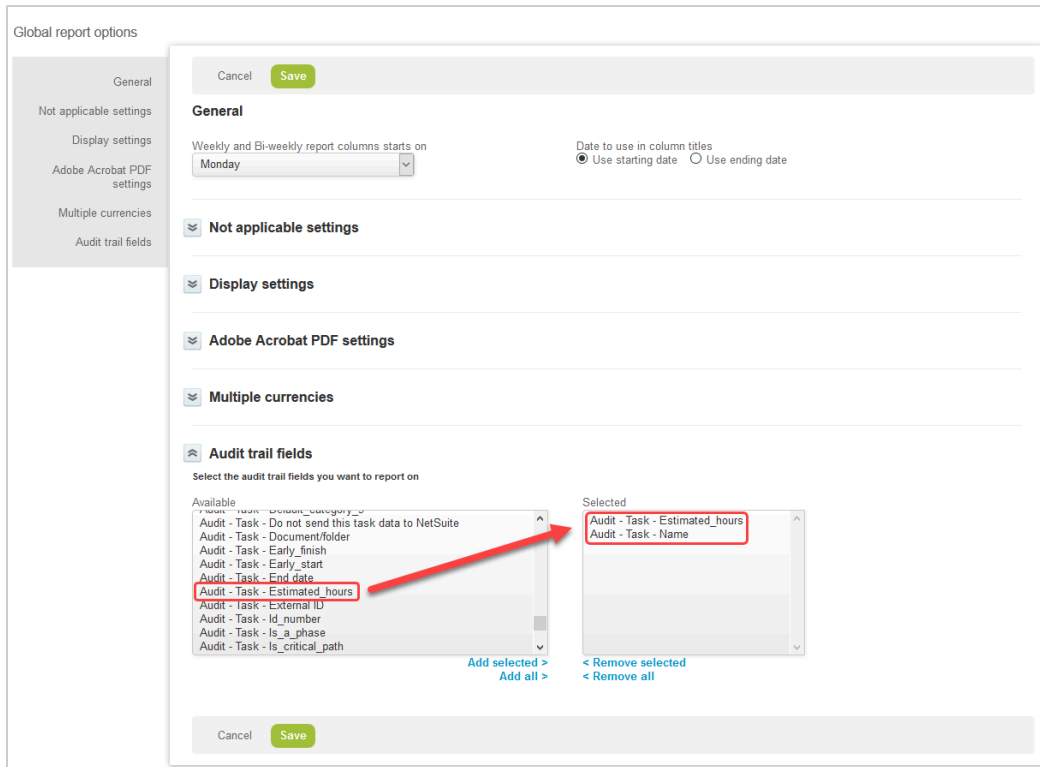
- Ma — My Account
- Km — Workspaces
- Om — Opportunities
- Rm — Resources
- Pm — Projects
- Ta — Timesheets
- Te — Expenses
- Po — Purchases
- Tb — Invoices

## Viewing audit trail values in summary reports

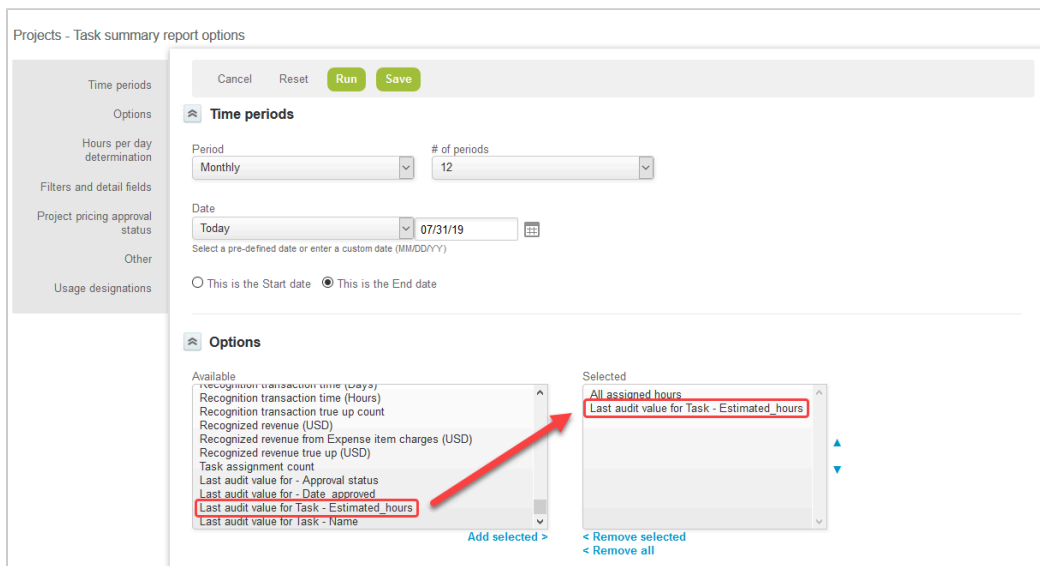
An optional features lets you run summary reports and include audit trail values. Users with the appropriate privileges can run a summary report on individual form values for a specified time period and have the report return what the value was at given points in time as determined by the time periods set in the summary report options. The report also displays the user name of the employee who changed the value. Contact OpenAir Customer Support and ask for the following feature to be enabled: **Audit trail values in summary reports**. Once the feature enabled, any user with the **View audit trails** role privilege can view this audit information.

### To show audit trail values in a summary report:

1. Go to Reports > Options.
2. Scroll down to the Audit trail fields section. The available audit trail values show as **Audit - [Entity] - [Field]**.
3. Select the Audit trail values you want to report on.



4. Click **Save**.
5. Go to Reports > Summary.
6. Select a summary report.
7. The audit trail values are available under the Options section. Select **Last audit value for [Entity] [Field]** to include the audit trail value in the summary report.



8. Select any other options as required.
9. Click **Run** to run and display the report.

## Quick Audit Trail on Forms


Account administrators and users with the appropriate role permissions can view the audit information for company switches and custom fields directly on the form. The audit information appears in a pop-up window and is presented in table format, displaying the user who made the change, the date the change was made, what the previous value was, and what the value was changed to.

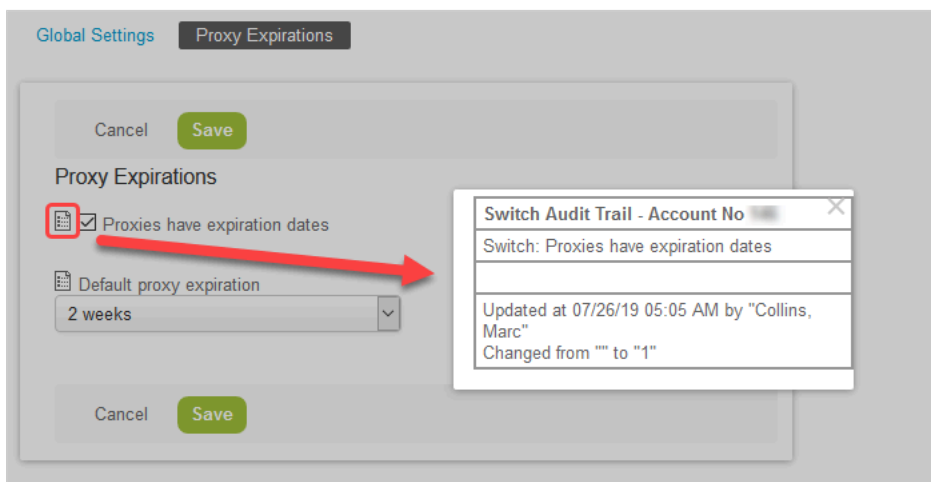
Refer to the following:

- [Quick Audit Trail for Global Settings](#)
- [Quick Audit Trail for Custom Fields](#)

## Quick Audit Trail for Global Settings

The Quick Audit Trail for Administration Settings optional feature enables you to keep track of changes made to Global Settings and determine the impact it has on the account. To enable this feature, Contact OpenAir Customer Support.

When the feature is enabled, an audit trail icon  next to the setting label indicates that an audit trail is available. Click the Show audit trail icon to display a popup window showing the account number, the name of the company switch, and a history of changes made, when, and by whom.



Audit trail information is available on several forms in Administration > Global settings. These include:

- Account
  - Filter Set Settings
  - Integration: SAML Single Sign-on > [Select a SAML identity provider profile] (Requires the Self-Service SAML Identity Provider Profile Configuration feature).
  - Optional Features
  - Proxy Expirations
  - Security Options
- Display
  - Email Settings
  - Interface: Display

- Interface: Other
- Print Settings
- Regional Settings
- Time Settings
- Organization
  - Approval Options
  - Tax Options
- Reports
  - Reporting Options

## Quick Audit Trail for Custom Fields

The Quick Audit Trail for Custom Fields optional feature lets you keep track of changes made to custom fields directly from the entity form. When the feature is enabled, account administrators and users with the **View quick audit trail for custom fields** role permission can access audit information for custom fields.

Audit information is supported for all custom field types. However, for custom fields of type Text Area, Pick List, Multiple Selection and Allocation Grid, the custom field audit needs to be converted to an extended audit to include the values before and after the update in the audit trail.

Contact OpenAir Customer Support and ask for the Quick Audit Trail for Custom Fields and Custom Field Extended Audit features to be enabled.

### To convert a custom field to an extended audit:

1. Go to Administration > Global Settings > Custom Fields > [select a custom field].
2. Check the **Convert to extended audit** box at the bottom of the form.

Convert to extended audit  
Conversion to extended audit is permanent and cannot be undone

3. Click **Save**.

### To view the audit trail for a custom field:

1. Go to the form, the custom fields is associated with.
2. Locate the custom field on the form and point to the custom field label. A hand cursor appears.
3. Click the field label. A pop-up window displays a history of changes made. Details include the employee who updated the custom field, the date and time as well as the values before (From) and after (To) the update.

The example below shows the custom field used to store authorized IP addresses on the Employee record — refer to [IP Restriction](#).

**Note:** The audit field must be extended if a record of values is required in the audit trail. If the audit field is not extended, the **To** and **From** columns in the audit trail read “CHANGED” instead of the values after and before the update. See the last row in the audit trail example below.

Authorized IP addresses

192.0.2.0/24

Changes to 'Authorized IP addresses'

Employee	Date	To	From
Marc Collins	07/31/19 07:22 AM	192.0.2.0/24	192.0.2.255
Marc Collins	07/31/19 07:21 AM	192.0.2.255	192.0.2.0/24
Marc Collins	07/31/19 07:20 AM	CHANGED	CHANGED


**Note:** Quick audit trail is not available for standard fields on entity forms. You need to run a detail report for the entity and select the audit trail field in the report layout to view any changes made to standard fields for this entity. See [Viewing full audit trail in detail reports](#).

## Data Export for Auditing


Account administrators and users with the **Export data** role permission can export OpenAir data for auditing purpose.

You can export all of your account data or selected tables in MySQL or delimited text format. See [Exporting OpenAir data](#).

You can then process the exported data to extract the desired audit information. See [Using the Exported OpenAir Data for Auditing](#).

 **Note:** If the Automatic Backup Service feature is enabled on your account, you can use the regular backup instead of exporting your account data manually. See [Automatic Backup Service](#).

 **Tip:** Consult the  [Database Guide](#) and OpenAir Data Dictionary for reference when selecting tables for data export and processing the exported data.


 **Note:** To view the OpenAir Data Dictionary, use the following URL: `https://<account-domain>/database/single_user.html`.

- The URL includes the domain name for your OpenAir account <account-domain>. For more information about your account-specific domain name, see the help topic [Your Account URLs](#).
- To view the details of a specific table, append a hash symbol # followed by the table name to the end of the data dictionary URL. For example, use `https://<account-domain>/database/single_user.html#project` to view the details of the Project table.
- You can access the data dictionary from the OpenAir Help Center using the link in the navigation bar if you have the View Help Center role permission.

## Exporting OpenAir data

### To export OpenAir data:

1. Go to Administration Global Settings > Account and click **Integration: Import/Export**.
2. In the Import/Export screen, click the **All data in text format** or **All data in MySQL format** link.
3. **Choose which tables to exclude** — select any tables to exclude from the export.

 **Tip:** If you only want to include a small number of tables, first click Select all to exclude all tables, and then select the tables you want to include.

4. If exporting the data as delimited text:
  - **Text delimiter** — Select comma-delimited, tab-delimited, or a regional setting CSV list separator.
  - **Data layout** — Select whether to include column headings in the exported data.
  - **New line format** — Specify the new line format corresponding to the Operating System on your machine.
  - **Suppress the audit field data** — Check this box if applicable.

**Important:** Do not check the **Suppress the audit field data** box when exporting data for auditing purposes.


5. Click **Export**. A progress bar displays while OpenAir generates a ZIP file containing the generated data.
6. Click the **Click here** link to download the ZIP file with your data.


7. Extract and review the content of the ZIP archive you downloaded. Depending on the format you chose for exporting your data, the ZIP archive will contain:
  - **A MySQL file** — Use this file to import the data into a MySQL database and run queries and reports.
  - **A series of CSV files (one for every table selected for export)** — Use these files to import selected data into a spreadsheet or run scripts to analyze the data.



## Using the Exported OpenAir Data for Auditing

You can use the OpenAir data exported in MySQL or delimited text format to extract auditing information. Review the [User access log](#) and [Deleted records log](#) examples below as well as the [Quick reference for fields/columns commonly use for auditing purposes](#).

See the  [Database Guide](#) and OpenAir Data Dictionary for more detailed information about the data structure, tables and fields available in the OpenAir database.

 **Note:** To view the OpenAir Data Dictionary, use the following URL: `https://<account-domain>/database/single_user.html`.


- The URL includes the domain name for your OpenAir account <account-domain>. For more information about your account-specific domain name, see the help topic [Your Account URLs](#).
- To view the details of a specific table, append a hash symbol # followed by the table name to the end of the data dictionary URL. For example, use `https://<account-domain>/database/single_user.html#project` to view the details of the Project table.
- You can access the data dictionary from the OpenAir Help Center using the link in the navigation bar if you have the View Help Center role permission.

### User access log

You can audit sign-in attempts using the exported OpenAir data.

#### To audit user sign-in attempts using export data:

1. Export the **user\_login** and **user** tables as delimited text. See [Exporting OpenAir data](#).
2. Extract the content of the ZIP archive containing the export data and open `user_login.csv` in a spreadsheet.
3. Review the following fields/columns:
  - **user\_id** — The unique ID of the user attempting to sign in. Cross-references user data in the **user** table.
  - **logintime** — The date and time of the sign-in attempt.
  - **source** — The location the sign-in originated from, typically an IP address.
  - **status** — The status or outcome of the sign-in attempt.
  - **api** — the sign-in mechanism used.

 **Note:** See [Quick reference for fields/columns commonly use for auditing purposes](#) for a detailed description of the **status** and **api** fields, including how to read the value for these fields

### Deleted records log

When a user deletes a record in OpenAir, the record is flagged as deleted and continues to be stored in the database for some time before it is permanently deleted. You can export OpenAir data and query all or selected tables for records with a **deleted** flag.

All tables storing records that can be deleted manually by users in OpenAir include a **deleted** field. This field is blank by default. When a user deletes the record, the value of the **deleted** field is set to **1**. Use the **audit** field to identify who deleted the record and when it was deleted.



**Important:** Records flagged as deleted which have not been updated for more than 180 days are removed permanently from the database according to a routine schedule. See [Data Deletion](#).

## Quick reference for fields/columns commonly use for auditing purposes

Field / Column	Table / CSV File	Description
status	<b>user_login</b>	<p>The status of the sign-in. The value is a status code:</p> <ul style="list-style-type: none"> <li>■ <b>S</b> — Successful</li> <li>■ <b>P</b> — Password incorrect</li> <li>■ <b>I</b> — Inactive user</li> <li>■ <b>L</b> — Locked user</li> <li>■ <b>R</b> — Restricted IP address</li> </ul>
api	<b>user_login</b>	<p>The login mechanism. Possible values:</p> <ul style="list-style-type: none"> <li>■ [empty value] — interactive (non-api) sign-in</li> <li>■ <b>1</b> — XML API sign-in</li> <li>■ <b>2</b> — SOAP API sign-in</li> </ul> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> A user_login entry with api values 1 and 2 is added when the client application uses the <code>Auth</code> (XML API) or <code>login()</code> (SOAP API) for authentication. No entry is recorded when using a OAuth 2.0 access token or client session ID for authentication.</p> <p>A user_login entry with an empty value for api is added when the user authorizes the client application as part of the OAuth2.0 authorization code flow.</p> </div>
mfa_status	<b>user</b>	<p>The user's two-factor authentication (2FA) status. Possible values:</p> <ul style="list-style-type: none"> <li>■ <b>0</b> – 2FA is not required.</li> <li>■ <b>1</b> – 2FA is required and the user must set up 2FA.</li> <li>■ <b>2</b> – 2FA is required and the user has paired an authenticator app with OpenAir.</li> <li>■ <b>7</b> – 2FA is required and the user has completed the 2FA setup.</li> </ul>
audit	Most tables — refer to OpenAir Data Dictionary.	<p>Each audit trail entry is recorded on a separate line in the audit trail field. Each audit trail entry follows a specific format of information delimited by commas. For example:</p> <pre style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> 1   C,2019-07-12 17:25:48,1,1,db_id:146 2   U,2019-07-13 12:40:40,1,1,db_id:146,name,'Collins, Marc',last,'Collins'</pre> <p>The audit trail entry information can be interpreted as follows:</p> <ul style="list-style-type: none"> <li>■ 1st value — Record Created / Updated:</li> </ul>

Field / Column	Table / CSV File	Description
		<ul style="list-style-type: none"> <li>□ <b>C</b> — Created</li> <li>□ <b>U</b> — Updated</li> <li>■ 2nd value — Timestamp. The timestamp may include a unique epoch reference if the modified fields include a custom field with extended audit. See audit_custom_[<i>custom field ID</i>] below.</li> <li>■ 3rd value — ID of the user creating/updating the record. This can be either:                             <ul style="list-style-type: none"> <li>□ <b>user_id</b></li> <li>□ <b>user_id:proxy_id</b> — ID of the signed in user followed by ID of the user for whom the signed in user is proxying in.</li> </ul> </li> <li>■ 4th value — Sign-in mechanism. Possible values:                             <ul style="list-style-type: none"> <li>□ <b>0</b> — User interface</li> <li>□ <b>1</b> — XML API</li> <li>□ <b>2</b> — SOAP API</li> <li>□ <b>3</b> — NetSuite integration</li> <li>□ <b>5</b> — Workday integration</li> <li>□ <b>6</b> — SOAP API via User Scripting</li> <li>□ <b>8</b> — REST API</li> </ul> </li> <li>■ 5th Value — db_id followed by your OpenAir account ID.</li> <li>■ Subsequent values — <b>[field name],[previous value]</b> pairs delimited by commas.                              In the above example, name and last_name were modified when the record was updated, to 'Collins, Marc' and 'Collins' respectively.</li> </ul>
custom_[ <i>custom field ID</i> ]	Table for the entity to which the custom field is associated	Custom fields appear in the database under generic names formed of the prefix 'custom_' followed by the unique ID of the custom field (its ID in the cust_field table).
audit_custom_[ <i>custom field ID</i> ]	Table for the entity to which the custom field is associated	<p>Audit extension fields for custom field of types Text Area, Pick List, Multiple Selection and Allocation Grid, appear in the database under generic names formed of the prefix 'audit_custom_' followed by the unique ID of the custom field (its ID in the cust_field table).</p> <p>For these custom field types, values will not be recorded in the audit trail entry unless the audit is extended. See <a href="#">Quick Audit Trail for Custom Fields</a>.</p> <p>If the audit is not extended, the audit trail entry in the <b>audit</b> field will show 'CHANGED' instead of the previous value for the modified field. For example:</p> <pre>1   U,2019-07-31 07:15:57,2,0,db_id:146,custom_120,CHANGED</pre> <p>If the audit is extended for the custom field, a unique reference is added to the timestamp for the audit trail entry in the <b>audit</b> field. For example:</p> <pre>1   U,2019-07-31 07:21:13 iBICToWz6RG93Kwt9zCm/A==,2,0,db_id:146,cus tom_120,CHANGED</pre>

Field / Column	Table / CSV File	Description
		<p>A similar entry is added to the audit extension field for the custom field and includes the value for the modified custom field. For example:</p> <pre>1   U,2019-07-31 07:21:13 iBICToWz6RG93Kwt9zCm/A==,2,0,db_id:146,cus tom_120,'192.0.2.0/24'</pre>



**Note:** To view the OpenAir Data Dictionary, use the following URL: [https://<account-domain>/database/single\\_user.html](https://<account-domain>/database/single_user.html).

- The URL includes the domain name for your OpenAir account <account-domain>. For more information about your account-specific domain name, see the help topic [Your Account URLs](#).
- To view the details of a specific table, append a hash symbol # followed by the table name to the end of the data dictionary URL. For example, use [https://<account-domain>/database/single\\_user.html#project](https://<account-domain>/database/single_user.html#project) to view the details of the Project table.
- You can access the data dictionary from the OpenAir Help Center using the link in the navigation bar if you have the View Help Center role permission.

## Configuring and Using OpenAir Integrations and Add-on Services

This section summarizes the security considerations for OpenAir integrations and add-on services. For more detailed information, refer to the individual guides for each of these integrations or add-on services.

The following integrations and add-on services are currently supported and covered in this section:

- Add-on services available as desktop or mobile applications — see [Add-on Services — Security Considerations](#). These includes:
  - Desktop applications for account administrators:
    - OpenAir Exchange Manager — enables to send project task assignments, resource bookings, and schedule request calendar commitments from OpenAir to Outlook calendars for all defined users.
    - OpenAir Integration Manager — enables the exchange of data between OpenAir and other applications using CSV text files.
  - Desktop applications for professionals and project managers:
    - OpenAir OffLine — extends your OpenAir access to your personal computer when offline.
    - OpenAir MS Outlook Connector — enables the export of OpenAir calendar items to an Outlook calendar for a single user.
    - OpenAir MS Projects Connector — enables the exchange of project plan information between OpenAir and Microsoft Project.
  - Mobile applications:
    - OpenAir Mobile for Android — enables Timesheets and Expenses entry using a native application on Android mobile devices.

- OpenAir Mobile for iPhone — enables Timesheets and Expenses entry using a native application on iPhone devices.
- OpenAir Business Intelligence Connector — enables access to OpenAir data as an OData V4 data feed from your Business Intelligence tools. See [Business Intelligence Connector — Security Considerations](#).
- OpenAir NetSuite Connector— provides a seamless data flow between OpenAir and NetSuite. See [NetSuite Connector — Security Considerations](#).

## Add-on Services — Security Considerations

This section addresses some general principles applicable to all add-on services application as well as specific considerations for individual applications.

### General principles

Some general principles apply to all OpenAir add-on applications:

#### Keep software up to date

OpenAir releases new versions of currently supported add-on applications from time to time. Download and install the new versions when they become available to take advantage of security updates as well as software fixes, new features and other product enhancements.



**Important:** You should exercise appropriate responsibility and perform regression testing for business-critical applications away from your production environment before upgrading.

Always test new versions of OpenAir Integration Manager in a sandbox environment before upgrading. In particular, test any shortcuts you may have created for processes such as accounting system integrations to verify that they run correctly under the new version of OpenAir Integration Manager.

Service changes impacting infrastructure are communicated to all OpenAir customers. Such service changes may include discontinued development / support and end-of-life for add-on applications. Discuss these changes with your technical teams as they arise to assess the implications and prepare for the change.

#### Download only from trusted OpenAir sources

Download OpenAir add-on applications only from the following sources:

- In OpenAir, go to Administration > Global Settings > Add-on Services.
- Go to the App Store on an iPhone or Play Store on an Android mobile device.
- Use links provided by OpenAir Customer Support, OpenAir Professional Services or in OpenAir documentation.


#### Follow the principle of least privilege

Access to OpenAir add-on services should be granted on a needs basis. Allow users to accomplish their task using the lowest privileges. For example, you may grant users rights to use OpenAir Mobile

applications for time or expenses entry, but grant access to OpenAir Projects Connector to Project Managers only. Other add-on services such as OpenAir Integration Manager should be restricted to trained individual users only.

In OpenAir, go to Administration > Global Settings > Users > Employees > [Select an Employee ID] > Access Control > Exchange Access. to grant or revoke access to an add-on service.

The mention “Not approved for download” appears above the download link in Administration > Global Settings > Account > Integration: Add-on Services if the user has not been granted access to that application. Users can still download and install the application. However, they will not be able to set up and use the application using their OpenAir credentials. See [Access Control Overview](#).

 **Note:** OpenAir Exchange Manager requires Administrator credentials. Access cannot be granted to other users and the application is not listed in the Access Control settings for individual users.

## Connection Settings


All add-on applications need to be configured to connect with your OpenAir account to enable the exchange of data.

The connection settings include:

- **Server** — Enter the URL for your OpenAir account. The server URL includes the domain name for your OpenAir account <account-domain>. For more information about your account-specific domain name, see the help topic [Your Account URLs](#).

 **Important:** Make sure you connect to your OpenAir account over a secure layer using the HTTPS protocol. OpenAir uses the industry standard Transport Layer Security (TLS) protocol to encrypt communication between the OpenAir server and add-on applications, and to ensure the security of the data transferred.


- User credentials (**Company ID, User ID and Password**) — The application will connect successfully to OpenAir only if the user has the relevant access rights allowing them to use the application to access OpenAir data. See [Follow the principle of least privilege](#).
- Remember Password — This option is disabled by default. If enabled, the password will be stored on the device and encrypted using industry standard security measures.

 **Important:** Make sure you have appropriate security policies in place around physical access to devices. If the Remember Password is enabled, anyone with access to your unlocked device will be able to access your Oracle Service account using your Device; a person having access will be able to view, add, and edit information in your Oracle Service account. As a precaution, you should always utilize a passcode lock on your device and change your password regularly. If your device is lost or stolen, you must immediately report the incident to your Oracle account administrator and change your Oracle Service password. By enabling the Remember Password option, you accept full responsibility for any losses and/or damages, and you agree not to hold Oracle or its affiliates liable for any losses and/or damages resulting from saving your password and/or session information.

## OpenAir Access Control

The access control mechanisms configured for the OpenAir web application also apply to add-on service applications. The features and data available depend on a variety of factors such as user settings, role privileges, form permissions and filter sets.

## OpenAir Exchange Manager

See  [Exchange Integration Manager](#) for more information about configuring and using OpenAir Exchange Manager for the integration.

Specific considerations include:

- Access cannot be granted to users other than account administrators. OpenAir Exchange Manager is not listed in the Access Control settings for individual users.
- Configuring the OpenAir MS Exchange integration requires Administrator roles for OpenAir, the Active Directory Domain and MS Exchange Server.
- After OpenAir Exchange Manager is set up, any domain user with read/write access to all users exchange folders can run OpenAir Exchange Engine.
- When configuring access to MS Exchange server - Integration Settings > Exchange Access:
  - Only enable the **Use http** option if the integration is local to the Exchange Server and the Exchange Server is not setup to accept HTTPS traffic.
  - Check the **Override SSL Exceptions** box if the SSL certificate is not signed, or if the domain name used by the integration does not match the domain in the SSL certificate. Again, only enable if the integration is local to the Exchange Server.

## OpenAir Integration Manager

See  [Integration Manager](#) for more information about configuring and using OpenAir Integration Manager.

Specific considerations include:

- Only users who have received training on using OpenAir Integration Manager should have access to the integration. Having an understanding of the OpenAir application and how its database is structured is critical.
- OpenAir Professional Services provide you with a link for downloading OpenAir Integration Manager after you have attended the relevant training.
- Windows user must have full access privileges to the OpenAir Integration Manager installation folder (typically C:\Program Files(x86)\OpenAir\IntegrationManager).
- OpenAir Integration Manager does not support a multi-user setup. The application and Integration Manager shortcuts should be installed, created and launched using the same single Windows account. Running OpenAir Integration Manager from different Windows user accounts can lead to inconsistent application behavior.
- When uninstalling the application, delete the OpenAir Integration Manager installation folder manually to delete the mapping data.

## OpenAir OffLine


See  [OffLine](#) for more information about configuring and using OpenAir OffLine.

Specific considerations include:

- Access to OpenAir OffLine is granted in the Access Control settings for individual users.
- Users access rights and privileges are governed by the access control mechanisms configured in the web application.

- When uninstalling the application, delete the OpenAir OffLine installation folder (typically C:\Program Files(x86)\OpenAir\OffLine) manually to delete the mapping data.

## OpenAir Projects Connector

See  [Projects Connector](#) for more information about configuring and using OpenAir Projects Connector.

Access to OpenAir Projects Connector is granted in the Access Control settings for individual users.

## OpenAir Mobile

Refer to  [OpenAir Mobile 3 User Guide](#) for more information about configuring and using OpenAir Mobile.

Specific considerations include:

- Access to OpenAir Mobile (Android) or OpenAir Mobile (iPhone) is granted in the Access Control settings for individual users.
- OpenAir Mobile uses the OAuth 2.0 authorization framework to access OpenAir data. Users authorize access by signing in to OpenAir on their mobile browser. The OpenAir sign-in page was redesigned and adapted for mobile devices, and users can use biometric authentication if enabled on their device. OAuth 2.0 supports the following authentication mechanisms:
  - Password Authentication by OpenAir — Employees use their OpenAir credentials (company ID, username and password) to connect OpenAir Mobile to OpenAir.
  - SAML Authentication — If SAML authentication is enabled for your account, you can enable employees to sign in using one of the following methods:
    - Service Provider initiated Single Sign-on (SP-initiated SSO).
    - Identity Provider initiated Single Sign-on (IdP-initiated SSO). Users need to close the OpenAir Mobile application and launch OpenAir from their company SSO page before they can access OpenAir Mobile.
- If you use the IP Restriction optional feature to restrict access to the OpenAir account to specific IP addresses, the IP address of the user's device must be in the IP address allowlist for this user for OpenAir Mobile to exchange information with your OpenAir account. If the IP address changes and the new IP address is not in the IP address allowlist for the user, the OpenAir Mobile app can no longer exchange information with your OpenAir account. The OAuth 2.0 access and refresh tokens become invalid at the first attempt to exchange information with your OpenAir account, when the user saves changes or runs the synchronization manually. OpenAir Mobile 4.4.2 or later version shows an error message. Previous versions of the app initiate the authorization process without error message. The user must ensure that the device IP address is authorized before connecting OpenAir Mobile again with your OpenAir account.
- Privileges enabling users to approve timesheets and expenses using OpenAir Mobile apps are granted in the Employee Demographic form in OpenAir.
 


Go to Administration > Global Settings > Users > Employees > [Select an Employee ID] > Demographic and select as applicable:

  - **Enable Approval on mobile for Timesheets** (under Timesheets Options)
  - **Enable Approval on mobile for Expenses** (under Expenses Options)
- Role permissions, form permissions and permission rules defined in OpenAir by account administrators are also enforced in OpenAir Mobile. However, note that for Timesheets, only permission rules and form default values for the main entity form are supported. Permission rules and form default values for the time entry form are not supported.



- Access to Timesheets and Expenses can be disabled separately for mobile applications and the web interface. Contact OpenAir Customer Support and ask for the **Disable Timesheets on Mobile apps** or **Disable Expenses on Mobile apps** internal switches.
- OpenAir uses the industry standard Transport Layer Security (TLS) protocol to encrypt communication between the OpenAir server and the OpenAir Mobile app on your device, and to ensure the security of the data transferred.
- OpenAir Mobile stores data locally on your device. Only the data relevant to the authenticated employees timesheets and expenses is stored. The app always encrypts your data with industry standard encryption.

## Business Intelligence Connector — Security Considerations

See  [Business Intelligence Connector](#) for more information about configuring and using the Business Intelligence Connector feature.


The OpenAir Business Intelligence (BI) Connector feature allows you to access OpenAir data as an OData V4 data feed from other applications without the need to write any code. Contact your OpenAir account manager to enable the Business Intelligence Connector feature on your account.

- The OpenAir OData service follows the same security best practice as OpenAir.
- All data is encrypted in transport using the industry standard transport layer security (TLS) protocol.
- Your published report and list view data is stored securely on OpenAir servers.
- You can remove published resources from the OpenAir OData service at any time.
- You must enter your OpenAir sign-in details to access published resources from your OpenAir OData feed.
- You can only access published resources from the OpenAir OData service if the Business Intelligence Connector feature is enabled for your account and if you have the relevant role permissions.
- Access to your OpenAir OData feed resource data is read-only.
- Data access in the OpenAir OData feed follow the same privileges and restrictions as in OpenAir.
- Administrators can control employees access to the Business Intelligence Connector functionality by role permission:
  - Publish reports
  - Enable publishing of shared reports to OData service with recipient's permission
  - Enable publishing of shared reports to OData service with owner's permissions
  - Publish ListView via OData



**Important:** The Business Intelligence Connector feature does not support authentication using SAML Single Sign-on. Users must sign in using their OpenAir company ID, user ID and password to access their OpenAir OData feed.

## NetSuite Connector — Security Considerations

Refer to  [NetSuite Integration](#) for more information about configuring and using OpenAir NetSuite Connector.

OpenAir NetSuite Connector provides a seamless data flow between OpenAir and NetSuite. Contact OpenAir Customer Support to enable the integration and NetSuite. Contact OpenAir Professional Services to request the configuration of your account for the integration and to obtain detailed instruction for, and assistance with, its implementation.

OpenAir uses the industry standard Transport Layer Security (TLS) protocol to encrypt communication between OpenAir and NetSuite, and to ensure the security of the data transferred.


This section outlines the following security-related configuration settings:

- [Authentication](#)
- [Role Permissions in OpenAir](#)
- [NetSuite Connector Administration Form Access and Safeguard](#)
- [Logging](#)


## Authentication

OpenAir must connect to your NetSuite account to enable the integration. Two authentication methods are supported:

- **Authentication using a custom role in NetSuite** — NetSuite's Two-Factor Authentication feature is not compatible with SuiteTalk (Web Services) or SuiteAnalytics Connect. To use Web Services or SuiteAnalytics Connect, you must be signed in with a role which does not require Two-Factor Authentication. This requires you to create new user account with a custom role created specifically for the integration.

Refer to the  [NetSuite Integration](#) for instructions to create a custom role in NetSuite for the integration under Configuring NetSuite for the Integration > Creating a Custom Role in NetSuite for the Integration.

- **Token-Based Authentication** — Token-based authentication (TBA) is now the only supported authentication method for the OpenAir <> NetSuite integration. TBA's request-level signatures enhances security and TBA lets you use your Two-Factor Authentication role in NetSuite for the integration.

Refer to the  [NetSuite Integration](#) under Configuring NetSuite for the Integration > Creating and Assigning an Access Token for the Integration.

## Role Permissions in OpenAir

Account administrators can assign role permissions for the OpenAir NetSuite integration to ensure employees have the required privileges to accomplish their tasks. See [Roles Overview](#).

The following role permissions are available once the OpenAir NetSuite integration is enabled:

- View the NetSuite integration
- View and run the NetSuite integration
- View and edit the NetSuite integration settings
- Allow employee to export invoices to NetSuite
- Allow employee to export Expense reports to NetSuite
- Allow employee to export project data to NetSuite
- Allow employee to export timesheets to NetSuite
- Allow employee to export recognition transactions to NetSuite
- Allow employee to export purchase requests to NetSuite
- Allow employee to view last NetSuite error on expense reports
- Allow employee to view last NetSuite error on invoices
- Allow employee to view last NetSuite error on timesheets

## NetSuite Connector Administration Form Access and Safeguard

Designated account administrators can control NetSuite Connector administration settings. Effective April 10, 2021 the NetSuite Connector administration form is self-service, instead of controlled by OpenAir Customer Support. Account administrators with the relevant user privilege can save changes to the NetSuite Connector administration form without a password.

### To let an account administrator edit settings on the NetSuite Connector administration form:

1. Contact OpenAir Customer Support and request the NetSuite Connector Administration Form Editor Permission optional feature.
2. In OpenAir, go to Administration > Global settings > Users > [Select an employee] > Demographic.
3. Check the **View and edit NetSuite Connector administration form** box under the Optional features section. This employee demographic setting is only available if the employee is an account administrator or has the "View and edit integration settings" role permission.
4. Click **Save**.



**Important:** Make sure you read the documentation and consider changes carefully before you save the NetSuite Connector administration form. The integration may stop working, or may not work as expected and cause data corruption if configured incorrectly.

An optional feature disables the Save button if there are any active scheduled or real-time integrations configured for your account. This forces authorized account administrators to deactivate all scheduled and real-time integrations before they can make any changes to the NetSuite Connector administration form. To add this additional level of protection, contact OpenAir Customer Support and ask for the following feature: Prevent Saving NetSuite Connector Administration Form if Workflows are Scheduled or Set for Real-Time Integration.

## Logging

The OpenAir NetSuite Connector **Status Screen** lets administrators see the status of any OpenAir + NetSuite integration runs at a glance, including performance statistics.

The OpenAir NetSuite Connector **Settings History** lets administrators see the history of integration configuration changes, including information about what changes were made, when, and by whom.

## Enabling and Controlling Access to OpenAir Platform Tools

### APIs


OpenAir provides the XML API, SOAP API (Web Services), REST API as layers for the exchange of OpenAir data between the main site and peripheral programs. These programs include partnered websites, OpenAir add-on applications that do not need direct database access, and third party applications

indirectly supported through OpenAir. Before you begin using these services, review the best practice guidelines in [Security Considerations for Developers](#). See also [API Best Practice Guidelines](#).


Contact the OpenAir Customer Support or your OpenAir account manager to request API access. See Troubleshooting for instructions. When access is granted, you will receive an API namespace and an API key. These are the two pieces of information required for API access in addition to your regular OpenAir sign-in credentials. The namespace and key attributes are used to verify that the request is coming from a valid partner that has permission to use our API. You will not be able to access an account with just the namespace and the key. You will also need to know the Company ID, User ID, and Password of the account.

Request the **Web Services log detail report** feature to record and report on all web service requests and responses. When this feature is enabled, you will be able to go to Reports > Detail > Web services and select **Web services logs** to configure and run the reports. These reports can be used for auditing purposes or to help troubleshooting API requests.

You can also use web services reports to audit and revoke authorizations granted by OpenAir users to integration applications. For more information, see [Auditing and Managing OAuth 2.0 Authorizations](#).


 **Note:** This feature includes an optional component, which may be enabled to help troubleshoot any issues with the add-on services provided by OpenAir.

If you are using Web services log reports to track your API usage limits, note that API requests made by OpenAir Mobile apps, OpenAir Integration Manager and other OpenAir add-on services do not count toward your usage limits.

 **Important:** The Web services log report feature has the following limitations:

- If you do not use this feature for more than 30 days, the feature is disabled and the log entries are deleted.
- Log entries are retained for 7 days only, then they are purged from the database.

## User Scripting

User scripting features allow you to customize OpenAir to better meet the unique needs of your business. Scripts are stored in a dedicated workspace used exclusively for scripting and can only be altered through the Scripting Center. Before you begin using these features, review the best practice guidelines in [Security Considerations for Developers](#) as well as the  [User Scripting](#).

Contact OpenAir Customer Support to enable the following User Scripting features:

- **Form Scripts** — allows the creation of scripts triggered by events on specific entity forms.
- **Scheduled Scripts** — allows the creation of scripts executed according to a schedule.

The Scripting Center and the built-in script editor — or Scripting Studio — are automatically enabled if either Form Scripts or Scheduled Scripts are enabled. Enabling these features also enable Script deployment reports allowing you to review deployment logs for form and scheduled scripts respectively.

The following optional features are also available for User Scripting.

- **Script support for HTTPS methods**— enables outbound calls using built-in functions in your scripts.
- **Script support for Web Service API methods** — enables access to the SOAP API using built-in functions in your scripts.

- **Unapprove Event** — enables to create scripts that are triggered when items are unapproved. This applies to Timesheets, Schedule requests, Booking requests, Bookings, Purchase requests, Purchase orders, Envelopes and Invoices.

Once user scripting features are enabled, account administrators can access the Scripting Center by going to Administration > Scripting Center and use it to develop, test, deploy and manage scripts for your OpenAir account.

## Platform Role Permissions

Administrators can assign Platform Roles to users to control access to critical features of the Scripting Center and Scripting Studio. You can create Platform Roles by navigating to Administration > Roles. Use platform role permissions to control access to critical features of the Scripting Center and Scripting Studio.

OpenAir recommends creating the following roles:

- Script Administrator
- Script Developer
- Script QA
- Script Deploy

Roles can be assigned a number of role permissions:

- View Scripting Center — allows users to access and view the Scripting Center by navigating to Administration > Scripting Center.
- Create script — allows users to create a new script.
- Change script log level — allows users to set what types of information to log.
- View script in Scripting Studio — allows users to view a script in the Scripting Studio.
- View and modify script in Scripting Studio — allows users to view a script and make changes to it in the Scripting Studio.
- Enable script testing — allows users to move a script to “In testing” status.
- Upload script revision code — allows users to upload new code revisions after a script has been deployed.
- Disable script testing — allows users to move an “In testing” script to “Inactive” status.
- Discard script changes — allows users to discard any script changes made since the last save.
- Deploy new script — allows users to save a new script and move it to “Active” status.
- Deploy script changes — allows users to save changes to an “In testing” script and move it to “Active” status.
- Undeploy script — allows users to move an “Active” script to “In testing” status.
- Delete script — allows users to delete a script.
- Set form script “Execute As Employee” — set an employee for script deployment when running a script under another user.
- Run schedule script test code — allows users to run schedule script test code in either “In testing” or “Active: revising” states.
- Run schedule script code — allows users to run currently deployed script code.
- Cancel schedule script queued runs — allows users to cancel any previously-scheduled runs waiting for processing in the queue.
- View script parameters — allows users to view, create, and modify script parameters.

- View and modify script parameters — allows users to view, create, and modify script parameters.
- Set script parameter value — allows users to use the “Set” link for the script parameter value.
- View solutions — allows users to view solutions, but not edit them.
- View and modify solutions — allows users to view, create, and modify solutions.
- Export solution — allows users to export a solution based on a particular script deployment.
- Upload solution — allows users to upload a solution XML file.
- Apply solution — allows users to create all objects specified in a solution and create a log file.
- Delete solution — allows users to delete a solution, all of its history, and logs.

The table below shows the permissions OpenAir suggest should be assigned to each role:

Permissions	Script Administrator	Script Developer	Script QA	Script Deploy
View Scripting Center	*			
Create script	*	*		
Change script log level	*	*	*	
View script in Scripting Studio	*	*	*	
View and modify script in Scripting Studio	*	*		
Enable script testing	*	*	*	
Upload script revision code	*	*		
Disable script testing	*	*	*	
Discard script changes	*	*		
Deploy new script	*			*
Deploy script changes	*			*
Undeploy script	*			*
Delete script	*	*		
Set form script Execute As User	*			
Run schedule script test code	*	*		
Run schedule script code	*			
Cancel schedule script queued runs	*	*		
View script parameters	*	*	*	
View and modify script parameters	*	*		
Set script parameter value	*	*		*
View solutions	*	*	*	
Create solution	*	*	*	
Upload solution	*	*	*	*

Permissions	Script Administrator	Script Developer	Script QA	Script Deploy
Download solution	*	*	*	*
Apply solution	*	*	*	*
Delete solution	*			





## Script deployment log reports


Administrators have access to deployment logs for form scripts and scheduled scripts in Reports > Detail > Script deployment. These reports allow to view all log messages recorded for all form script deployments and scheduled scripts deployment, respectively. Assign the **View the script deployment log report** role permission to enable other users to view these reports.

# Security Considerations for Developers

OpenAir API integrations and OpenAir scripts must be designed with the security requirements of cloud computing and OpenAir platform best practice guidelines in mind.


Before you start leveraging the XML API, SOAP API (Web Services), REST API, or User Scripting platform tools:

- Ensure your OpenAir account is fully configured and in production.
- Familiarize yourself with the relevant documentation. This includes:
  -  [REST API](#)
  -  [XML API & SOAP API](#)
  -  [User Scripting](#)
  -  [Database](#)
  - OpenAir Data Dictionary

 **Note:** To view the OpenAir Data Dictionary, use the following URL: `https://<account-domain>/database/single_user.html`.

- The URL includes the domain name for your OpenAir account `<account-domain>`. For more information about your account-specific domain name, see the help topic [Your Account URLs](#).
- To view the details of a specific table, append a hash symbol `#` followed by the table name to the end of the data dictionary URL. For example, use `https://<account-domain>/database/single_user.html#project` to view the details of the Project table.
- You can access the data dictionary from the OpenAir Help Center using the link in the navigation bar if you have the View Help Center role permission.

You should work with OpenAir Professional Services to design API integration and platform solutions. The knowledge you gain about how tables and data fields are used in your business processes will save development time and help you optimize your integration and platform solutions on an ongoing basis.

 **Important:** Develop and test your API integration or scripts in a sandbox account. It is crucial that you use a non-production environment until you can be sure that the integration or script runs smoothly without error and does not corrupt vital production data.

This chapter contains considerations for developers using OpenAir as a platform to develop integration applications or to deploy scripts customizing OpenAir functionality. This chapter includes the following sections:

- [Limitations](#)
- [Connecting to the API](#)
- [Roles and Permissions](#)
- [Validate Data Input](#)
- [Programmatic Access to OpenAir Passwords](#)



- [OAuth 2.0 Authorization Code](#)
- [External System Tokens, Passwords and User Credentials](#)
- [Credit Card Information](#)

## Limitations

OpenAir enforces some limitations on platform tools usage to ensure the security and stability of OpenAir:

- For API integrations, there are limits on the number of records and objects any method can accept or return and frequency limits of transactions allowed within a 24-hour or a 60-second interval.
- For user scripting:
  - There are limits on the amount of time scripts can run for, or the amount of Web Services API time they can use, as well as the number of functions a script can call, based on a governance unit system.
  - There are limits on the number of emails a script can send, the number of log entries a script can record.
  - The number of redirects as well as the response time and size are limited for outbound calls.
  - The Web Services API limits apply when accessing the API using built-in user scripting functions.
  - User scripting is prevented from accessing DOM methods, the file system, and sockets.

## Connecting to the API

When access to the API is granted, you will receive an API namespace and an API key. These are the two pieces of information required for API access in addition to your regular OpenAir sign-in credentials. The namespace and key attributes are used to verify that the request is coming from a valid partner that has permission to use our API. You will not be able to access an account with only the namespace and the key. The user credentials including Company ID, User ID, and Password are also required to initiate a session and send request calls to the API.

Connection must be made over a secure layer using the HTTPS protocol. Ensure connections from any integration tools have supported cipher suites enabled. See [TLS Protocol and Cipher Suites](#).

## Roles and Permissions

A secure enterprise application should allow its users to accomplish their tasks using the least possible access to data and lowest possible privileges to perform system tasks. In OpenAir, this is done using a set of access control mechanisms including roles, permissions and filter sets. See [Configuring and Using Access Control](#).

These access control mechanisms grant OpenAir users permissions to the records and privileges they need to perform their work, but restrict access to other records and privileges that are not required for their jobs. As a developer, you should rely on and reuse these access control mechanisms where applicable.

By default, form scripts are executed within the context of the user who is signed in. Therefore, you need to make sure your script can run correctly for any user that may trigger the script:

- When deploying a script, you must select a user to execute the script deployment. This user acts as a proxy, and is needed when the signed in user's access permissions are too restrictive for the script

to run successfully. You can create a dedicated user with minimum possible privileges and gradually add only those permissions required to execute the script successfully. This approach adheres to the security principle of enabling users to perform their tasks using the least possible level of access and privileges.

**Note:** Form scripts are explicitly prevented from being deployed to be executed as Administrators. Make sure you test your scripts as the user selected to execute the script and not as an administrator.

- The user filter sets will be applied unless disabled. If **script support for web service API methods** is enabled on your account, you can use the `NSOA.wsapi.disableFilterSet( [ flag] )` function to enable or disable user filter sets.

The access control model for integration applications (applications that use the XML API or SOAP / Web services API) are also based on the role and filter sets assigned to the authenticated user. You will typically authenticate as an administrator when developing an integration application. The administrator role is convenient because it gives full permissions to access all records and to perform all tasks – something that is vital during development. However, the best practice is to rely on OpenAir's role-based access control model when developing your API integration. When user privileges are too restrictive or too loose, you should create a dedicated user with role permissions and filter sets that are tailored to the specific access requirements of your integration application. The design principles for dedicated users and custom roles should be driven by the following considerations:

- What tasks do the users need to do by using the integration application?
- What is the lowest role level they can have to access data?
- What is the least amount of privileges needed to perform system tasks?

**Note:** An exception to the security best practice of using a non-administrator role is if your integration application needs to perform tasks that can only be accomplished with administrator privileges.

## Validate Data Input

Sanitize all data inputs in your integration applications to avoid data integrity issues or security breaches. Data sanitation includes checking data type, length, ranges, and expected choices. A request must have all of its data sanitized before it is permitted to be processed.

## Programmatic Access to OpenAir Passwords

OpenAir sign-in passwords for existing users cannot be accessed through the browser interface, scripts or APIs. Applications should not be designed based on the assumption that user passwords can be programmatically obtained.

On the Employee record, the password field can be set using APIs only during create and update.

For integration applications, sign-in must be done by prompting the user for passwords either during initial configuration or each time the application is invoked. OpenAir user passwords must be hashed if stored outside of OpenAir for the benefit of easier authentications.

OpenAir supports the OAuth 2.0 authorization code grant type. You can eliminate the need to store OpenAir user sign-in details outside of OpenAir or to prompt users for credentials.


## OAuth 2.0 Authorization Code

OpenAir supports OAuth 2.0, a robust authorization framework. This authorization framework enables client applications to use a token to access OpenAir through the XML API, SOAP API, or REST API. The application accesses the protected resources on behalf of a user who gave an explicit permission for the access. This method eliminates the need for API integrations to store user credentials.

The OAuth 2.0 authorization code grant type eliminates the need to collect or to store OpenAir user sign-in details in your applications.

For more information, see:

- [OAuth 2.0 for Integration Applications Developers](#)
- [OAuth 2.0 Token Based Authentication](#)

 **Note:** OpenAir only supports the OAuth 2.0 authorization code grant type. The REST API supports OAuth 2.0 exclusively for authorization and authentication.

## External System Tokens, Passwords and User Credentials

Tokens, passwords and user credentials for external systems should not be stored in OpenAir in an unencrypted format.

You may create password script parameters to store tokens, passwords and user credentials in an encrypted format. The value is hidden both on the form used to set the parameter value and in the parameters list view. You can use the `NSOA.context.getParameter(name)` function to read the values for specified password parameters in your outbound calling scripts. Only HTTPS URLs are supported for outbound calls to ensure end-to-end secure connections to external systems.

Similarly you may use password custom fields to store tokens, passwords and user credentials in an encrypted format, then use a read request to read the values of these custom fields in your integration applications.

## Credit Card Information

Credit card information must **never** be stored in OpenAir.