Oracle® Communications Connector for Microsoft Outlook

Security Guide

Release 8.0.2

E55107-01

August 2014

This guide provides an overview about security for Oracle Communications Connector for Microsoft Outlook. It also provides links to security topics that provide more in-depth information for configuring and administering Connector for Microsoft Outlook security.

Overview of Connector for Outlook

For an overview of the features in Connector for Microsoft Outlook, see the overview in *Connector for Microsoft Outlook Installation Guide*. For information on general security principles, such as security methods, common security threats, and analyzing your security needs, see the discussion about designing for security on the Oracle wiki:

`https://wikis.oracle.com/display/CommSuite/Designing+for+Security`.

For an overview of operating system security, see *Oracle Solaris Security for System Administrators*. For more information on Connector for Microsoft Outlook high-level architecture, see the discussion on Connector for Microsoft Outlook system architecture in *Connector for Microsoft Outlook Installation Guide*.

Secure Installation and Configuration

This section outlines the planning process for a secure installation and configuration.

Installation Overview

This section describes recommended secure installation guidelines and deployment topologies for the systems.

Understanding Your Environment

To better understand your security needs, ask yourself the following questions:

1. Which resources am I protecting?

   In a Connector for Microsoft Outlook production environment, consider which of the following resources you want to protect and what level of security you must provide:

   - Protocols: HTTP, SMTP, WCAP, IMAP, WABP, and LDAP
   - Dependent Products: Directory Server, Messaging Server, Convergence Server (Address Book), and Calendar Server. Be sure to check the security policies governing these dependent products.
   - Calendar Server front- and back-end hosts

- Messaging Server front- and back-end hosts
- Dependent resources, such as Directory Server

2. From whom am I protecting the resources?

   In general, resources must be protected from everyone on the Internet. But should the Connector for Microsoft Outlook deployment be protected from employees on the intranet in your enterprise? Should the system administrators have access to all resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. On the other hand, perhaps it would be best to allow no system administrators access to the data or resources.

3. What will happen if the protections on strategic resources fail?

In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or to users who use Connector for Microsoft Outlook. Understanding the security ramifications of each resource help you protect it properly.

Deployment Topologies

Connector for Microsoft Outlook depends on a Calendar Server and Messaging Server deployment. For more information, see:

- *Developing a Messaging Server Architecture* at: https://wikis.oracle.com/display/CommSuite/Developing+a+Messaging+Server+Architecture
- *Developing a Calendar Server Architecture* at: https://wikis.oracle.com/display/CommSuite/Developing+a+Calendar+Server+Architecture
- *Developing a Communications Suite Logical Architecture* at: https://wikis.oracle.com/display/CommSuite/Developing+a+Calendar+Server+Architecture

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture. For more information on addressing network infrastructure concerns, see *Determining Your Communications Suite Network Infrastructure Needs* at: https://wikis.oracle.com/display/CommSuite/Determining+Your+Communications+Suite+Network+Infrastructure+Needs.

Connector for Microsoft Outlook is not a server by itself, but a client that communicates with the Calendar Server and Messaging Server in the back-end. So there is no deployment involved. However, to understand Connector for Microsoft Outlook installation, see the discussion on pre-installation tasks in *Connector for Microsoft Outlook Installation Guide*.

Installing Infrastructure Components

As mentioned previously, Connector for Microsoft Outlook does not require installing infrastructure components, as it is a client which interacts with the Calendar Server, Messaging Server, Convergence Server (for Address Book support), and LDAP Server (for Corporate Directory support). For more information about how Connector for Microsoft Outlook communicates with Calendar Server and Messaging Server, see the Calendar Server and Messaging Server documentation. You can refer to the following:

- *Calendar Server 7 Index* at:
  https://wikis.oracle.com/display/CommSuite/Calendar+Server+7+Index
- *Calendar Server 6.3 Index* at:
  https://wikis.oracle.com/display/CommSuite/Calendar+Server+6.3+Index
- *Messaging Server Index* at:
  https://wikis.oracle.com/display/CommSuite/Messaging+Server+Index

Installing Connector for Microsoft Outlook Components

Installing Connector for Microsoft Outlook consists of the following high-level steps:

1. Preparing a comprehensive Deployment Plan
2. Installing the Deployment Configuration Program
3. Configuring end-user packages
4. Deploying end user packages

For more information, see the discussion on administration process overview in *Connector for Microsoft Outlook Administration Guide* and the discussion on installing the desktop deployment toolkit in *Connector for Microsoft Outlook Installation Guide*. For more information on installing Connector for Microsoft Outlook components, see the discussion on getting started in *Oracle Communications Connector for Microsoft Outlook Administration Guide*.

The configuration parameters for Connector for Outlook are configured by entering details in the following tabs:

- Processes
- User Profiles
- User.psts
- Servers
- Mail
- LDAP
- Calendar
- Address Book
- Single User

For information about desktop installation packages for end users, see the discussion on configuring end-user packages in *Connector for Microsoft Outlook Administration Guide*. For more information about configuring parameters, see the deployment configuration program online help.

Security Features

The following are the specific security mechanisms offered by Connector for Microsoft Outlook:

- SSL support for all the protocols, such as IMAPS, HTTPS (WABP and WCAP), SMTP+SSL, and LDAPS
- Option to not store/cache password

- SMIME support (message signing and encryption support)
- Certificate-based authentication

For more information about certificate-based authentication as part of Connector for Microsoft Outlook security, see the discussion on certificate-based authentication for Connector for Microsoft Outlook in *Connector for Microsoft Outlook Administration Guide*.

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.

Oracle Communications Connector for Microsoft Outlook Security Guide, Release 8.0.2
E55107-01