

Oracle Web Conferencing Real Time Collaboration Platform Security Overview

*An Oracle Technical White Paper
June 2004*

Oracle Web Conferencing Security Overview

ABSTRACT

The Oracle Real-Time Collaboration (RTC) platform is a real-time collaboration product that has been designed from the ground-up to meet the security and compliance requirements of today's businesses. The Oracle RTC platform is part of the Oracle Collaboration Suite, a single integrated system for all your organization's communications and information, including web conferencing, files, email, voicemail, fax and wireless.

This paper discusses the need for secure real-time collaboration and explains how the architecture and run-time characteristics of the RTC platform meet corporate information security requirements. This paper will help technical professionals who are familiar with Oracle Web Conferencing to understand the security of the Oracle Real-Time Collaboration platform.

THE NEED FOR SECURE REAL-TIME COLLABORATION

In successful collaborative enterprises, teams of people work together to achieve common business goals, improving the quality of decisions and tasks. However, enterprises today have geographically dispersed employees, business partners, customers, and suppliers. These enterprises spend millions of dollars on travel costs and other logistics-related costs to enable collaboration among the dispersed entities.

In recent years, enterprises have increased their reliance on Internet-based communications to do business and reduce costs. Enterprises have also begun to use the Internet to do real-time online collaboration with their customers, partners, and remote employees. However, the recent spate of virus attacks, the incidents in which confidential data (such as Social Security Numbers) has been compromised, and other security incidents have made corporations increasingly sensitive to the security of products and technologies built for this medium. Collaborative enterprises are now looking for a scalable, reliable and real-time collaboration platform that is secure.

Additionally, recent legislation such as the California Online Privacy Protection Act of 2003 and the Sarbanes Oxley Act places tremendous burdens on businesses and makes them responsible for breaches of security, corporate governance over sensitive material, and the like. The financial services industry and the healthcare industry have their own specific compliance requirements (SEC17a, NASD 3110 and HIPAA). Corporations need to have appropriate technical and physical safeguards to protect the privacy of the information they deal with, be it healthcare, finance or defense. Corporations understand that there is no privacy without security. Businesses demand that information and computer systems assist them in meeting the various compliance requirements.

Oracle has been delivering secure solutions to customers for more than 25 years. Oracle products are built with a software development process comprised of secure coding practices, code reviews and security audits of products. Oracle products provide data and application security throughout the enterprise using industry standard protocols. The Oracle RTC platform is designed from the ground up to meet your enterprise's real-time collaboration needs. Oracle RTC provides data integrity,

confidentiality, authentication and access control for protection against unauthorized access to conferences, content, and archives. The Oracle RTC platform also provides auditing and logging facilities.

Using a RTC platform offers tremendous opportunities for increasing efficiency and reducing costs, and it substantially raises the risks and concerns about the confidentiality of business communication and data. A secure RTC platform should provide easy collaborative access and experience to legitimate users while keeping out hackers, disgruntled employees, criminals and corporate spies.

The Oracle RTC platform has been designed to meet the security and compliance requirements of today's businesses.

INTRODUCTION TO ORACLE WEB CONFERENCING

Oracle Web Conferencing is a single, comprehensive product that gives you a variety of ways to *securely* collaborate, from one-to-one instant conferences to large, scheduled Web seminars. Oracle Web Conferencing is the first set of Real-Time Collaboration services delivered in the RTC platform.

The Oracle RTC platform consists of client and server applications. Each component of the Oracle RTC platform has been secured, from the client console running on your desktop to the middle-tier Oracle RTC Server (built on the Oracle Application Server) to the Oracle RTC Repository, ensuring that your data is well protected. There is no patchwork of technologies from different vendors with varying security needs. The Oracle RTC platform is built on the reliable and secure standards-based Oracle infrastructure that gives you a high level of safety combined with ease of use and administration.

Oracle Web Conferencing security features include:

- Centralized User Management – Oracle Web Conferencing provides enterprise user security and identity management with Oracle Internet Directory (OID) and Oracle Single Sign-On (SSO) Server. It uses OID and SSO to provide centralized user provisioning, user authentication and authorization.
- Conference Security – Oracle Web Conferencing supports different levels of conference access controls via the Regular and Restricted Conference types. Conference time privileges are granted with various Web Conferencing roles that can be assigned to the participants at conference time.
- Conference Document/Content Security – Oracle Web Conferencing provides a convenient and secure method to share your conference documents before, during, and after the conference, limiting content access and visibility to only authorized participants of the specific conference.
- Conference Archives Security – Oracle Web Conferencing archives allows secure management and access to completed conferences, providing the conference host with capabilities to publish the full conference recording to the actual participants or to other users across the enterprise and beyond.
- Network traffic encryption – Oracle Web Conferencing provides 128-bit industry-standard Secure Socket Layer (SSL) encryption for data transmitted over the network.
- Firewall and Proxy Support – Oracle Web Conferencing can work with any Internet proxy and firewall without the need to open any additional ports on the firewall.

Oracle Web Conferencing security consists of:

- Centralized user management
- Conference security
- Conference document / content security
- Conference archives security
- Network traffic encryption
- Firewall and proxy support
- Database security

- Database security – Oracle RTC Repository uses the Oracle Database technology that can enforce data privacy and security down to the most granular level.

This paper is divided into three sections:

- **Security by Design:** Provides an overview of the security architecture of the Oracle RTC platform.
- **Web Conference Security:** Covers the security aspects of who can create or attend web conferences, security during the conference and post-conference security features.
- **Compliance:** Describes how the RTC platform can meet regulatory and compliance requirements.

SECURITY BY DESIGN

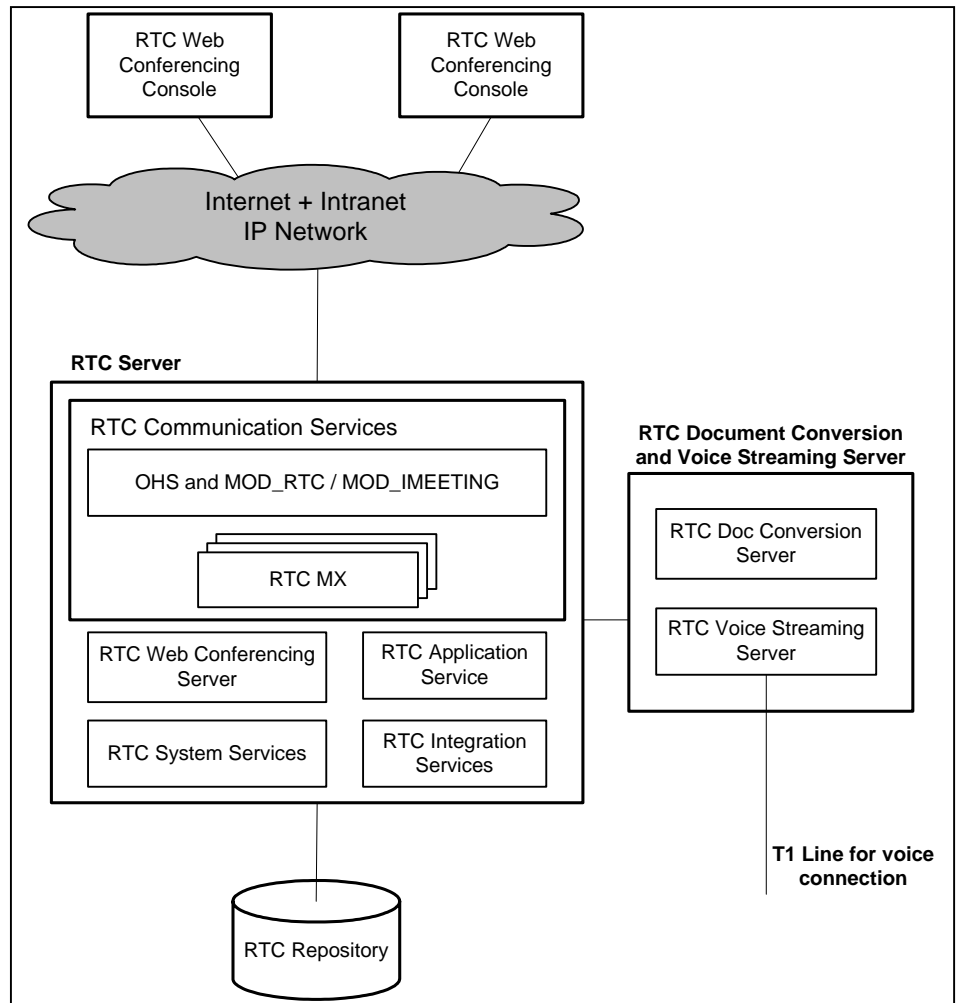


Figure 1. Architecture Diagram

Secure Architecture

The Oracle RTC platform is built on top of the Oracle Application Server and the Oracle Database. The Oracle RTC platform includes the following logical components and services designed to provide a system with the required level of security for the enterprise.

RTC Server

The RTC server consists of a set of components that work together to provide a web conference. The server has been designed to be seamlessly and securely deployed in middle-tier server boxes along with the Oracle Application Server. It uses the Oracle HTTP Server (OHS), an Apache Web Server, from the Oracle Application Server to broker the RTC client connections to the RTC server, as shown in figure 1. The RTC server also uses the Oracle Application Server infrastructure to provide the Web-based RTC Application Service.

The RTC Server consists of:

RTC Communication Services

The RTC Communication Services, consisting of MOD_RTC/MOD_MEETING and RTC Multiplexers (RTC MX), provide the communication channels for RTC client-server interaction. The MOD_RTC/MOD_MEETING plugs into OHS and brokers client connections to the RTC server via the RTC MX. The client connections can be direct or through firewalls via standard ports (Port 80 and Port 443) with no additional configuration. The client connections can be either SSL or non-SSL.

RTC Web Conferencing Server

The RTC Web Conferencing Server runs the actual conference. It is protected behind the communication services and authenticates all client connections and communicates with the RTC clients using a proprietary protocol.

RTC Application Service

The RTC Application Service is the entry point for the user to the Oracle RTC platform. The Application Service uses the Oracle Identity Management Infrastructure, consisting of the Oracle SSO and OID, to authenticate users and provide single sign-on across applications. Users are provisioned to use Oracle Web Conferencing when their OID accounts are created. This facilitates centralized management of user accounts. The Application Service can be deployed with any kind of standard security and network devices, such as hardware load balancers and hardware SSL accelerators.

RTC Integration Services

RTC Integration Services provides a rich set of APIs to enable customers to integrate RTC into their existing business applications, processes and workflows. These APIs use industry standard XML over HTTP/HTTPS protocol. The RTC Integration services can be used to integrate RTC into enterprise applications such as sales and marketing, service and support, human resources and training, financials, order management and corporate portals and websites.

RTC System Services

RTC System Services software provides the system administrator with services to facilitate centralized administration and management service of the RTC system, and to facilitate deployment of the Oracle RTC system into your enterprise. The System Services consist of the Property Manager, Process Monitor, Availability Services and Web Pages to centrally configure, manage and monitor the RTC system.

The System Services let administrators monitor the health of the RTC platform and the number of active conferences in real time, as well as the status of the RTC Server instances and components. The administrator can also look at the meta-data for all active conferences, including details such as conference ID, title, start time, conference

type, current mode, number of attendees, and number of guest users if any. However, administrators do not have any privileges to join a conference to which they have not been invited.

RTC Voice Streaming and Document Conversion Server

The RTC Voice Streaming server is an optional server that provides the ability to stream voice to the participant's desktop. For voice streaming, the RTC Voice Streaming server connects directly to the PSTN network and streams the Global System for Mobile Communication [GSM] codec voice stream over the communication services to the clients.

The RTC Document Conversion server enables conference hosts to upload documents and store them as materials that can then be used during the conference. This server converts Microsoft Office documents (e.g. PowerPoint and Word) to Portable Network Graphics [PNG] and HTML formats to be used in Document Presentation mode.

RTC Console

The RTC Console is downloaded the first time the user joins a Web conference. The Console is digitally signed and verified and does not require administrative or power user rights on the user's desktop to be downloaded.

The RTC Console communicates with the RTC Server through a dynamically assigned RTC MX, over a bi-directional communication channel using a proprietary RTC protocol. This proprietary communication is tunneled through the standard firewall and proxy ports. The RTC console automatically attempts the following three connection scenarios to establish the best secure network channel to the RTC MX, depending on the console's location:

The RTC Console communicates with the RTC Server over a bi-directional communication channel using a proprietary protocol that is tunneled through the standard firewall and proxy ports.

- **Direct TCP/IP** – This method is typically successful for RTC Console clients within a corporate intranet. The connection is directly made to the RTC MX port that is open only to the corporate intranet.
- **HTTPS Direct** – If direct TCP/IP fails, the RTC Console tries to connect through HTTPS direct. This connection is typically successful for RTC Console clients in the open Internet or across transparent proxies. Once a connection is established by Oracle HTTP Server (OHS), it is handed off to the RTC MX by MOD_RTC using a socket hand-off mechanism. The RTC Console and the RTC MX then communicate directly with each other.
- **HTTPS Tunnel** – This option is the only connection method for RTC Console clients that are part of a different intranet and behind their own internal proxy. The RTC Console client automatically retrieves the browser settings on the client machine and relies on the HTTP proxy's HTTPS CONNECT method to establish the connection via the RTC server's Oracle HTTP server and MOD_RTC to the RTC MX. In this case the RTC Console client and the RTC MX communicate over the HTTPS tunnel through the remote proxy.

The following figure illustrates these three methods for connection.

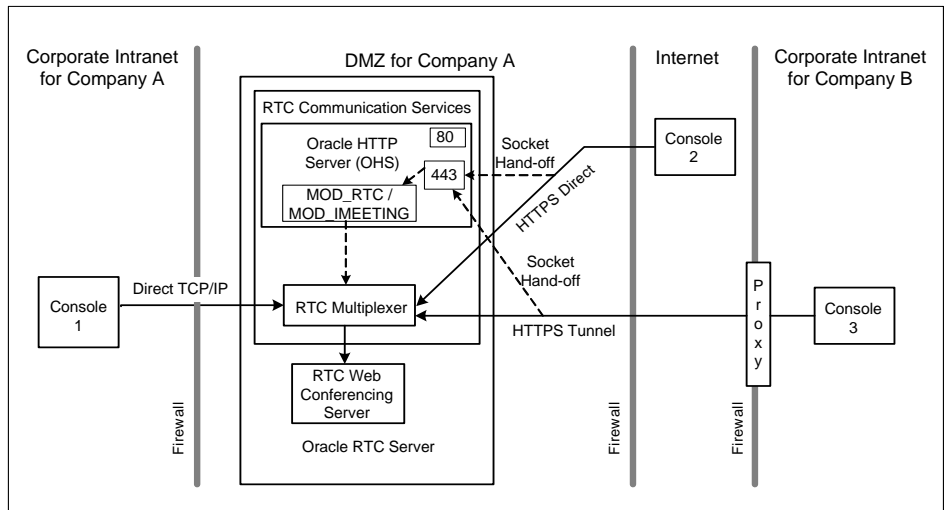


Figure 2. RTC Console Connections

RTC Repository

The RTC Repository uses the Oracle Database to store the user roles, user documents that can be shared during conferences, conference details, and the conference archives. The RTC Repository is never directly accessible to end users. The database is accessed via a secure RTC Application database account. Administrators have the full set of Oracle database security features to protect the data in the RTC Repository.

RTC COMMUNICATION SERVICES AND THE IT INFRASTRUCTURE

The Oracle RTC platform fits seamlessly into your existing IT network/security infrastructure of load balancers, SSL accelerators, firewalls and proxies.

The RTC communication service provides superior network performance across corporate firewalls and proxies without compromising security. This industry-leading network performance is achieved via a firewall traversal algorithm that results in a direct or HTTPS tunneled bi-directional TCP/IP connection to the specific RTC MX handling the web conference traffic.

The typical configuration requirements for the RTC Communication Services are:

- **Client Side Firewall/Proxy Traversal:** The Oracle RTC product uses the HTTPS CONNECT method to traverse the client side firewall and/or proxy if any. The proprietary RTC protocol is tunneled through this connection and no special configuration of Client Side Proxy ports is required. However, since some proxies restrict HTTPS CONNECT to only port 443, the RTC Server's HTTP listener may have to listen on port 443. Alternatively, a load balancer can be configured to pass the HTTPS traffic from port 443 to the Oracle HTTP Listener Port on the RTC Server.
- **Internet Routable IP Addresses for RTC Server nodes:** The RTC Server nodes must have an Internet Routable IP Address to enable direct connections from clients to the RTC Communication Service. This was designed to provide real-time performance during the web conference session.
- **Hardware Load Balancers and Network Address Translators (NATS):** The RTC Application Service works with your existing load balancers to scale out to support heavy loads and to improve availability with standard fail-over features. This allows the RTC installations to be geographically distributed on a network to distribute the meetings and minimize network delays. During the Web conferencing session, the console requires a direct connection to the RTC Servers.

The RTC communication service provides superior network performance across corporate firewalls and proxies without compromising security.

Oracle Web Conferencing provides real-time performance by enabling direct connection from the client to the RTC server. This requires the RTC Server to have an Internet Routable IP Address.

The RTC server provides a software-based real-time load balancing of conferences across the RTC Server nodes, therefore not requiring any additional load balancers for this traffic. As a result, the load balancer should be configured to enable direct connection between the console and the RTC Server.

- **SSL Accelerators:** The RTC Application Service can run behind standard SSL accelerators just like any other web application. Similar to the above scenario, the SSL accelerator should be placed along with or in front of the load balancer shown in Figure 2.

A typical deployment diagram is shown below.

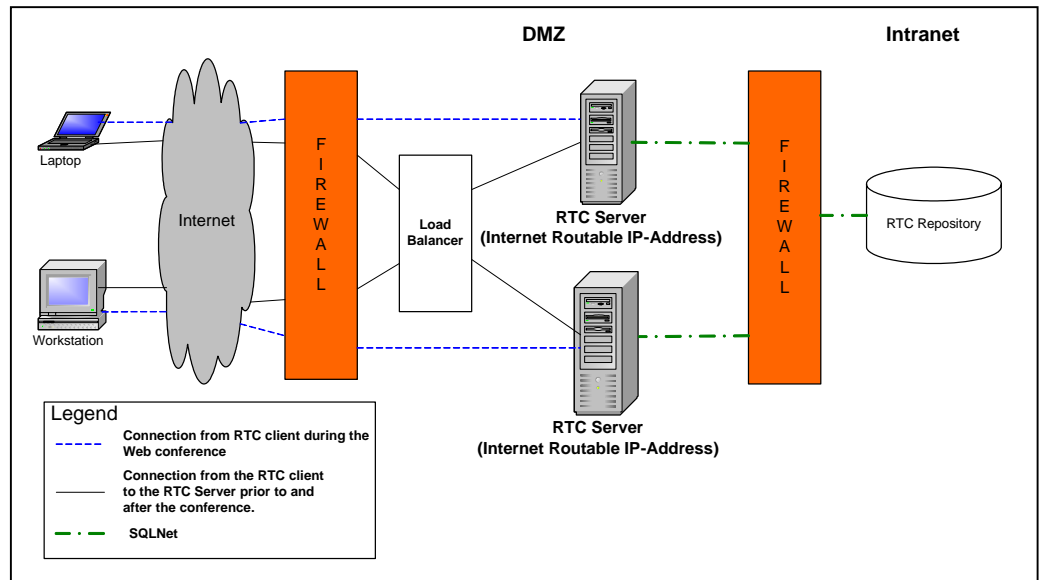


Figure 3. Typical Deployment Diagram¹

Advanced configurations are possible depending on the IT infrastructure and the customer need.

ORACLE WEB CONFERENCING SECURITY

Oracle RTC Web conferencing ensures that your conferences, conference material, conference archives and the system as a whole are secure. The following roles are supported by the RTC platform:

- **Registered User:** The user exists in the OID, an LDAP-based directory, and is the default role given to users of the Oracle RTC platform. It lets them upload documents, host conferences, and record and publish conferences. It also lets them be invited to and attend other conferences that are restricted to registered users only.
- **Guest User:** The user does not exist in OID. They can be invited to and attend conferences.
- **Business Monitor:** This user belongs to a special class of registered users who have the ability to monitor the system and have access to system reports.
- **Business Administrator:** This user belongs to a special class of registered users who have the ability to start, stop, configure and administer the system deployment.

¹ A separate server may be required for RTC Document Conversion and Voice Streaming

Who can create / attend a conference?

Oracle Web Conferencing uses the OID as the user repository. This directory can interface with other industry standard directories, like Microsoft Active Directory and Sun's iPlanet Directory. Oracle Web Conferencing uses the Oracle Identity Management Infrastructure, that includes OID and SSO servers, to authenticate users. Only authenticated users are allowed full access to the Oracle Web Conference Application functionality and to schedule and host Web conferences.

An authenticated user can schedule either a Regular or a Restricted conference based on the security needs of the conference.

Regular Conference:

- Allows authenticated users to conveniently host conferences with both guest and registered users as participants.
- Can be secured via a meeting key that limits access to these conferences. Any guest or registered user can attend these conferences if they know the conference ID and conference key.
- Can be optionally published to the public conference web page of the RTC Application, making it visible to all users.

Restricted Conference:

- Lets hosts restrict conferences to only those users who are registered users.
- Registered users must authenticate against the OID/SSO servers before they can join the conference
- A registered user with the correct meeting ID and meeting key cannot join the conference unless he or she is on the host's invited attendee list for the conference.
- Guest users are not allowed to attend the restricted conferences.

How secure is my Web Conferencing session?

The RTC platform supports 128-bit SSL encryption of all network traffic between the RTC Console and the RTC Server and the RTC Application Service. While scheduling a conference, the user can set the conference to be SSL-encrypted. The RTC administrator can alternatively put a policy in place to enforce all conferences be SSL-encrypted conferences at the System or at the Site level.

During a conference, all user requests are authorized and users are granted privileges based on the role granted to the user by the conference host. The possible roles for participants during a web conference are:

- **Host:** Initiates the conference and has ultimate control over it. During a conference the host can present the content himself, enable voice streaming, record the conference, and conduct polls. The host can also grant presenter control to other attendees to present any content, decline presenter role requests from attendees, revoke the role of a presenter or shared-control attendee, revoke all control assigned to other attendees, assign the host role to another attendee, or expel an attendee from the conference.
- **Presenter:** An attendee whom the host allows to present content of the conference. A presenter can switch modes, conduct polls, use mode-specific tools, and, in Desktop Sharing mode, decline, grant, or revoke shared control of the

Only authenticated users can schedule a regular or a restricted web conference. A regular conference can be attended by anyone who knows the conference ID and the conference key. A restricted conference can be attended only by registered users who have received an invitation to attend.

Oracle Web Conferencing supports 128-bit SSL encryption. The administrator can set a policy to enforce all conferences to be SSL encrypted at the System or the Site level

The possible roles during a web conference:

- **Host is the person who initiated the conference and has complete control over the entire session.**
- **Presenter is an attendee whom the host has allowed to present content during the conference.**
- **Attendee is a participant with no privileges, but who can be given shared-control or even be promoted to be a presenter anytime during the conference**

content with another attendee. A host can appoint more than one presenter at a time or revoke presenter privileges of any user at any time.

- Attendee: A conference participant with no conference control privileges. Any attendee can be assigned shared control or even promoted to a presenter by the host.

How secure are my archives?

The details of every Web Conferencing session conducted on the system are archived. A conference archive consists of information about who attended the conference, which documents were sent as pre-conference materials, which documents were presented during the conference, which URLs were visited during the conference, chat transcripts, information about any polling that was conducted, and the recording of the conference if it was recorded.

The archive of a conference is not published by default. The conference archive feature allows the host to choose which aspects of the conference archive to publish. The host can publish the full conference details such as conference title, type, date, time, number of attendees, the actual attendee list and the conference recording if one was made. The host can additionally choose whether or not the conference polls, attendee chats, are included.

Oracle Web Conferencing makes your conference archives secure by retaining and applying the security restrictions of the actual conference. Archives of Restricted conferences are available only to the users who were invited to the actual conference. This ensures that a confidential and restricted conference is not inadvertently published to a wider audience. Archives of Regular conferences can be made available to a wider audience. The playback of the recording can also be secured via SSL encryption.

COMPLIANCE

Oracle recognizes the increasing corporate governance and compliance needs of your enterprise. The RTC Web Conferencing platform repository is built on the industry-leading Oracle database, letting you use off-the-shelf database tools for searching conferences by specific users, attendees, keywords in chats, conference documents, and so forth.

The repository stores a plethora of information such as: list of scheduled conferences, list of conference attendees, types of conferences, conference materials, chat transcripts, conference polls, documents, web pages and other content viewed and shared during the conference, duration of the conference, and attendance times of the participants.

The conference archival system allows the playback of recorded conferences. The recorded archive can be played back on-demand from the RTC Application Service pages or downloaded for offline viewing or separate archiving specifically for compliance needs.

CONCLUSION

The Oracle RTC platform supports different levels of security to match your corporate security requirements. The Oracle RTC platform facilitates easy access to users while allowing enterprises to control secure information. The Oracle RTC platform provides security controls at the system, conference and individual user level. Administrators can configure the system to mandate that SSL connections be used for

all conferences. The administrator can also set up the system to either easily allow guest users to attend conferences or restrict the conferences to users authenticated by your company's reverse proxy.

The Oracle RTC platform meets your corporate security needs before, during and after conferences.



Oracle Web Conferencing
Security Whitepaper
June, 2004
Author: Amar Padmanabha
Contributing Authors: Mary Ann Davidson, Barbara Heninger, Bhaskar Roy, P.V. Shivkumar, Ramu Sunkara

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Copyright © 2003, Oracle. All rights reserved.
This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.