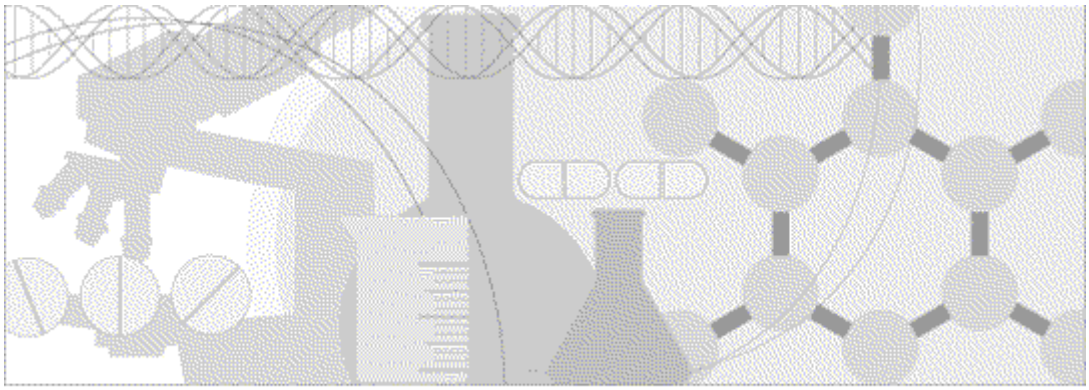
Secure Configuration Guide

Clintrial™ 4.7.1



ORACLE

Part Number: E27581-01

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 Clintrial application, including details about the general principles of application security, and how to install, configure, and use the Clintrial application securely.

Audience

This guide is for users who install and configure the Clintrial application.

Related information

Clintrial 4.7 documentation

The Clintrial 4.7.1 documentation includes the documents in the following table. All documentation is available from the Download Center (https://extranet.phaseforward.com) and the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

Title	Description
Release Notes	The *Release Notes* document describes enhancements introduced and problems fixed in the current release, upgrade considerations, release history, and other late-breaking information.
Known Issues	The *Known Issues* document provides detailed information about the known issues in this release, along with workarounds, if available. **Note:** The most current list of known issues is available on the Extranet. To sign in to the Extranet, go to https://extranet.phaseforward.com.
Getting Started	The *Getting Started* guide: • Provides a summary of each Clintrial module, a description of the relationships between modules, and descriptions of key concepts. • Describes how to install, upgrade, and de-install the Clintrial software. • Describes how to configure the Clintrial application. • Provides information and procedures for customizing the Windows Registry. • Explains how to use the Medika Sample Studies.
Admin and Design	The *Admin and Design* guide describes how to use: • The Admin module to work with user accounts, access rights, parameters, and system administration tools. • The Design module to set up and maintain Clintrial application objects, such as protocols, panels, and study books.
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Clintrial application including details about the general principles of application security, as well as how to install, configure, and use the Clintrial application securely.

Title	Description
Reference Guide	The *Reference Guide* provides: • Definitions of the Oracle database tables that store Clintrial metadata and clinical data. • Descriptions of the use of PL/SQL for Clintrial-specific procedures. • Explanations of data types and naming conventions. • Information on using SQL, setting up custom menus, and running batch jobs. • A glossary of terms.
Manage, Classify, and Lab Loader	The *Manage, Classify, and Lab Loader* guide describes how to use: • The Manage module to perform data management tasks such as coding (including integration with Central Coding), global modification, validation, auditing, and batch loading of clinical data. • The Classify module to track, review and solve for values that fail automatic coding; to audit the contents of a coding thesaurus protocol; and to build and test effective thesaurus algorithms. • The Lab Loader module to batch load laboratory data and to set up Lab Loader objects.
Enter, Resolve, and Retrieve	The *Enter, Resolve, and Retrieve* guide describes how to use: • The Enter module to enroll subjects, enter and edit data, verify data, and work with reports. • The Resolve module to identify, track, and report data discrepancies, as well as how to customize the Resolve module, including writing rules that reference data items. • The Retrieve module to extract clinical data from the database and work with query results.
Multisite	The *Multisite* guide describes: • How to distribute codelists and protocols. • How to set up a replication environment. • How other Clintrial modules work differently in a Multisite environment.
Quick Reference for Enter	The *Quick Reference for Enter* lists Enter module menu commands and shortcut keys.

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 visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

CHAPTER 1

Security overview

In this chapter

Application security overview

Installation

- Create system user accounts and passwords.
- Verify the Oracle database password used for installation of the software.

Post-installation

- Create user accounts and usergroups.
- Assign access rights and access levels.
- Assign panel access rights.
- Set system parameters.

To ensure security in the Clintrial application, carefully configure all areas of the application that have security implications. These areas, and the types of configuration required include:

- Admin
  - User passwords.
  - Access levels.
  - Access rights.
    - Protocol access rights.
    - Non-protocol access rights.
    - Panel access rights. <<Check this out in Design.>>
- Design
  - Panel security.
- Multisite (if applicable)
  - Distribution passwords.
  - Proxy account passwords.
  - Protocol and System account passwords.

General security principles

Require complex and secure passwords

Each password should meet the following requirements:

- Contains a minimum of 8 characters.
- Contains at least one upper case character, and at least one number or special character.
- Expires after 90 days.
- Does not contain a common word, name, or any part of the user name.

For more information, see *Configure strong user passwords* (on page 7).

Keep passwords private and secure

- Users cannot enter information into the Clintrial application until they change their initial passwords.
- Tell users never to share passwords, write down passwords, or store passwords in files on their computers.
- Encourage users to choose a password that is 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. For more information, see *Login security* (on page 10).

Provide only the necessary rights and access to perform an operation

Assign rights to users so that they can perform only the tasks necessary for their jobs. For more information, see *Rights assigned to usergroups* (on page 16), *Users assigned to usergroups* (on page 17), and *Users assigned to protocols* (on page 17).

Protect sensitive data

- Collect the minimum amount of sensitive data needed.
- Tell users not to send sensitive information over email.
- Provide access to sensitive data only to users who need it for their jobs.

CHAPTER 2

Secure installation and configuration

In this chapter

Installation overview

Use the information in this chapter to ensure the Clintrial application is installed and configured securely. For information about installing and configuring the Clintrial application, see the *Getting Started* guide.

Configure strong database passwords

Non-user password accounts, such as the system accounts, are created as you install the Clintrial software. One of the accounts created is a system database administrator. Only a system database administrator can perform the Clintrial software installation.

As you install the Clintrial software, you create system accounts and assign passwords to them. You also create system passwords to Multisite links as the module is installed. All these passwords use the Oracle database DEFAULT profile. System accounts are automatically encrypted as they are created during installation.

Oracle database profiles also can be the basis for creating Clintrial users and usergroups. These accounts may be augmented by manually assigning protocol and non-protocol access rights.

Ensure all your database passwords are strong passwords.

Network security considerations for installers

The Clintrial application may be used with:

- The Oracle Central Coding application to code items.
- The Oracle CIS application to transfer data to and from the Oracle InForm application.

In general, Clintrial uses SQL.Net for communication between the Clintrial client and the server, as well as for CIS communications.

Communications between Clintrial and Central Coding use SQL.Net and IP through the Oracle UTL_HTTP package. For HTTPS communications with Central Coding, SSL is used.

For more information on configuring the Clintrial application for use with these applications, see the *Getting Started* guide. For more information on configuring the Central Coding application to work with the Clintrial application, or on configuring network devices to work with the Central Coding application, see the *Central Coding Installation Guide*.

For more information on configuring the CIS application to work with the Clintrial application, or on configuring network devices to work with the CIS application, see the *CIS Installation Guide*.

Post installation configuration

Configure strong user passwords

In general, rules that govern passwords are created when you install the Oracle database. However, you can further refine password requirements by setting Clintrial system parameters. For example, the system parameter PASSWORD_MINIMUM sets the minimum password length for all Clintrial software users. The Oracle recommendation of a minimum required password length of 8 characters and a maximum required password length of 12 characters requires users to create more secure and complex passwords than a minimum required password length of 1 character and maximum required password length of 4 characters.

Oracle database password rules are applied to all users and usergroups sharing the same profiles and system parameters.

For more information, see *Password rules for user and usergroup security* (on page 10).

Restrict access to panels during the protocol design process

A panel is a Clintrial software object that groups together a set of logically or clinically related items as viewed on a page by a data-entry person during protocol design.

Protocol designers create Protocol access rights for all panels in a protocol. In some cases the designer may want to limit access rights to certain panels. Access to a panel that has the **Protected** attribute set is limited.

For more information, see the Design section in the *Admin and Design* guide and the *Design Help*.

CHAPTER 3

Security features

In this chapter

User security features

Login security

Users must enter their usernames and passwords to log in. The application does not allow duplicate user names.

If either a username or password is incorrect, an error message appears, but does not tell the user the value that is incorrect. Therefore, if someone else is using the account to attempt to log in, the message does not confirm either a username or password.

Password rules for user and usergroup security

Passwords are defined in Clintrial on different levels:

- When you install the Oracle database, you configure security parameters which affect passwords for all database users, whether or not they are also Clintrial users. You do this using profiles. These parameters can be set for both usergroups and users. For more information, see the *Oracle Database Security Guide*.
- These are examples of parameters that may be assigned when installing the Oracle database software or through the Clintrial software:
    - Number of previous passwords that cannot be reused. Oracle recommends **10**.
    - Number of login attempts allowed. Oracle recommends **5**.
    - How long a user will be locked out if he exceeds the configured number of login attempts. Oracle recommends **15 - 30 minutes**.
    - Whether users must change their passwords after logging in the first time. Oracle recommends **Yes**.
    - Minimum and maximum length of passwords that must conform to the Password Minimum parameter. Oracle recommends no less than 8 characters.
    - Whether passwords are encrypted. Oracle recommends **Yes**.
    - Number of days before the password expires. Oracle recommends no more than **90 days**.
- After you install the Clintrial software, you set system parameters. System parameters define characteristics of the work environment for all users of an Oracle database instance to which the users connect through the Clintrial software. An example of a system parameter that affects security and can only be addressed in the Clintrial software is whether audit security is enabled. (Oracle recommends **Yes**.)
- When you create Clintrial users and usergroups, you can supplement or over-rule the password configuration that covers all the Oracle database users. This is done by assigning system parameters that are accessible from the Clintrial Admin module. Usergroups also may be assigned these parameters, and even they may be over-ruled by individual user parameters.

No data loss after a session inactivity time-out

The application requires users to re-enter their user names and passwords after a defined period of inactivity. The user can log in and continue working without losing data.

Create a verify function to ensure that passwords meet security standards

You can create a password verification function to ensure that passwords meet the standards contained in the Clintrial system parameters or a database profile. This function can be assigned in the Clintrial application using the Admin system parameters, or be part of an Oracle database profile created for users or usergroups.

The *Oracle Database Security Guide* describes a method for enforcing password complexity for database user accounts. Briefly, the database administrator creates a password verification function and associates it with a user profile. In the Clintrial application, you also can associate the function using the system parameter in the Admin module. The sample given in the *Oracle Database Security Guide* associates this function with the DEFAULT profile. However, there are special considerations when applying this methodology to Clintrial.

- Non-user accounts, such as system accounts and the accounts for each protocol, use the DEFAULT database profile. The passwords are assigned during installation or upgrade, and encrypted. The resulting encrypted password strings are not constrained to specific characters, and therefore you cannot expect any verification function which relies on character comparisons, such as checking for the existence of at least one number and one non-number to work correctly. For that reason, Oracle strongly suggests that you do not add a verification function to the DEFAULT profile.
- In the case where the Clintrial PASSWORD_ENCRYPTION system parameter is set to No in the Admin module, an encryption verification function can be created and assigned using the Admin module. At least one additional profile must be created for use with Clintrial users, and that profile also can be associated with the verification function. For example, the below command creates a new profile. When creating users in Admin, you should create a profile like the below example and set additional profile limits like those in the DEFAULT profile:

  CREATE PROFILE CT_USER_PROFILE LIMIT PASSWORD_VERIFY_FUNCTION <function_name>;
- In the case where the PASSWORD_ENCRYPTION system parameter is set to Yes, the verification function should not be associated with any profiles which are used for Clintrial users in the Admin module system parameters. Similar to the Protocol account case, the encrypted passwords would not function as expected.

This new system parameter that has been added (PASSWORD_VFY_FUNC) allows the Administrator to specify the name of a password verification function which will be called from Clintrial before the encryption of the password. The function is applied to all Clintrial users created in Admin during creation of the users as well as modification of the password by either the Administrator or the user.

The function must have the same parameters as described in the Oracle database documentation. It does not have to be installed into the **SYS** account. The value of the system parameter should specify the owner and function name, for example, **SYS.CT_VFY_FUNC**. Additionally, execute privileges on this function must be granted to the system account **CTPROC**, using this command:

Grant execute on <function_name> to CTPROC;

For the Clintrial system account **CTSYS**, the function cannot be defined and called until after core server installation has succeeded, so the initial **CTSYS** password supplied during installation is not checked in this way.

Example verify function

```
CREATE OR REPLACE FUNCTION verify_function_11G_1
(username varchar2,
  password varchar2,
  old_password varchar2)
  RETURN boolean IS
   n boolean;
   m integer;
   differ integer;
   isdigit boolean;
   ischar  boolean;
   ispunct boolean;
   db_name varchar2(40);
   digitarray varchar2(20);
   punctarray varchar2(25);
   chararray varchar2(52);
   i_char varchar2(10);
   simple_password varchar2(10);
   reverse_user varchar2(32);

BEGIN
   digitarray:= '0123456789';
   chararray:= 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';

   -- Check for the minimum length of the password
   IF length(password) < 8 THEN
      raise_application_error(-20001, 'Password length less than 8');
   END IF;

   -- Check if the password is same as the username or username(1-100)
   IF NLS_LOWER(password) = NLS_LOWER(username) THEN
     raise_application_error(-20002, 'Password same as or similar to user');
   END IF;
   FOR i IN 1..100 LOOP
      i_char := to_char(i);
      if NLS_LOWER(username)|| i_char = NLS_LOWER(password) THEN
        raise_application_error(-20005, 'Password same as or similar to user
name ');
      END IF;
    END LOOP;

   -- Check if the password is same as the username reversed

   FOR i in REVERSE 1..length(username) LOOP
     reverse_user := reverse_user || substr(username, i, 1);
   END LOOP;
   IF NLS_LOWER(password) = NLS_LOWER(reverse_user) THEN
     raise_application_error(-20003, 'Password same as username reversed');
   END IF;

   -- Check if the password is the same as server name and or servername(1-100)
   select name into db_name from sys.v$database;
   if NLS_LOWER(db_name) = NLS_LOWER(password) THEN
      raise_application_error(-20004, 'Password same as or similar to server
name');
   END IF;
   FOR i IN 1..100 LOOP
      i_char := to_char(i);
      if NLS_LOWER(db_name)|| i_char = NLS_LOWER(password) THEN
        raise_application_error(-20005, 'Password same as or similar to server
name ');
      END IF;
    END LOOP;
```

```
   -- Check if the password is too simple. A dictionary of words may be
   -- maintained and a check may be made so as not to allow the words
   -- that are too simple for the password.
   IF NLS_LOWER(password) IN ('welcome1', 'database1', 'account1', 'user1234',
'password1', 'oracle123', 'computer1', 'abcdefg1', 'change_on_install') THEN
      raise_application_error(-20006, 'Password too simple');
   END IF;

   -- Check if the password is the same as oracle (1-100)
    simple_password := 'oracle';
    FOR i IN 1..100 LOOP
      i_char := to_char(i);
      if simple_password || i_char = NLS_LOWER(password) THEN
        raise_application_error(-20007, 'Password too simple ');
      END IF;
    END LOOP;

   -- Check if the password contains at least one letter, one digit
   -- 1. Check for the digit
   isdigit:=FALSE;
   m := length(password);
   FOR i IN 1..10 LOOP
      FOR j IN 1..m LOOP
         IF substr(password,j,1) = substr(digitarray,i,1) THEN
            isdigit:=TRUE;
             GOTO findchar;
         END IF;
      END LOOP;
   END LOOP;

   IF isdigit = FALSE THEN
      raise_application_error(-20008, 'Password must contain at least one
digit, one character');
   END IF;
   -- 2. Check for the character
   <<findchar>>
   ischar:=FALSE;
   FOR i IN 1..length(chararray) LOOP
      FOR j IN 1..m LOOP
         IF substr(password,j,1) = substr(chararray,i,1) THEN
            ischar:=TRUE;
             GOTO endsearch;
         END IF;
      END LOOP;
   END LOOP;
   IF ischar = FALSE THEN
      raise_application_error(-20009, 'Password must contain at least one \
              digit, and one character');
   END IF;

   <<endsearch>>
   -- Check if the password differs from the previous password by at least
   -- 3 letters
   IF old_password IS NOT NULL THEN
     differ := length(old_password) - length(password);

     differ := abs(differ);
     IF differ < 3 THEN
       IF length(password) < length(old_password) THEN
         m := length(password);
       ELSE
         m := length(old_password);
       END IF;

       FOR i IN 1..m LOOP
         IF substr(password,i,1) != substr(old_password,i,1) THEN
```

```
            differ := differ + 1;
          END IF;
        END LOOP;

        IF differ < 3 THEN
          raise_application_error(-20011, 'Password should differ from the \
             old password by at least 3 characters');
        END IF;
      END IF;
    END IF;
    -- Everything is fine; return TRUE ;
    RETURN(TRUE);
END;
/
CREATE PROFILE CT_USER_PROFILE1 LIMIT PASSWORD_VERIFY_FUNCTION
verify_function_11G_1;
/
```

Application security features

Access rights and levels

An *access right* is a predefined set of Clintrial application activities that can be associated with a usergroup or a user. You define an *access level* for each access right for each usergroup or user.

An *access level* determines what the user can do within the activity. These levels are:

- Full
- Read
- None
- NoDelete
- Publish
- Write
- Basic

Access rights can be granted for both protocols and Clintrial application modules.

Protocol access rights

Protocol access rights relate to activities that require access to protocols and must be associated with a protocol as well as with a usergroup or user.

Non-protocol access rights

A *non-protocol* access right, which is associated with a usergroup or user, pertains to Clintrial application activities that do not require access to a particular protocol. Examples of non-protocol access rights are codelist creation and modification in the Design module and setting parameters in the Admin module.

Rights assigned to usergroups

The Clintrial application comes with a predefined set of rights, that are not configurable. The list of available rights is the same in every protocol.

Rights grant access to different parts of the application or to protocols. Entire parts of the application are hidden when users do not have the rights to work in those areas.

You can change the access rights that are assigned to each usergroup or user to suit the needs of your organization or individual protocol.

Users assigned to usergroups

After you review the rights that are assigned to usergroups and make any necessary changes, you can assign users to usergroups. A user assigned to a usergroup has the rights that are granted to that usergroup. Changes to a usergroup are immediately applied to all users assigned to the usergroup.

Rights can be further tailored at the user lever.

Users assigned to protocols

Users can view patient and visit information only for the protocols to which they or their usergroups are assigned.

Restricted access to the application

You can restrict the access of current users to the Clintrial application by manually revoking access rights to the application from the Admin module. This effectively locks out users. Typically, a Clintrial Admin revokes access rights to the application for a user when the user leaves the organization or if it is suspected that an unauthorized user is trying to log in. After you revoke the application access rights, you must regrant the user access rights to the application before the user can work again in the application. All users, including users without application access rights, remain in the system for audit purposes. They cannot be deleted.

For more information, see the *Admin and Design* guide.

Restricted viewing of Protected Health Information

You can use access rights to restrict the users that can view Protected Health Information by specifying the protocols to which users have access.

You can also protect certain panels during the design function. Users without access to protected panels do not see the information entered in the panels.

Audit and Security Reports

The Clintrial application provides the below access audit reports. You choose these reports from the **Audit** menu in the Admin module. The reports show changes made since the installation or upgrade to Clintrial 4.7.

- User Audit Report—Shows the history of the creation, modification or deletion of user accounts.
- User Access Audit Report—Shows the history of the modification of user Protocol and Non-Protocol access rights.
- Usergroup Audit Report—Shows the creation date of the usergroups and the history of the addition and removal of user accounts.
- Usergroup Access Audit Report—Shows the history of the modification of usergroup Protocol and Non-Protocol access rights.
- Protocol Access Audit Report—Shows the history of the modification of user or usergroup protocol access rights.
- Panel Access Audit Report—Shows the history of the modification of user or usergroup protected access rights.

The Clintrial application provides the below access rights reports. You choose these reports from the **Security** menu in the Admin module. The reports show changes made since the installation or upgrade to Clintrial 4.7.

- Protocol Access Rights Report—Provides a listing of user and usergroup protocol access rights.
- Non-Protocol Access Rights Report—Provides a listing of user or usergroup non-protocol access rights.
- Panel Access Rights Report—Provides a listing of user or usergroup panel access rights.

Panel security

Protocol access rights are for all panels in a protocol. In some cases the designer may want to limit access rights to certain panels. Access to a panel that has the Protected attribute set is limited. A user or usergroup with the following protocol access rights cannot exercise these rights in a protected panel, unless specifically authorized in the Admin module:

- Enter—Merged or Unmerged data. (Access to the update table or to the data tables.)
- Retrieve—Merged or Unmerged data. (Access to the update table or to the data tables.)
- Manage—Coding, Global and Other.
- Resolve—Create, Propose, Manage and Produce.
- Lab Loader—Design and Transfer.

By default, each of these access rights has the access level **None** if the panel is protected. You can override the default and allow these access rights in the same way that you allow access rights for users and usergroups for the protocol in the Admin module.

Multisite security

When installing Clintrial multisite, you must create or modify various passwords. These include:

- Distribution passwords—Passwords used by the current multisite site for the link between the current site and a site that it has registered for distribution. Distribution is the movement and management of metadata objects among multiple sites.
- Proxy account passwords—Passwords used for proxy accounts that allows another multisite site to connect to and perform operations at that site.
- Protocol and account passwords—Passwords used to link a protocol or account at a Multisite Replication Subordinate site to the protocol or account at the Replication Master site

For more information, see the *Getting Started* guide and the *Multisite* manual.

Data security features

Audit trails for data security

Audit trails and histories record updates to the following information:

- User profiles.
- Data on forms.
- Queries.
- Study profiles.

Most audit trails include the user who made the change, the date and time of the change, and the change itself. You cannot modify data in an audit trail.