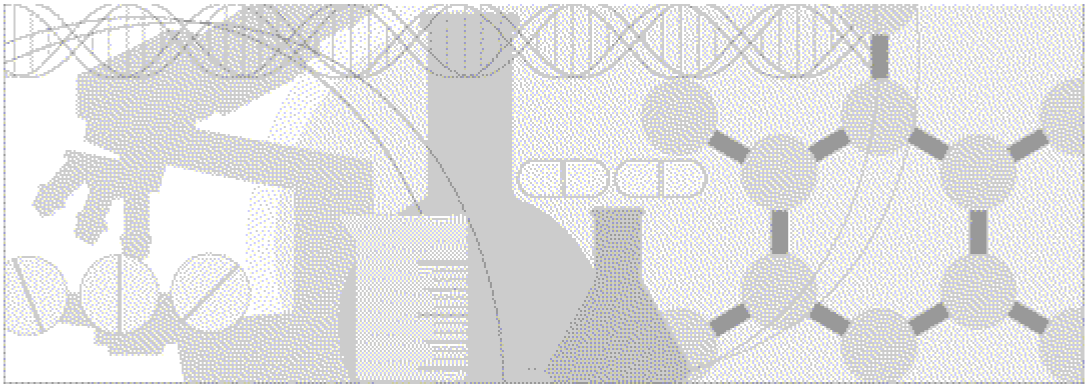
Secure Configuration Guide

Oracle® Health Sciences OutcomeLogix 3.2.2



Part Number: E51131-01

Contents

About this guide

In this preface

Overview of this guide

The *Secure Configuration Guide* provides an overview of the security features provided with the OutcomeLogix application, including general principles of application security. Throughout the *Secure Configuration Guide* are references to chapters in the OutcomeLogix *User Guide* covering how to configure and use the OutcomeLogix application securely.

Audience

This guide is for those who install, configure, or administer the OutcomeLogix application. Detailed procedures for ensuring that only authorized users can access OutcomeLogix functions, view patient information and data, and export data without violating patient privacy appear throughout the *User Guide*.

Related information

Documentation

All documentation is available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com) and the Oracle Technology Network (http://www.oracle.com/technetwork/documentation).

All documents may not be updated for every OutcomeLogix release. Therefore, the version numbers for the documents in a release may differ. For a complete list of the documents in this OutcomeLogix release, their release version numbers, and part numbers, see the *Release Notes*.

Document	Description	Last updated
Release Notes	The *Release Notes* document describes hardware and software requirements and describes the new features, enhancements, and fixed issues in this release.	3.2.2
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available.	3.2.2
User Guide	The *User Guide* provides an overview of the OutcomeLogix application including details on how to navigate through the user interface and how to use the application to accomplish typical tasks you perform while running a late-phase, registry, or observational study. This document is also available from the Documentation CD and the OutcomeLogix user interface.	3.2.2
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the OutcomeLogix application, including general principles of application security. Throughout the *Secure Configuration Guide* are references to chapters in the OutcomeLogix *User Guide* covering how to configure and use the OutcomeLogix application securely.	3.2.2
Standard Data Extracts Guide	The *Standard Data Extracts Guide* contains information about the standard data extract that is available for the OutcomeLogix application, and includes descriptions of the default views for the extract, naming conventions for the views and the columns in the views, and contact information for requesting a standard data extract.	3.2.2
Third Party Licenses and Notices	This document includes licenses and notices for third party technology that may be included in or distributed with the OutcomeLogix software.	3.2.2

If you need assistance

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

CHAPTER 1

Security overview

In this chapter

Application security overview

The Oracle Health Sciences Global Business Unit (HSGBU) organization provides global customer delivery and implementation of OutcomeLogix products through software configuration and custom and standard solutions development. The software configuration methodology is a framework designed by Oracle HSGBU for the planning, management, and delivery of configured software for the use of the customer. OutcomeLogix services documentation, standard operating procedures, work instructions, templates, and forms guide all OutcomeLogix activities.

For more information, visit the Oracle website at www.oracle.com.

General security principles

Require complex and secure passwords

Configure password rules to require a secure level of complexity. For example, a minimum required password length of 9 characters and a maximum required password length of 12 characters require users to create more secure and complex passwords than a minimum required password length of 1 character and a maximum required password length of 4 characters.

Specify the minimum number of characters, and whether the password needs to contain lower-case letters, capital letters, numbers, or special characters. Specify the number of days after which the password expires, as well as any restrictions on whether the password can contain a common word, a name, or any part of the user name.

Keep passwords private and secure

If a patient has limited access to a computer and enrolls at a site, a site user can provide a password for the patient. The patient must change the password after signing in the first time. Patients cannot enter information into the OutcomeLogix application until they change their passwords.

Tell users and patients never to share passwords, write down passwords, or store passwords in files on their computers.

Encourage users and patients to choose password-reset and memorable questions and answers that are easy for them to remember, but difficult for someone else to guess.

Lock computers to protect data

Encourage users entering data to lock computers left unattended.

Provide only the necessary rights to perform an operation

Configure rights and assign roles to users so that they can perform only the tasks necessary for their jobs.

Protect sensitive data

Set up the Patient Profile page to collect only the minimum amount of Personal/Protected Health Information needed for the study. Tell users not to send sensitive information, such as Personal/Protected Health Information or passwords, over email. Provide access to Personal/Protected Health Information only to users who need it for their jobs.

CHAPTER 2

Security features

In this chapter

User security features

Sign-in security

Users and patients must enter their user names and passwords to sign in. If either a user name or password is incorrect, an error message appears but does not tell the user or patient which value is incorrect. Therefore, if someone else is using the account to attempt to sign in, the message does not confirm either a user name or a password.

The application does not allow:

- Duplicate user names.
- Passwords identical to the user ID or user name.
- Passwords identical to dictionary words.
- Passwords consisting of commonly used patterns or combinations such as "welcome1," "12345678," or "football."

Use user-known-only security questions to prevent unauthorized use

When the user signs in for the first time, using the password supplied by Oracle or the study sponsor, the OutcomeLogix application prompts the user to create a new password and select security questions to answer when subsequently changing the password.

If you exceed the number of allowed sign-in attempts, resulting in a locked user account, you can answer security questions to reset your password and unlock your account. The following security-related features are available in the application to control access to some studies:

- Password-reset questions and answers:
  - Not all studies support password-reset questions and answers.
  - An example of a password-reset question is the name of your first school.
  - The Help Desk can view the questions, but only the user or patient knows the answers.
  - Both patients and non-patient users select password-reset questions and provide answers after signing in the first time.
  - To reset a password in the application, a user or patient must provide the correct answers.

  > **Note:** **If the study does not support password-reset questions, the user must call the Help Desk to reset the user password.**

- Memorable date:
  - The Help Desk can view the memorable date.
  - Both users and patients select a memorable date after signing in the first time.
  - To reset a password in the application, a user or patient must provide the correct date to the Help Desk.

For more information, see the chapter on OutcomeLogix basics in the *User Guide*.

Limit sign-in attempts

Each study allows the user a defined number of attempts to sign in correctly. The application locks the user out if the user exceeds that number.

If a session expires after the timeout interval specified for a study is exceeded, the application prompts the user to re-enter the user name and password. The user or patient can sign in and continue working on the form without losing data.

If a user exceeds the number of allowed sign-in attempts, the application locks the user account. An automatically locked account is unlocked after a certain interval, defined at the study configuration level.

For more information, see the chapter on OutcomeLogix basics in the *User Guide*.

Establish password rules that users must follow

A password rule defines the formatting, entry, and reuse requirements for passwords. When you assign a password rule to a role, the passwords of all users who are assigned to that role must conform to its requirements. By creating multiple password rules, you can apply different levels of security to different roles. The default password rule is applied to all roles without an explicitly assigned password rule.

You can define the following formatting, entry, and reuse requirements:

- The minimum and maximum length of passwords.
- Whether the password must include a number.
- Whether the password must include a lower-case letter.
- Whether the password must include a capital letter.
- Whether the password must include a nonalphanumeric character.
- Number of previous passwords that cannot be reused.
- Number of consecutive failed sign-in attempts allowed.
- Whether users must change their passwords after signing in the first time.
- Number of days before the password expires.

For more information, see the chapter on password rules in the *User Guide*.

Set passwords for new patients

When you create a patient who has provided an email address, the patient receives an email containing a link to an application webpage, where the patient specifies a password.

If a patient has limited access to a computer and enrolls at a site, a site user can provide a password to the patient. Patients must change the password when they first sign in. Patients cannot enter any information into the OutcomeLogix application until they change their passwords.

If patients forget their passwords, a user with the appropriate rights can reset the passwords.

> **Note: When you reset a password, the new password does not appear in the profile. When you set a temporary password, the new password appears in the profile and the password must be changed immediately.**

For more information, see the chapter on patients in the *User Guide*.

Application security features

Study configuration levels

The OutcomeLogix application is highly configurable. Configuration options are available:

- **During study design**—Sponsors can work with their Oracle project managers to configure many settings. For example, the columns to include on the Patient List page or when a new patient is required to sign the Informed Consent Document.
- **After study deployment**—Sponsors can work with their Oracle project managers to further refine study settings.
- **After study deployment with built-in administrative functions**—Built-in administrative functions cover the most frequently used configuration changes; for example, the number of password-reset questions and how many minutes before the session times out. You perform these changes in real time; no coding is required.

Security-related configuration settings

The table below describes some of the security-related configuration changes that the OutcomeLogix application supports.

Configuration change	Description
Auto unlock interval	Changes the number of minutes that must pass before the OutcomeLogix application automatically unlocks a locked user or patient.
Initial password assigned to users	Changes the password that the application sends to users and patients to enable them to sign in for the first time. **Note:** If study designers specify a default initial password, all new users and patients automatically receive that password on creation. For security reasons, it is recommended that study designers leave the Initial password assigned to users field blank. That way, upon user creation, the new user receives a unique temporary password by email.
Password string	Changes the masking characters displayed in the Password fields.
Session timeout	Changes the number of idle minutes before a user session times out.
Force session timeout	Changes whether a session can be forced to time out even if the user is active.
Second password reset question	Changes the number of reset questions on the Reset Password page so that users need to answer two questions before the password is reset.
Link expiration day	Changes the length of time a new user has to sign into the OutcomeLogix application for the first time after receiving a user name and password.

Configuration change	Description
Showing patient profile core data	Indicates whether to show the core fields from the patient profile, such as email address, memorable date, reset password, and user name.
Hide, mask, or make a form, or items within a form, read-only for selected roles	Hidden items do not appear in the audit trail and are not included in reports. Masked items make Personal/Protected Health Information unreadable. Read-only items may not be edited.
Assign access to standard reports to roles	Allows users to access specific standard reports.
Password rules	Sets password parameters for selected roles, including time before expiration and the password default rule.
Rights groups	Creates a role and an associated rights group consisting of selected management and user functions.
Activate or deactivate a site	Changes the status of the site.

For more information, see the chapter on study configuration and preferences in the *User Guide*.

Roles and rights

Roles are labels for typical site and sponsor users. Rights grant permission to perform specific activities in the application. Rights and users are assigned to roles. Users with administrative rights assign users to roles when they create users or when they edit user profiles. The ability of the user to perform a particular function depends on the role the user has been assigned to and the rights associated with that role.

The OutcomeLogix application comes with a predefined set of roles, which are configurable in the OutcomeLogix user interface, and rights, which are also predefined for the study and are not configurable in the OutcomeLogix user interface. The user can, however, modify the rights assigned to the predefined roles.

The rights assigned to a role form a rights group, which is assigned to all the users assigned to the role.

For more information, see the chapter on roles and rights in the *User Guide*.

Require appropriate rights to enter data into forms

Federal regulations and data protection laws in different countries require that access to personal information be restricted. Access to patient confidential information is also restricted. Therefore, studies are set up so that only specific users, such as investigators, clinical research coordinators, and patients, can enter patient data.

- **Site users**—A site user enters information into the OutcomeLogix application based on data obtained from patient visits to a clinical site. Site users can be investigators, nurses, Clinical Research Coordinators (CRCs), or clinical technicians.
- **Patients**—A patient signs into the study website and answers questions. The answers are entered into the OutcomeLogix application as patient diaries, which can be viewed by site users with the appropriate rights.

For more information, see the chapter on roles and rights in the *User Guide*.

Assign users to the sites they can access

A site is the location where users collect study-related information. Sponsor users, such as medical monitors and clinical data managers, review the information and issue queries. Site users, such as investigators and clinical research coordinators, answer the queries and sign off on the items, forms, visits, and patients. Sponsor representatives then use the information to generate reports for publication or to fulfill regulatory requirements.

Users with administrative rights can add a user to individual sites or all sites, including new sites that are added to the study. Users can work only with patient and visit data collected at their assigned sites. For example, an investigator who works at only one site is assigned to that site and has access to the data for only that site. A medical monitor who has to review data across several sites is assigned to those specific sites and can see only data for those sites.

When a user is assigned to a site, the data that a user can view and edit is determined by the role to which the user is assigned.

For more information, see the chapter on sites in the *User Guide*.

Restrict access to the application

Users and patients are managed separately. You can restrict access to the application in the following ways:

- **Deactivate a user**—Typically, you deactivate users who leave the organization. Deactivated users cannot sign in and do not receive notifications. All users, including deactivated users, remain in the study for audit purposes.
- **Discontinue a patient**—Enrolled patients may choose to stop participating in a study at any time. When a patient decides to stop participating, a user with the appropriate rights can discontinue the patient. You might discontinue a patient for other reasons, such as noncompliance with the study protocol. Discontinued patients are deactivated, cannot sign in, and do not receive notifications. The audit trail reflects the reason for discontinuing the patient. You cannot re-activate a discontinued patient.
- **Lock a user**—Typically, a member of the Help Desk locks a user account when the Help Desk member suspects that an unauthorized user is trying to sign in. After you lock a user account, you must manually unlock the user before the user can work in the application.
- **Lock a patient**—Before you can lock or unlock a patient, the patient must be assigned to a site to which you are also assigned. After you lock an account, you must manually unlock it before the patient can work in the application.

For more information, see the chapters on patients and users in the *User Guide*.

Be aware of the OutcomeLogix hierarchy

A hierarchical relationship exists between the major components of the OutcomeLogix application, and this affects most actions you perform.

You can perform actions at each hierarchical level. The actions you perform at a higher level impact the lower levels. For example, locking a patient locks all of the visits and forms for the patient, even though you did not lock the visits and forms individually.

For more information, see the chapter on OutcomeLogix basics in the *User Guide*.

Data security features

Encrypt and restrict viewing of Personal/Protected Health Information

All Personal/Protected Health Information that is stored in the database is encrypted.

If the study is designed to contain Personal/Protected Health Information, and designers and sponsors choose to encrypt it, they have the ability to indicate which items on forms contain sensitive information that should be encrypted and also excluded from email messages, data exports, and reports by default.

You can use roles and rights to restrict the users that can view Personal/Protected Health Information that appears in patient profiles.

Access to patient confidential information is also restricted. Therefore, your study is set up so that only specific users, such as investigators, clinical research coordinators, and patients, can enter patient data.

For more information, see the chapter on OutcomeLogix basics in the *User Guide*.

Use display overrides

You can restrict access to items for users in a specific role by using study display overrides. The display overrides are hidden, read-only, and masked (displayed, but blocked out). When a user within the restricted role signs in, the OutcomeLogix application hides or masks the item or makes the item read-only, depending on the setting.

Display overrides on a repeating form apply to each instance of the form unless overridden by validation rules.

For more information, see the chapter on study configuration and preferences in the *User Guide*.

Freeze and unfreeze data on the patient, visit, form or item level

A user with the appropriate rights can freeze or unfreeze patients, visits, forms, and items with any status except Locked. Freezing prevents changes in data—either temporarily, during a study, or permanently, at the end of a study. Updates can occur, however, via automatic or manual queries.

For more information, regarding freezing and unfreezing data, see the chapter on visits and forms in the *User Guide*.

Lock and unlock data on the patient, visit, form or item level

A user with the appropriate rights can lock or unlock patients, visits, forms, and items. Locking, like freezing, prevents changes in data—either temporarily, during a study, or permanently, at the end of a study. Locked patients, visits, and forms cannot be signed.

For more information, see the chapter on visits and forms in the *User Guide*.

Manage electronic signatures

According to 21 CFR Part 11, which regulates electronic records and electronic signatures, each electronic signature must be unique to one individual and cannot be reused by, or reassigned to, anyone else. The OutcomeLogix application authenticates each user and patient signature, comprising a user name and password, to ensure that each is unique and associated with a valid account.

For more information, see the chapter on visits and forms in the *User Guide*.

View audit trails and history

Changes to most fields for a site, user, or patient are audited and are viewable in the audit trail. The audit trails for visits and forms are accessible to users at all times. The Audit Trail button (**A**) appears on every page. The audit trail for a visit or form includes the signing history of that visit or form.

Most audit trails include the person who made the change, the date and time of the change, and the change itself. Sensitive data can be masked. You cannot modify data in an audit trail.

The OutcomeLogix application also allows users to view the history of a query or the call center history of a patient, as well as generate standard and ad hoc reports.

For more information, see the chapters on patients, sites, and users in the *User Guide*.