



Interested in learning more about security?

## SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

### Oracle Collaboration Suite Security

The Oracle Collaboration Suite is a great product, putting all your information within a single framework. Email, Calendar entries, Documents, Voicemail and Portal content are all just a click away. What needs to be acknowledged is that the single sign-on identity needs the highest protection. A single application like IMAP that allows for a leak of a user's password would give the attacker access to all information authorized for that user. Security for the Oracle Collaboration Suite is attained by implementing firewa...

Copyright SANS Institute  
Author Retains Full Rights



AD

## **Oracle Collaboration Suite Security**

Christopher A. Bennett

June 14, 2003

GSEC version 1.4b

### Abstract

Oracle Collaboration Suite version 9.0.3 is a many faceted product delivering a collaborative communication platform including email, IMAP, POP3, Webmail, Portal, calendar, Oracle Files, wireless, voicemail and fax services. Oracle Collaboration Suite is built upon the Oracle 9iAS version 2 application server and Oracle 9i version 2 Database. "Oracle is the undisputed market leader in formal security evaluations, with fourteen independent security evaluations against every major worldwide criteria over the past ten years" (Davidson, p.5). "Oracle's Unbreakable commitment means making products progressively more secure by default, so that products are acceptably secure out-of-the-box, with minimal additional action by administrators" (Davidson, p.11). The Security design process for the implementation of Oracle Collaboration Suite requires evaluation and execution of a number of systems and configuration choices.

The "Unbreakable" claim that Oracle makes is based on products being capable of the highest security, but they must still be deployed following best practices and using security measures at many levels. Security design for a system that includes single sign-on to many applications, like Oracle Collaboration Suite does, should be looked at both from the individual application point of view and also at the whole system as one, as the relationship of the applications to one another under a common directory and authentication store require all systems to have equivalent safeguards for security. Securing the Information within the Oracle Collaboration Suite requires a careful look at many pieces of this complex system.

### Product Overview

Oracle Collaboration Suite is early in its product life cycle and so many new functions and internal design changes will be coming as future releases come out. The version discussed here is version 1 of the Collaboration Suite packaged as Oracle Collaboration Suite 9.0.3 Available for download in October 2002. In an Oracle magazine article John Dolan, vice president of strategy in Oracle's Mobile Products and Services division states:

And of course, IT departments must wrestle with diverse e-mail, voice-mail, fax, file-sharing, and conferencing solutions. "Reliability and security is notoriously poor, and maintaining the systems is an ongoing chore" (Baum, p38)

The Collaboration Suite is positioned to simplify these systems by combining systems and functions to reduce the number of administration points. The Oracle Collaboration Suite (OCS) is targeted at companies that are looking at upgrading from earlier versions of the Microsoft Exchange server.

For customers using legacy messaging products such as Microsoft Exchange, Oracle Collaboration Suite plans to directly address pain points such as increasing costs, continued forced migrations, and lack of integration across different communication technologies. In addition, Oracle's centralized approach may provide a manageable alternative to administering the number of Microsoft Exchange and file servers required in an enterprise (Kawamoto, p.1).

The design and configuration issues are many and include:

- ✓ General systems design
- ✓ Basic systems security
- ✓ Database security
- ✓ The Single Sign-on (SSO) and Oracle Internet Directory (OID) server(s)
- ✓ Apache web server and Portal security
- ✓ Oracle SMTP in and SMTP out processes
- ✓ IMAP and POP
- ✓ Oracle Calendar
- ✓ Oracle Files
- ✓ Voicemail and Fax
- ✓ Outlook

### General Design

The general design of the OCS system allows for great flexibility in the architecture of the security infrastructure. The application is usually divided into three separate functional server types. The client connects to a layer of Middle-tier servers that host the end user servers like IMAP, Web and calendar. An Infrastructure server that maintains the LDAP directory, SSO/login server and Portal definitions also requires direct client connections. The last server type is the database engine, well protected on the network, only communicating with the Middle-tier and Infrastructure servers. The Middle-tier services and the Infrastructure services can be split onto multiple servers in a myriad of configurations to solve high availability, scalability, manageability and security requirements. The ECOstructure "Resilient" Blueprint is an example of this design (Unknown #1). The Web/Middle-tier and Infrastructure/SSO servers are located in the DMZ. The database servers are then further protected behind an internal firewall. Hardware on the DMZ is attached to switched network equipment to help safeguard the communications of other servers from being sniffed. Refer to Oracle 9i Application Server Release 2: Firewall and Load Balancer Architectures for Detail information (Lowenthal).

The Oracle Email system is not recommended to be placed directly accessible from the Internet. The system expects the use of an intelligent relay or gateway. As many larger organizations use a central SMTP gateway to handle all inbound and outbound email, this is not a limiting factor. A good design for this gateway comes from Jason D. McLellan in GSEC practical "A Secure Sendmail Based DMZ for the Corporate Email Environment" (McLellan) for an SMTP infrastructure that supports the design concepts of the Oracle Email System. The email DMZ

also provides an additional layer of virus protection before reaching the Oracle Email system.

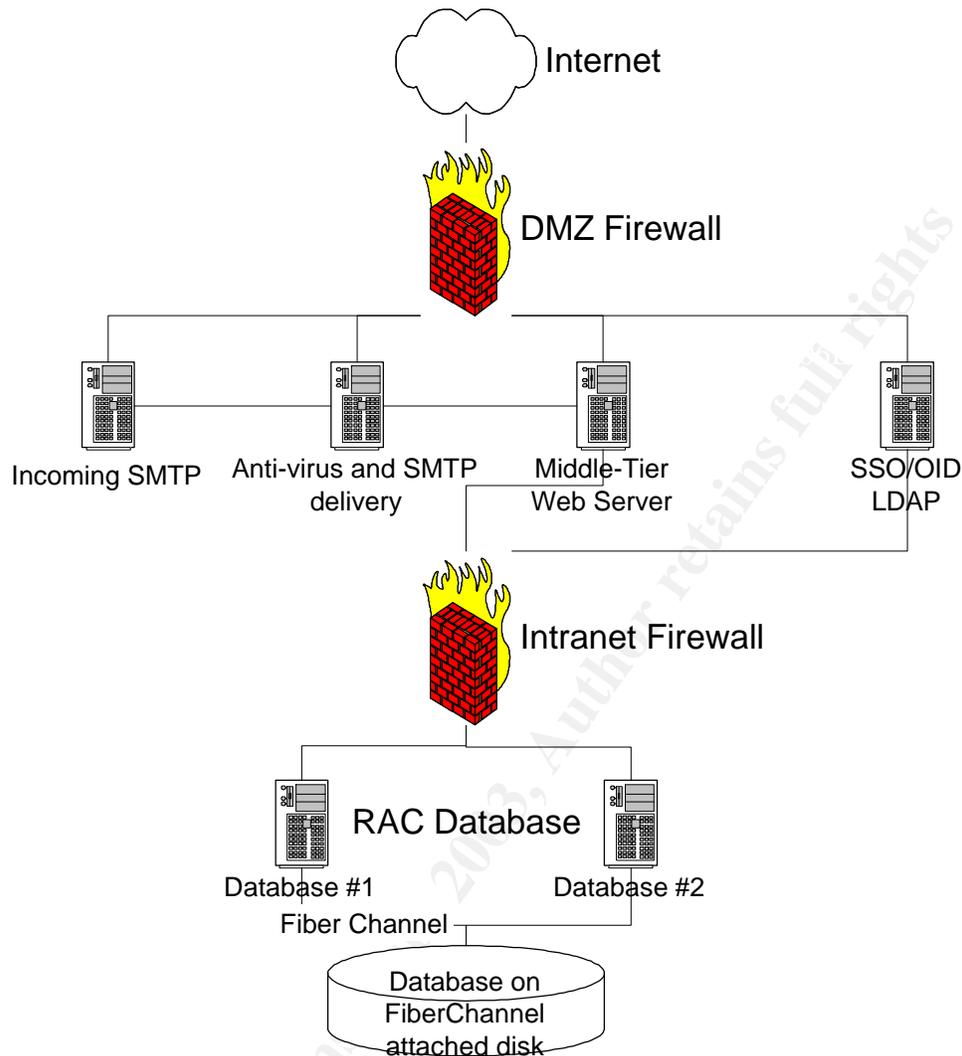


Figure 1. General Design Concept with server placement

The Infrastructure server, also called the SSO/OID server, has a very global function in the Oracle 9iAS infrastructure. The Infrastructure server holds all the information for the 9iAS configuration, management, user management, application authentication and portal configurations. The SSO/OID server should not run other applications and databases to maximize the uptime of the directory. Without the OID LDAP directory; none of the applications that rely on it can function.

The Middle-tier or Web server delivers the content to the Client. The Middle-tier makes all client requests for the information that is stored in the databases. The Oracle 9iAS installs by default with a WebCache layer that will cache the web content for greater performance. Also located on the Middle-tier are the SMTP, IMAP, POP3, Oracle Files and Calendar processes. The Oracle

Files are accessible through the web browser and with the WebDAV interface to Microsoft's web folders.

The client interfaces can be configured to use SSL for WebCache, Apache web server, IMAP and POP3. The OCS is an application that makes use of a single sign-on infrastructure, so protecting that single password is very important. In addition, an SSL accelerator appliance, possibly built into a load balancer, could be used to perform the SSL translations without the performance hit on the Middle-tier (Lowenthal, p.6).

The DMZ firewall should be configured to allow access only to the required ports. Following is a list of the ports from a default installation of the 9iAS server. Carefully consider each port's usage in your installation as you determine what ports are opened through the firewall.

Port	Application	Usage	Server
7777	WebCache	Non-SSL Web traffic	Middle-tier
4443	WebCache	SSL Web traffic	Middle-tier
7778	Apache Server	Non-SSL web server traffic	Middle-tier
4444	Apache Server	SSL web server traffic	Middle-tier
7777	Apache Server	Non-SSL web server traffic	Infrastructure
4443	Apache Server	SSL web server traffic	Infrastructure
25	Email	SMTP in	Middle-tier – open to email gateway only
110	Email	POP3	Middle-tier
995	Email	POP3 over SSL	Middle-tier
143	Email	IMAP	Middle-tier
993	Email	IMAP over SSL	Middle-tier
2121	Oracle Files	FTP	Middle-tier
5730	Calendar	Calendar	Middle-tier
5731	Calendar		Middle-tier
5732	Calendar		Middle-tier
4032	LDAP	LDAP – for Directory Info	Infrastructure – open to administrative subnets only
4031	LDAP	LDAP over SSL – Directory Info	Infrastructure – may be opened based on Directory policy.
1810	Enterprise Manager	Config and Monitor of Oracle components	Should be opened to administrative subnets only
4000	WebCache	WebCache administration	Middle-tier for administrative subnets only

Many other ports are listening on the systems, but they are mostly for server to server communications and internal processes. These ports should be closed in any firewall configuration.

## Basic Systems Security

The OCS will be placed on multiple servers and each of those servers should be installed with guidance by best practices for the operating system that is used. It is outside the scope of this paper to include many of the issues associated with securing the operating system, but it is an expectation that the Oracle software is installed on a server that provides a strong security base. The Oracle Collaboration Suite 9.0.3 software should be installed following the numerous installation guides and documents available on Oracle Metalink. The Oracle software should be updated with all relevant security patches as these patches address publicly announced security holes (Anton, p.175). The other process that needs to be completed before the system is configured to be accessible from the Internet is to change all the default passwords and remove accounts used for samples and examples (Anton, p.175). The Oracle applications come with a number of well known default passwords, but the number is growing smaller all the time as more accounts come configured as locked and expired. Refer to "Hackproofing Oracle Application Server" by David Litchfield for a long list of accounts and default passwords (Litchfield, p.24). There is also an Oracle 9iAS specific vulnerability scanner called orascan available from NGSsoftware that tests for these accounts. ([www.ngssoftware.com](http://www.ngssoftware.com))

## Database

The database that holds all the mail and files stores is the main repository of all the information. Little to no information should be stored on the Middle-tier servers. The Database machine should only talk to the Middle-tier and Infrastructure servers. No end user clients should need to directly attach to these databases. The communication is over standard Oracle Net traffic with the Listener using the default port of 1521. The use of Oracle Advanced Security allows for encryption of this traffic if you need it.

Oracle has a security checklist for the 9iR2 Database (Unknown #4, p.1-9) which covers the following topics:

- Install only what is required
- Lock and expire default user accounts
- Change default user passwords
- Enable Data Dictionary protection
- Practice principal of least privilege
- Enforce access controls effectively
- Restrict network access
- Apply all security Patches and workarounds

## Single Sign-on SSO/OID

Oracle 9iAS version 2 introduces a new install type of Infrastructure that installs the Oracle Internet Directory (OID) and a newly positioned Single Sign-on (SSO) Server that consolidates all the authentication functions of the OCS applications along with many other Oracle and external applications. The SSO server was called the Login Server in previous releases and the use of the Login

Server was optional or not supported for most products. The Oracle 9iAS version 2 and especially with the addition of OCS makes the SSO/OID server a requirement. The SSO server now becomes the single authoritative source for users and their authorizations. All of the OCS products are written to use the SSO/OID infrastructure for authorizing, authenticating and configuration management. The SSO server makes use of the Oracle HTTP server to perform web authentications and to create the SSO cookies that provide the SSO capabilities for web-based applications. The OID is an LDAP v3 compliant directory with a predefined LDAP tree structure. The OID uses a special purpose Oracle 9i database for the storage of all OID information. The Oracle products store most of their configuration information in the OID in this predefined structure. The users and groups that are stored in the tree use a flat name space when using the standard utilities. The OID by default opens an un-encrypted port (4032) and an SSL encrypted port (4031) for LDAP access. Anonymous binds are accepted and give out directory type information including email address. If this information is required by clients on the Internet for directory access, the SSL port only should be opened and anonymous access should be restricted.

Because of the role of the SSO/OID in Collaboration Suite's accessibility, the Infrastructure Server as a whole needs special consideration for high availability. An outage on the SSO/OID server will mean no single sign-on configured application can be accessed. You should not run any other application or process on the Infrastructure Server. A highly available design would include multiple SSO/OID server front-ended by a load balancer and would have the database that is associated with the server installed in a RAC cluster (Anton, p.182)

The SSO http server should always use SSL to protect the login process. The password in a single sign-on environment becomes that much more valuable as this password will get you into many applications. The users should also be instructed to only enter their userid and password into a known single sign-on server and that the sign-on screen has not changed (Anton, p.184). The users should be very suspicious of a login screen from a different server as attacks have been designed before around creating false login pages to gather user password information. The single sign-on environment must be protected by standard security mechanisms, but the environment overall is easier to manage. This should be a resulting increase in user security as the user no longer has numerous userids and passwords to remember. It has been difficult in the past to get users to follow good password standards, not write them down and not stick them to their monitors. A user would often set the same password for all accounts that they have, making for an SSO system that has none of the user productivity advantages. The SSL encryption of the LDAP and HTTP server starts with using the Oracle Wallet manager application to request a security certificate. (Refer to this Oracle document for assistance [http://portalcenter.oracle.com/pls/ops/docs/FOLDER/COMMUNITY/INTERNALP/RODDEVFOLDER/TECHREADINESS/ARCHIINFRA/SECURITY/SETUPSSL/HOW%20TO%20SET%20UP%20SSL%20\(9.0.2\).HTML](http://portalcenter.oracle.com/pls/ops/docs/FOLDER/COMMUNITY/INTERNALP/RODDEVFOLDER/TECHREADINESS/ARCHIINFRA/SECURITY/SETUPSSL/HOW%20TO%20SET%20UP%20SSL%20(9.0.2).HTML))

## Web server/Portlets

The Oracle 9iAS is built upon the Apache web server engine. Oracle has developed several extensions to the base server, like mod\_osso, in support of the 9iAS product that support the additional functionality required. Many of the same issues and vulnerabilities that need to be addressed on an Apache server also apply to the Oracle 9iAS server, but use the Oracle specific patches for any security issues that arise. Refer to the Oracle TechNet security alerts page and subscribe for updates by email (<http://otn.oracle.com/deploy/security/alerts.htm>). The security patches will address system level errors, but still web pages/applications that are developed should be evaluated for cross-site scripting attacks, double encoding attacks and buffer overflows before being moved into production. Applications should also be evaluated for information leaks that can occur. The Portal development environment has a very easy to use Form creation wizard. With very little work you can create a query and update form over any existing table in the database. The security issues arise from the Form application placing the information from ALL columns of the table as hidden fields in the resulting HTML page, rather than just the fields used in the form. If you are allowing a user to update their work phone in a directory application, but the table also has information like SSN, address and other private information, you are passing that information into the browser. The information can also be captured while traversing the network if SSL is not used and the information is cached on a local machine for users that used a public/shared computer. Specific table views should be developed for these applications that will limit the information leakage.

Many Oracle applications are developed in Java to run within the Oracle9iAS Containers for J2EE (OC4J). The OC4J environment is extended by the JAAS provider for security. The JAAS provider should be used to simplify and increase the security of user management, authentication, authorization and storage of application metadata (Anton, p.179). The HTTP server passes requests to the mod\_oc4j modules that pass them to the application providers. An OC4J application provider must interface with the SSO/OID by using JAAS to verify the user request.

A default installation of the Oracle 9iAS Middle-tier includes Oracle WebCache. This product is integrated with the whole Oracle infrastructure to enable substantial performance improvement. The WebCache will make requests to the Apache web server on behalf of the client for any content not located in the Cache or that has expired. The WebCache uses invalidation based caching, which allows the different Oracle components to signal the WebCache when a particular piece of information is no longer current and a new request should not be serviced from the cache. The WebCache provides a web based administration application located by default on port 4000 of the Middle-tier server to make most configuration changes. Make sure that you remember to update this default password. The WebCache logging process stores access (access\_log) and cache events (event\_log) in a directory of the file system. The location is \$ORACLE\_HOME/webcache/logs/. This log is the only log that holds the real TCP/IP address of the computer accessing the server. The HTTP server

logs only show the address of the WebCache server, so these HTTP server logs are not useful to track down malicious activity. The WebCache logs are in standard web server format, but also are in GMT time format. The Time Format should be changed to local time for the log within the administration application. The WebCache, because of its location ahead of the HTTP server, is where clients establish connections to and therefore where the configuration of SSL must happen. The default installation already includes a configured SSL listening port, but without a real SSL Certificate. Use Oracle Wallet Manager, the application that manages all your certificates, to request a new certificate. Once the certificate is installed in Wallet Manager, you need only to update the WebCache with the location of your Wallet File. The communication between the WebCache and the HTTP server does not need to be SSL encrypted if the applications are both installed on the same server. If you separate the WebCache application on a separate server or set of servers, you will need to determine, based on the design, if SSL is required.

Some applications, like Oracle Files, generate web content and links that reference the HTTP server's listening port instead of the WebCache port. If you are implementing SSL for all the OCS applications the SSL certificate will need to be configured for the HTTP server in addition to configuring it for WebCache. SSL certificates for the HTTP server are also managed by using Oracle Wallet Manager. The Certificate that was created for use with the WebCache can be the same one used for the HTTP server, assuming that you have implemented both on the same server.

All of the Oracle Collaboration Suite applications and the SSO infrastructure that supports them use cookies to manage sessions. The most important security task that a user must perform is the Logout at the end of their session. This both protects their user credentials and also allows the servers to release resources. The logout, usually in the upper right hand corner of every page, will log the user out of all SSO enabled applications with one click. If you have external applications open, the SSO logout will not be able to log the user off and the user should logout and close the web browser for that application.

### SMTP in and out

The SMTP capability was written by Oracle for the OCS product and provides support for all the SMTP standards. The SMTP functions are supported within the Oracle Collaboration Suite by two processes. One is called smtp\_in and the other is called smtp\_out. The configuration of these processes is controlled by using the Oracle Enterprise Manager (OEM). OEM is used to modify the configuration of all the 9iAS version 2 applications and also can be used for starting and stopping the applications. The current design of the Oracle Collaboration Suite SMTP process requires that the system be placed behind an enterprise mail gateway/intelligent relay. This requirement will be removed in future releases as the software functionality is enhanced. Many organizations may already have a mail gateway that all the domain's mail exchange (mx) records point at and will possibly also relay all outbound email for all the SMTP servers located within the organization. This gateway protects the corporate

email server (OCS) from having to handle directly many denial-of-service attacks and system exploits.

Email queues and data are stored within the Mailstore database and incoming email will be placed into the user Mailstore. All of an organizations email resides in this single email store, instead of multiple mail stores when using Lotus or Microsoft messaging products. Email stored in a single place is easier to secure and requires much less administration time to manage when an incident arises. The OCS has, because of the fact that it is stored in a single database, a very beneficial feature for virus and SPAM eradication. You can scrub a database of any message with a defined fingerprint (delete or quarantine). You do not need to wait for your anti-virus provider to release the updated signature files and then start cleaning up. This also applies to a particular SPAM message that may have been sent to all of your users. You can use the same feature to delete the spam message out of the Mailstore. Here is an example of the mail anti-virus API to quarantine all email with a particular subject line into a '/Infected' folder of the admin.

```
ESM1> create or replace procedure move_by_subj (mailsubj in varchar2) as
2 sessionid number;
3 begin
4 mail_session.login(user_name=>'userid',
5                   password => '*****',
6                   domain  =>'mail.domain.com',
7                   ldap_host=>'ldap.domain.com',
8                   session_id=>sessionid,
9                   ldap_port =>'4032');
10 mail_av.quarantine(sysdate,14,mail_av.attr_subject,
11                  mailsubj, '/Infected');
12 end;
13 /
```

Procedure created.

```
ESM1> exec move_by_subj ('Popcorn Chicken Returning');
```

PL/SQL procedure successfully completed.

The SMTP process also has support for using an external service to check for viruses. Symantec ([www.symantec.com](http://www.symantec.com)) is one company that has support for the Oracle Collaboration Suite already developed.

The Oracle Email provides for address rewriting rules for recipient and sender addresses. The smtp\_in and smtp\_out processes each call the address rewriting rules. The rewriting rules use a similar syntax to the Sendmail software, but are defined within the Oracle Enterprise Manager (OEM) interface. The rules are executed in the order that they appear within the text window.

The Oracle Email product has support for S/MIME and signatures to allow for secure and/or authenticated messaging through the system. These are

capabilities that are built into the clients to allow for a user to encrypt or digitally sign the message. The message will be stored in the database in its encrypted form. The product also supports SMTP delivery over SSL for encryption during transmission. This capability is only between the OCS and the first SMTP server hop that it delivers to, therefore this capability only works reliably if you have control over all the servers in the path.

Logs for the SMTP process as well as the IMAP, POP3 and List processes do not use the syslog system. Logging is done to an application defined file system space on the Middle-tier within the ORACLE\_HOME. The default is `$ORACLE_HOME/oes/log/um_system/[smtp_in|smtp_out|imap]/<pid>/<pid>.log`. The logs contain valuable information about the activities of the SMTP processes, but the format is different than syslog style sendmail messages and new log management practices must be put in place.

The settings for the smtp\_in and smtp\_out process closely relate to the configuration settings of other email applications like sendmail. The smtp\_in process has many ways to limit untrusted email sites and allow trusted hosts. Figure 2 shows a screen shot from Oracle Enterprise Manager showing some of the available configuration parameters. The smtp\_out process should be pointed at an SMTP relay for delivery of email to other hosts. Figure 3 is a screen shot that shows the entry of the SMTP relay.

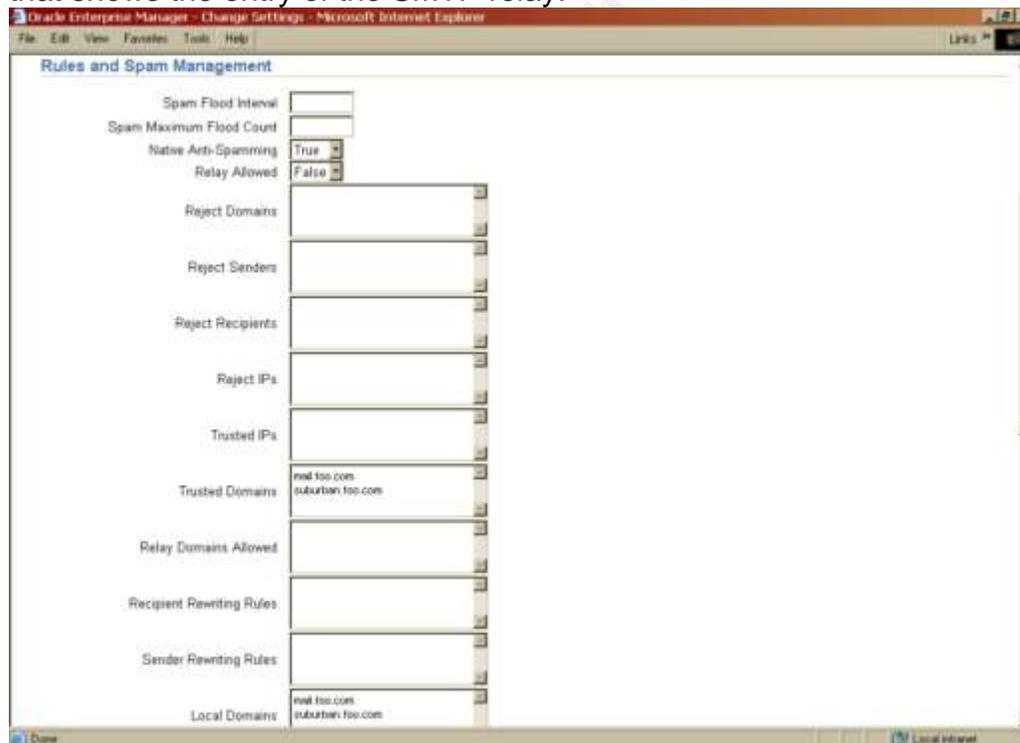


Figure 2. smtp\_in Rules and Spam Management settings

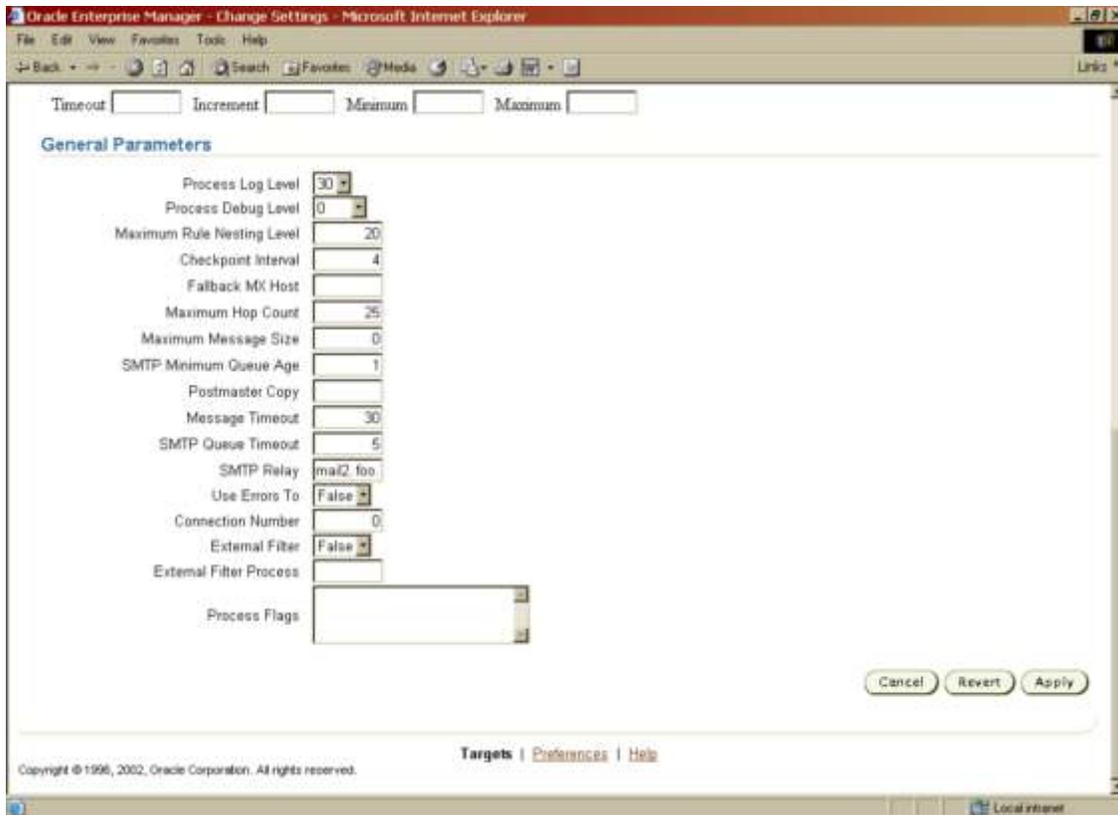


Figure 3. smtp\_out General Parameters settings

### IMAP and POP3

Security for the IMAP and POP3 protocols is mostly about authentication and encryption. IMAP is the client interface for software like Outlook, Outlook express and Netscape Messenger that allows the mail to stay on the server. Leaving your email in the Oracle email store is a safer place to store your email content than on your PC. The IMAP interface supports both non-SSL, the default, and SSL connections, but since IMAP uses plain text userids and passwords it is suggested to use IMAP over SSL to protect your users from having their account information captured from the network. The IMAP and POP protocol listeners use the Oracle standard listener technology. The implementation of SSL certificates for these protocols involve adding directives to the listener.ora and sqlnet.ora files as detailed in the Oracle Email Administration Guide (Tabora, p.120). IMAP client authentications also require the use of a domain. The OCS supports multiple email domains within a single server with the new release, so the client configuration requires you to use [userid@domain.com](mailto:userid@domain.com) style userids when you authenticate. The credentials are then checked against the Single Sign-on server.

The POP3 protocol can also be used with these email client applications. This method will download the content of the email into a local PC mailbox. This is not a good method to use especially on shared or public computer systems and also does not allow Web/Portal access to your email messages. The OCS does support POP3 over SSL for encryption if you do need to use POP3.

The IMAP and POP3 processes have their own set of logs in the Oracle email file system. The default location of the log files are at:  
ORACLE\_HOME/oes/log/<install\_name>/[imap|pop3]/<pid/<pid>.log

### Calendar

The Oracle Calendar server was added recently to the Oracle Collaboration Suite. It is a very nice Calendaring system that has all the important features needed in a Corporate Calendar. The Calendar system does not use the Oracle Database for the storing of Calendar and resource information. The software in this release uses its own data files on the Middle-tier, but does use the OID/LDAP directory for user and group management and also takes advantage of the SSO infrastructure. It is suggested that the Calendar server is installed on its own server if financial resources are available (Unknown #3, p.137). The need for its own server may also be required based on the number of calendar users that you are trying to support. The Calendar processes listen for client connections on a set of proprietary ports 5730, 5731, and 5732.

The security of the Calendar system is provided by the ACE framework (Authentication, Compression and Encryption.) Communications between the different nodes and to the client are controlled by the ACE configurations. The server and the client agree on a preferred authentication and encryption method through a negotiation process during start up. The only clients that support the ACE framework are the Oracle Web Client 2.0 and higher, Oracle Corporate 3.0 and higher and the Oracle Outlook Connector.

The Calendar server logs many different types of information in the /users/unison/log directory. The act.log should be reviewed to watch for login attempts. The logs in this directory should be reviewed to discover irregular patterns of usage. The Calendar product includes a utility called unicksum that is used to generate checksums of the binary files. This utility can be used as a Host-based Intrusion Detection system for the Calendar binaries if you are not using similar software configured for the entire system. You can compare the checksums against previous runs of the utility to verify that the binaries have not changed.

### Oracle Files

Oracle Files is used for a central repository for documents and other files associated with an individual, a workgroup or to all Files users. The security access definitions allowed are simple, but are easily comprehended by the normal user to allow for the self-service model of this online file system. A workgroup has three security levels for users authorized to work with the folder: Administrator, participant, and viewer. Access can be gained by many different protocols, but Web, WebDAV and FTP are the most common. The product also has support for the SMB, NFS, AFP and IMAP protocols. The Files application extends the Oracle Internet Directory entry for the user to include additional password storage attributes in support of these other protocols. The password

for FTP, since it is passed in clear text, does not use the regular SSO password, but sets an FTP specific password in the web client.

WebDAV uses the HTTP protocol to communicate with the server, and does allow for update-in-place functionality for Microsoft Office and other applications (Unknown #2, p.40). By default this communication is not encrypted and the confidentiality of the content of the files should be considered when accessing files from the Internet. Files access could be evaluated based on the organization's security policies to only be allowed over VPN connections or over SSL to limit the exposure of information.

### Voicemail/fax

Oracle Collaboration Suite Voicemail and Fax is a product that allows for the storage of voicemail and faxes as email messages. The system still functions as a normal voicemail system allowing for message retrieval, forwarding and mailbox administration through your telephone handset. When you access your email, either through the web or through a client like Outlook, you will see a combined message list of email, voicemail and faxes. The voicemails are stored in the OCS system as an email message with a WAV file attachment. The Fax is stored in the OCS system as an email message with a TIF graphic attachment. The From: address of the email will include the telephone number of the caller for external callers, but will pick up the name for other OCS Voicemail and Fax users. The To: address is actually an email alias created for your account consisting of your 10 digit [telephone\\_number@email.domain](#). It was discovered by Oracle that this is also an easy way to send spam to the organization if you know the area code and exchange that all their phone numbers are in.

The software is installed on a Windows 2000 server separate from the Middle-tier server. The software is built on the ECTF standard and uses the Intel CT Media Server platform. The Voicemail and Fax System can be integrated with several PBX systems, including Nortel Meridian and Cisco CallManager. Integration with the Cisco CallManager uses a Cisco voice gateway called a DPA 7610. This gateway translates Cisco IP phone signaling into Nortel digital telephone (2616) signaling. The server interfaces on one side through its telephony cards with the telephony system or gateway and through its Ethernet port to the database and Infrastructure servers on the other. The CT Media server with the Oracle software will make Oracle Net calls to the Database server for the delivery and retrieval of voicemail content. All access to subscriber configuration information is made through LDAP calls to the Infrastructure server. The system also controls the Message Waiting Indicator (MWI) on each phone by communicating with a MWI process located on the Middle-tier. This Microsoft Windows server should not be accessible by any system except for the OCS set of servers. No direct user connections are required.

The pin (password) for the voicemail system can be user modified either through the handset or in the Preferences section of their Webmail client. The pin is all numeric, but you do get to set the minimum number of digits the pin must be.

## Outlook

Microsoft Outlook is the best supported client for the Oracle Collaboration Suite. To make for an easy change for existing Outlook users, Oracle has developed a piece of software called the Oracle Outlook Connector. This is a piece of software that handles certain translation needed to successfully connect to the Oracle email and calendar applications.

Oracle Outlook Connector provides e-mail and real-time calendaring through the familiar, integrated interface of Microsoft Outlook. With access to information both online and offline, full-featured mail functionality, and PDA synchronization, Oracle Outlook Connector takes advantage of all of Microsoft Outlook's most popular features. In addition, users benefit from enhanced calendaring capabilities through real-time access to information and up-to-date free/busy time lookups with Oracle Calendar. (Strohm, chapter 8)

Outlook as an email client must still be configured to safeguard against many types of scripting and HTML content vulnerabilities as the OCS can not stop all types of email content based vulnerabilities.

It was also discovered that the Oracle Outlook Connector does correctly identify itself as the originating email client in outbound email headers that are sent to its defined SMTP server, but that an application called SpamAssassin, that is used to identify SPAM, incorrectly adds points to the score for this email. The SpamAssassin rules refer to the email as having a forged Outlook header. If SpamAssassin is used on the SMTP gateway server for your system you can zero out the score for that rule if any of your email gets identified as SPAM.

## Summary

The Oracle Collaboration Suite is a great product, putting all your information within a single framework. Email, Calendar entries, Documents, Voicemail and Portal content are all just a click away. What needs to be acknowledged is that the single sign-on identity needs the highest protection. A single application like IMAP that allows for a leak of a user's password would give the attacker access to all information authorized for that user. Security for the Oracle Collaboration Suite is attained by implementing firewalls, installing on secured operating systems, using highly available hardware, encrypting communications and securely configuring the applications. The Oracle Collaboration Suite is an integration of many applications to support the collaboration of its users. The security design of the system is an integration of many security best practices to support the protection of its user collaborations.

## References:

Anton, Jesse, et al. "Oracle 9i Application Server Best Practices." January 2003. URL: [http://otn.oracle.com/products/ias/pdf/best\\_practices/903iASBestPractices.pdf](http://otn.oracle.com/products/ias/pdf/best_practices/903iASBestPractices.pdf) (June 14, 2003)

Baum, David. "Collaborate Consolidate Connect." Oracle May/June 2003(2003):37-44.

Davidson, Mary Ann. "Unbreakable: Oracle's Commitment to Security." February 2002. URL: <http://otn.oracle.com/deploy/security/pdf/unbreak3.pdf> (June 9, 2003)

Kawamoto, Wayne. "Oracle Announces Availability of Oracle Collaboration Suite." October 8, 2002. URL: <http://www.serverwatch.com/news/article.php/1478171> (June 14, 2003)

Litchfield, David. "Hackproofing Oracle Application Server." 10<sup>th</sup> January 2002. URL: <http://www.nextgenss.com/papers/hpoas.pdf> (June 14th, 2003)

Lowenthal, Bruce. "Oracle 9i Application Server: Firewall and Load Balancer Architectures." July 2002. URL: <http://otn.oracle.com/products/ias/pdf/firewallLoadbalancer.pdf> (May 17, 2003)

McLellan, Jason D. "A Secure Sendmail Based DMZ for the Corporate Email Environment" January 13, 2003. URL: [http://www.giac.org/practical/GSEC/Jason\\_McLellan\\_GSEC.pdf](http://www.giac.org/practical/GSEC/Jason_McLellan_GSEC.pdf) (March 9, 2003)

Strohm, Richard. "Oracle Collaboration Suite User's Guide." August 2002. URL: [http://download-west.oracle.com/docs/cd/B10191\\_01/collab.903/b10032/calendar.htm#1004936](http://download-west.oracle.com/docs/cd/B10191_01/collab.903/b10032/calendar.htm#1004936) (June 14, 2003)

Tobora, Ginger. "Oracle Email Administrator's Guide." August 2002. URL: [http://download-east.oracle.com/docs/cd/B10191\\_01/email.903/b10033.pdf](http://download-east.oracle.com/docs/cd/B10191_01/email.903/b10033.pdf) (June 9, 2003)

Unknown #1. "ECOstructure "Resilient" Blueprint." 2002. URL: <http://www.ecostructure.com/resilient.html> (June 2, 2003)

Unknown #2. "Files Administration Guide." August 2002. URL: [http://download-west.oracle.com/docs/cd/B10191\\_01/files.903/a97358/toc.htm](http://download-west.oracle.com/docs/cd/B10191_01/files.903/a97358/toc.htm) (June 14, 2003)

Unknown #3. "Oracle Calendar Server Administrator's Guide." August 2002. URL: [http://download-west.oracle.com/docs/cd/B10191\\_01/calendar.903/b10093/toc.htm](http://download-west.oracle.com/docs/cd/B10191_01/calendar.903/b10093/toc.htm) (June 14, 2003)

Unknown #4. "Secure Configuration Guide for Oracle9iR2" June 2002. URL: [http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2\\_checklist.pdf](http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf) (June 9, 2003)

© SANS Institute 2003, Author retains full rights



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industrial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA®; New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced