Oracle® On Track Communication

Security Guide

Release 1 (1.0)

E20958-03

June 2011

Oracle On Track Communication Security Guide, Release 1 (1.0)

E20958-03

Primary Author: Reza Rokni

Contributing Author: Madhubala Mahableshwar, Luis Ramos, Miguel Salazar

Contributor: Dan Rabe, Logan Bruns

Contents

Preface

This guide provides information on the security of Oracle On Track Communication.

Audience

This document is intended for system administrators or application developers who are working with Oracle On Track Communication. It is assumed that readers are familiar with Web technologies and have a general understanding of Windows and UNIX platforms.

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 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.

Related Documents

For more information, see the following documents in the Oracle On Track Communication documentation set:

- Oracle On Track Communication Administration Console Help
- *Oracle On Track Communication Installation Guide*
- Oracle On Track Communication Developer's Guide
- Oracle On Track Communication SDK Documentation
- Oracle On Track Communication Analytics Guide
- Oracle On Track Communication Licensing Information
- Oracle On Track Communication Release Notes
- Oracle Database Security Guide
- Oracle WebLogic Server Administration Console Online Help

- Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server
- Oracle Fusion Middleware Security Guide
- Oracle Fusion Middleware Administrator's Guide
- Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server
- Oracle Fusion Middleware Securing Oracle WebLogic Server

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Introduction

This chapter covers the general outline of the document, and provides an overview of Oracle On Track Communication (On Track).

1.1 About Oracle On Track

Oracle On Track is a collaborative Web application that provides a media-rich real-time contextual experience that helps drive business conversations to decisions. On Track enriches group interactions with active business intelligence, annotated content, voice, video and application sharing. On Track can be integrated with Oracle products to provide a facility for collaboration around any business process, while retaining the content for future use and discovery.

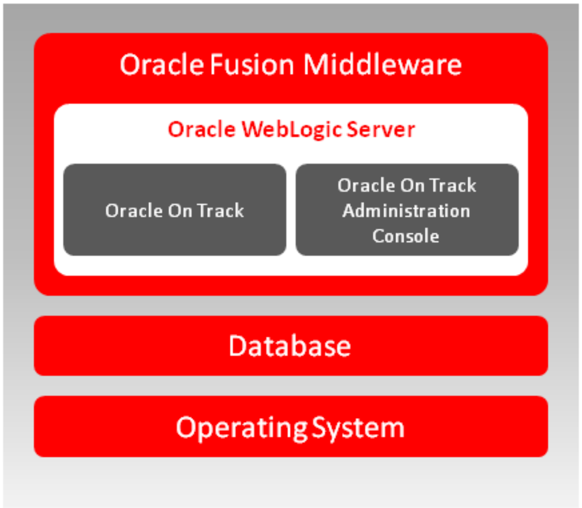
1.2 Guide to This Document

This document is organized as follows:

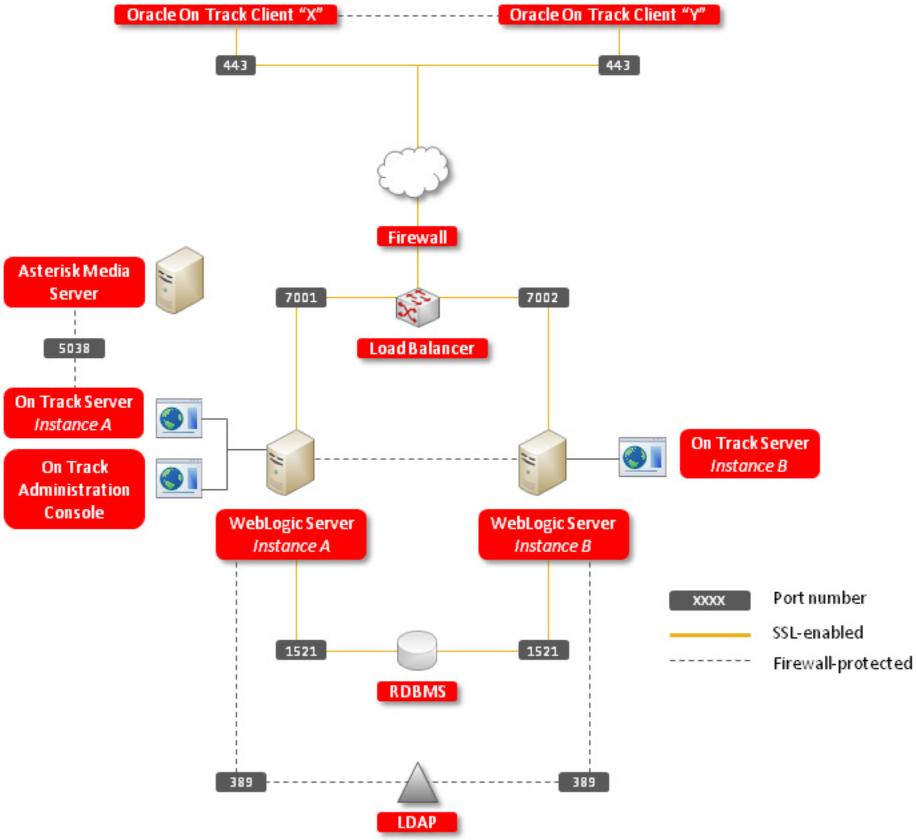
- Chapter 2, "Basic Security", covers basic security recommendations and guidelines for database and system administrators.
- Chapter 3, "Network Security", outlines the internal and external connections Oracle On Tracks uses to communicate with internal and external components through the network.
- Chapter 4, "HTTP Access and SSL Connections", covers secure connections done using the HTTP and SSL protocols.
- Chapter 5, "Securing User Realms", describes the different realms an administrator may use to provide user access and policies for managing user behavior.

1.3 Oracle On Track Overview

Oracle On Track is deployed as an Oracle WebLogic Server application within in an Oracle Fusion Middleware environment. Oracle On Track makes use of different components of the Oracle software stack. The following figure shows an overview of the Oracle On Track architecture:



Oracle On Track can be installed in a single-instance topology or in a high-availability topology. A high-availability topology typically consists of an Oracle Real Application Clusters (RAC) Database, one or more instances of an Oracle WebLogic Server cluster that hosts the On Track deployment, and a load balancer that acts as a proxy server. The following diagram shows a typical Oracle On Track high-availability topology:


Oracle On Track Client "X"
Oracle On Track Client "Y"
443
443
Firewall
Asterisk Media Server
7001
7002
Load Balancer
5038
On Track Server Instance A
On Track Administration Console
On Track Server Instance B
WebLogic Server Instance A
WebLogic Server Instance B
1521
1521
RDBMS
389
389
LDAP
xxxx Port number
SSL-enabled
Firewall-protected

2

Basic Security

This chapter covers security recommendations for different components of the software stack that interact with Oracle On Track.

2.1 Operating System

Oracle On Track can be deployed in different operating systems, such as GNU/Linux and Microsoft Windows. Oracle recommends to follow standard security practices for your specific operating system. To see a list of supported operating systems, and get more information and recommendations for your operating system, see the Certifications tab after logging in at `http://support.oracle.com`

2.2 Database Security

Oracle On Track Communication may use an Oracle Database 11*g* or an Oracle Real Application Clusters 11*g* database . This section addresses the most important security considerations for Oracle On Track's database interactions.

2.2.1 Database Administration and User Database Access

Oracle On Track may be deployed in single instance mode using an Oracle Database 11*g*, or in a high-availability mode using an Oracle Real Application Clusters. For in-depth information on Oracle Database 11*g* or Oracle Real Application Clusters security, see *Oracle Database Security Guide*.

2.2.2 Database Auditing

Database auditing is the process of monitoring and recording of selected user database actions. Oracle recommends to enable auditing on the database. To enable auditing, see *Standard Database Auditing* at

`http://www.oracle.com/technetwork/database/security/index-085803.html`

Once auditing is enabled, Oracle recommends reviewing, maintaining, and securing audit records. For more recommendations and best practices on database auditing, see the Oracle Audit Vault Documentation Library at

`http://www.oracle.com/technetwork/database/audit-vault/documentation/index.html`

2.2.3 Business Views Considerations

Oracle On Track Business Views are a collection of database views that are provided with On Track to facilitate statistical reporting. Database administrators can query a Business View to obtain statistical reports based on the Oracle On Track application data. To provide secure reporting, Oracle recommends to consider the following actions:

- Disable access to Business Views from the main schema.
- Create a new Reporting View schema for analytical purposes. This involves creating a new tablespace and a specific user with select access to Business Views.
- Disable default access to sensitive Business Views marked with X_S_RV, unless absolutely needed for analytical environments.
- Create Materialized Views that are synced once a week during off peak time to avoid performance issues when running data mining queries.

2.3 Oracle Fusion Middleware

Oracle On Track is deployed in a Fusion Middleware environment. Oracle recommends to follow standard security practices for Fusion Middleware components that interact with Oracle On Track.

2.3.1 Oracle WebLogic Server

Oracle On Track and the Oracle On Track Administration Console are deployed as separate Oracle WebLogic Server applications.

- The default path for accessing Oracle On Track is the following:

  ```
  https://<server_name>.<domain>:<port>/ontrack/
  ```

- The default path for accessing the Oracle On Track Administration Console is the following:

  ```
  https://<server_name>.<domain>:<port>/ontrack/Admin/
  ```

> **Note:** For more information on how to access and use the Oracle On Track Administration Console, see the *Oracle On Track Administration Console Help*.

The Oracle On Track deployment within the WebLogic Server instance runs either in development or production mode. Development mode is generally used for application and gadget development, and testing purposes. For increased security, Oracle recommends to enable production mode in WebLogic Server once ready to give access to users. For more information about how to change the runtime to production mode, see the *Oracle WebLogic Server Administration Console Online Help*.

Once production mode is enabled, follow Oracle standard practices for securing the production environment. For more information, see *Oracle Fusion Middleware Securing a Production Enviroment for Oracle WebLogic Server*.

To prevent unauthorized access to your WebLogic Server domains, Oracle recommends to use Roles and Policies from the WebLogic Security Service to determine who can access resources in a domain. See *Oracle Fusion Middleware Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

Note: For in-depth information on how to secure a WebLogic Server environment, follow the guidelines in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

2.3.2 Credential Store Framework

A credential store is a repository of security data called credentials. A credential can hold user name and password combinations, tickets, or public key certificates. Credentials are used during authentication, when principals are populated in subjects, and further, during authorization, when determining what actions the subject can perform. Credential Store Framework stores information such as Simple Mail Transfer Protocol (SMTP) password and bind password for LDAP realm.

By default Oracle On Track does not use the Credential Store Framework. For more information on how to access and use the Credential Store Framework, see *Oracle Fusion Middleware Security Guide*.

3 Network Security

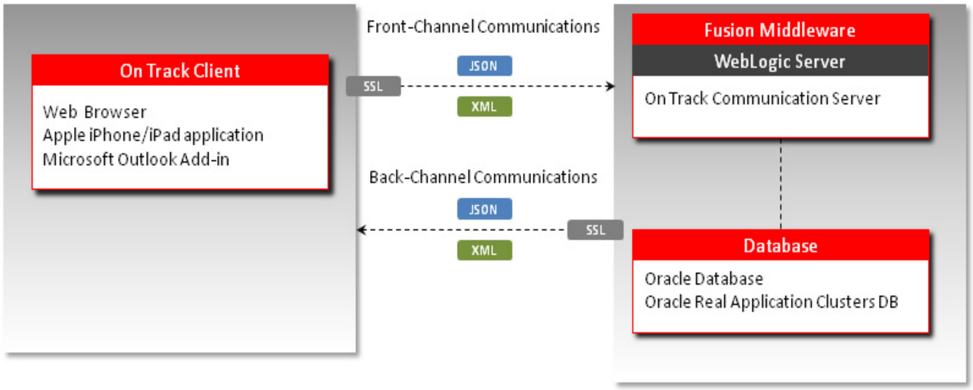
Oracle On Track communicates with external components and components within your own infrastructure. This chapter covers recommendations on how to secure your network environment.

3.1 Oracle On Track Communication Channels

Oracle On Track has two communication paths between the client and the server where messages are exchanged to update information. The client-to-server communication is called the Front Channel, and the server-to-client communication is called the Back Channel.

Oracle On Track uses the HTTP-RPC protocol to exchange messages between the client and the server. The client sends RPC messages to the server in serialized JSON or XML format. The server responds to the client using the same method, and can also send notifications to users through email and various desktop notification services such as Growl, GNTP (for Microsoft Windows systems), libnotify (for UNIX systems), and libGrowl (for Apple Mac OS X systems).

The following figure shows an overview of the Oracle On Track communication channels:


On Track Client
Web Browser
Apple iPhone/iPad application
Microsoft Outlook Add-in
Front-Channel Communications
SSL
JSON
XML
Back-Channel Communications
JSON
XML
SSL
Fusion Middleware
WebLogic Server
On Track Communication Server
Database
Oracle Database
Oracle Real Application Clusters DB

The Oracle On Track server implements a caching mechanism that reduces round trips to the database called On Track Object Cache. In a high-availability topology, the caches are cluster-aware and communicate directly with information of stored objects.

3.2 Oracle On Track High-Availability Topology

The high-availability topology for Oracle On Track consists of a WebLogic Server cluster in which multiple WebLogic Server instances run simultaneously and work together to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic Server instance. The server instances that constitute a cluster can run on the same machine, or be located on different machines.

Note: For more information on clusters, see *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*.

The Oracle On Track architecture consists of several components that communicate with each other on different tiers. The following table shows the interactions of such components and lists the default port they use to communicate:

Table 3–1 Oracle On Track Components Communication Channels

Network Connection From	Network Connection To	Type	Default Port
Oracle WebLogic Server Data Source	Database	SQLNET	1521
Orale WebLogic Server Cluster Node	Oracle WebLogic Server Cluster Node	Oracle WebLogic Server-Based Cluster Communication	No default port.
Oracle On Track Server Cache	Oracle On Track Server Cache	Oracle On Track Cache Cluster Communication	No default port.
Oracle On Track Server Back Channel Router	Oracle On Track Server Back Channel Router	Oracle On Track Back Channel Router Communication	No default port. Oracle recommends to use ports within the range from 49152 - 65535.
Oracle On Track Server	Voice Asterisk Server	Asterisk Channel Communication	The local Asterisk server uses AMI TCP port 5038.
Oracle On Track Server Application Port	Oracle On Track Server	Applications Sharing Port	For media Asterisk server, the port can be configured. But by default, SIP UDP port is 5060 and for RTP random UDP port, a range of ports is configured.

Note: For application sharing, SRTP access from the proxy to Oracle Fusion Middleware is required. Be sure to add to your proxy a static NAT rule so that the original user's IP address and port would not be rewritten. Application sharing also supports tunneling via standard proxy servers.

Note: For more information about Oracle WebLogic Server ports, see *Oracle Fusion Middleware Administrator's Guide*.

For more information on clusters, see *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*.

4

HTTP Access and Secure Sockets Layer

HTTP access is the primary way Web applications communicate with a server. Oracle On Track uses an additional level of security by using the Secure Sockets Layer (SSL) protocol to encrypt Front-Channel and Back-Channel communications. This chapter covers the required configurations to enable SSL and lists the connections from different components that connect using this protocol.

4.1 Configuring SSL for Oracle WebLogic Server

Oracle On Track requires the SSL protocol to be enabled in production mode. In Oracle WebLogic Server, SSL is disabled by default. For more information about how to configure and enable SSL in WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

4.2 List of SSL Connections

The following table shows a list of On Track SSL connections to other components:

Table 4–1 Oracle On Track SSL Connections

Network Connection From	Network Connection To	SSL-enabled?	Defaul Port
Oracle On Track Client	Oracle On Track Server	Yes	443
Oracle On Track Server (Cluster instance)	Oracle On Track Server (Cluster instance)	No	No default port
Oracle On Track Server (Cluster Instance)	Oracle On Tack Object Cache (Cluster Instance)	No	No default port
Oracle On Track Server	LDAP Server	No (default). To enable, See *Oracle On Track Administration Console Online Help*.	389 (Non-SSL). 636 (SSL)
Oracle On Track Server	Oracle Database 11*g*, Oracle Real Clusters Application	No (default). To enable, see *How To Configure and User Oracle JDBC Driver SSL with Oracle WebLogic Server.*	1521

Table 4–1 (Cont.) Oracle On Track SSL Connections

Network Connection From	Network Connection To	SSL-enabled?	Defaul Port
Oracle On Track Client	Oracle On Track Application sharing	No. Uses SRTP protocol for increased security, but optimized for RTP low latency.	9001
Oracle On Track Server	Asterisk Server	No	5060

5

Managing Security Realms and User Access

This chapter covers the different security mechanisms for authenticating user access to Oracle On Track.

5.1 User Repositories

A user can be a person (such as an application end user) or a software entity (such as a client application). To access any resource belonging to a realm, a user must be defined in a security realm. A security realm comprises mechanisms for protecting the resources. Each security realm consists of a set of configured providers, users, groups, security roles, and security policies.

Oracle On Track provides two main ways to authenticate users that access a security realm:

- Using the default Database Realm.
- Using the Lightweight Directory Application Protocol (LDAP) Realm.

The choice of either mechanism for user authentication and access, or a combination of both, depends on different requirements. See Section 5.2 and Section 5.3 for more information.

> **Note:** To limit the usage of Oracle On Track to a small set of users, you can add the users explicitly from the Oracle On Track Administration Console and then disable Self Signup on the realm. See the *Oracle On Track Administration Console Help* for more information.

5.2 Database Realm

For a self-contained Oracle deployment, Oracle recommends to use the database realm for user authentication. Every Oracle On Track instance has one database realm that is used for verifying and retrieving user names and passwords. Some of the security considerations for a database realm are as follows:

- Ensure that only users who can authenticate against LDAP can access Oracle On Track. To do this, grant the administrator privilege to an LDAP user and then disable the database realm.
- If you are using database realm and if you are not an LDAP user, then modify the password policy parameters for a secure and strong password.

5.3 LDAP Realm

The LDAP realm provides authentication through an LDAP server. This server allows you to manage all the users for your organization in the LDAP directory. For an existing LDAP server, Oracle recommends to use this mechanism for user authentication.

Some of the security considerations for LDAP Realm user authentication are as follows:

- Ensure that there is SSL communication between Oracle On Track and the LDAP server.
- Use the realm checking REGEXP parameter to exclude realms. For example, a non-Oracle e-mail ID cannot be provisioned in the Oracle account (@oracle.com).
- "Disable "User creation enabled" in the Administration Console if all your user accounts are in an LDAP Realm.