Oracle® Communications

EAGLE FTP Table Base Retrieval Security Guide

Release 5.0
F56241-01
April 2022

Oracle Communications EAGLE FTP Table Base Retrieval Security Guide, Release 5.0

F56241-01

Copyright © 2003, 2022, 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, Java, and MySQL 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.

Contents

1 Introduction

Overview 1-1
Scope and Audience 1-1
Documentation Admonishments 1-1
Manual Organization 1-1
Emergency Response 1-2
Related Publications 1-2
Customer Training 1-2
Locate Product Documentation on the Oracle Help Center Site 1-3

2 FTRA Security Overview

Basic Security Considerations 2-1
Understanding the FTRA Environment 2-1
Overview of FTRA Security 2-2

3 Performing a Secure FTRA Installation

Preinstallation Configuration 3-1
Installing FTRA Securely 3-1
Postinstallation Configuration 3-1

4 Implementing FTRA Security

Configuring STP Connection 4-1
Securing EAGLE Host Key 4-1

My Oracle Support (MOS)

My Oracle Support (MOS) is your initial point of contact for any of the following requirements:

- **Product Support**:
  The generic product related information and resolution of product related queries.
- **Critical Situations**
  A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:
  - A total system failure that results in loss of all transaction processing capability
  - Significant reduction in system capacity or traffic handling capability
  - Loss of the system's ability to perform automatic system reconfiguration
  - Inability to restart a processor or the system
  - Corruption of system databases that requires service affecting corrective actions
  - Loss of access for maintenance or recovery operations
  - Loss of the system ability to provide any required critical or major trouble notification

  Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.
- **Training Need**
  Oracle University offers training for service providers and enterprises.

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

Release 5.0 - April 2022

This section introduces the documentation updates for Release 5.0 in Oracle Communications EAGLE FTP Table Based Retrieval (FTRA).

- Updated Java ™ Runtime Environment (JRE) version throughout the document.
- Updated GUI screenshots for FTRA Software Installation on Windows. For more information, see #unique_10.

1 Introduction

This chapter contains general information such as an overview of the guide, how to get technical assistance, and where to find additional information.

Overview

This guide describes how to perform a secure installation of Oracle Communications EAGLE FTP Table Base Retrieval (**FTRA**) and explains **FTRA** security features.

Scope and Audience

This guide is for administrators that are responsible for product and network security.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Manual Organization

This guide contains the following chapters:

- **Introduction** contains general information such as an overview of the guide, how to get technical assistance, and where to find more information.
- **FTRA Security Overview** describes basic security considerations and provides an overview of **FTRA** security.
- **Performing a Secure FTRA Installation** describes the process to ensure a secure installation of **FTRA**.
- **Implementing FTRA Security** explains **FTRA** security features.

Emergency Response

During a critical service situation, Oracle provides emergency response services such as immediate coverage, automatic escalation, and other features to ensure that the critical service situation gets resolved as quickly as possible. You can contact Customer Access Support (CAS) at 1-800-223-1711 (toll-free in the US) or by calling the Oracle Support hotline for your local country from the following list http://www.oracle.com/us/support/contact/index.html

A critical situation is a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities requiring immediate corrective action. A critical situation can affect the service or system operations in the following ways:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that require service-affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our website to view, and register for, Oracle Communications training.

To obtain contact phone numbers for countries or regions, visit the Oracle University Education website:

https://education.oracle.com/OUcontactUs

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

2

FTRA Security Overview

This chapter describes basic security considerations and provides an overview of FTRA security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the minimal access they need to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using **TLS** (SSL), and secure passwords. For more information, see “Performing a Secure FTRA Installation” section.
- **Learn about and use the FTRA security features.** For more information, see “Performing a Secure FTRA Installation” section
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" at : https://www.oracle.com/security-alerts/

Understanding the FTRA Environment

When planning your FTRA implementation, consider the following questions:

- Which resources need to be protected?
  - You need to protect customer data, such as network routing data.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting the data from?
  For example, is the FTRA application being installed on a stand-alone server or virtual machine with restricted access, or on a server with shared access? The latter presents more open access and potential threats from both the users and other applications.
- What happens if protections on strategic resources fail?
  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you and your customers.
  Understanding the security ramifications of each resource will help you protect it properly.

Overview of FTRA Security

The FTRA is a stand-alone application that transfers EAGLE database tables using an FTP session to a remote server for offline processing. A secure connection is required between the FTRA and the EAGLE.

Operating System Security

FTRA is primarily a java built application with select components built in C/C++. FTRA runs under the Oracle Linux operating system, and the Windows ® 7 and Windows Server 2008 R2 operating systems. Java 1.8 or later is required. For more information about software and hardware requirements, see the ***FTRA Software Installation Guide***.

Restricting Access to FTRA

Restrict access to the FTRA program and its data files to authorized personnel only. To restrict access to personnel authorized to operate the program, see the *Restricting Access to FTRA on Windows* and *Restricting Access to FTRA on Linux* topics in the ***FTRA Software Installation Guide***.

Use SSH/SSL Connections

SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption. SSH/SSL provides secure data transmission through encryption keys.

Encryption is recommended for the connection between the FTRA and the EAGLE. The EAGLE has a key for each FTRA that it services. For more information, see the "Implementing FTRA Security" section.

3
Performing a Secure FTRA Installation

This chapter describes the process to ensure a secure installation of FTRA.

For information about installing FTRA, see the ***FTRA Software Installation Guide***.

Preinstallation Configuration

By default, Oracle Linux gets securely installed by disabling insecure protocols. This installation is recommended for FTRA.

For Windows® installation, network options for SFTP versus FTP and SSH versus Telnet ports configuration need to be selected.

Installing FTRA Securely

To ensure a secure installation of the FTRA, see the "Preinstallation Configuration" section.

For information about restricting access to FTRA to authorized personnel, see the *Restricting Access to FTRA on Windows* and *Restricting Access to FTRA on Linux* in the ***FTRA Software Installation Guide***.

Postinstallation Configuration

Security for FTRA is selected on a per connecting EAGLE basis. Oracle recommends that all attached EAGLE STPs be configured to use secure connections, and that the FTRA be configured to support secure connections to the EAGLE STPs. For more information, see the "Implementing FTRA Security" section.

4

Implementing FTRA Security

This chapter explains the FTRA security features.

Configuring STP Connection

For a secure connection from the FTRA to an EAGLE STP, make sure the EAGLE OA&M IP Security Enhancements feature is enabled and activated, and that the `SSH` and `SECURITY` parameters are **ON**.

For more information, see the description of the **Secure Connection** box of the **STP Connection Configuration Menu** in the ***FTRA User's Guide***.

Securing EAGLE Host Key

An EAGLE using secure connections has a unique host key for each service module. FTRA uses this key to identify or authenticate each service module.

When EAGLE and FTRA connect, FTRA authenticates a server by matching its preinstalled host key with the key received from EAGLE.

For information about adding EAGLE IP addresses to the FTRA `hosts.xml` file, see the *Secure EAGLE Host Key Provisioning* in the ***FTRA User's Guide***.