Oracle® Communications Connector for Microsoft Outlook

Security Guide

Release 9.0

E63671-01

September 2015

This guide provides an overview about security for Oracle Communications Connector for Microsoft Outlook.

Connector for Microsoft Outlook Security Overview

For an overview of Connector for Microsoft Outlook, see the overview discussion in *Connector for Microsoft Outlook Installation and Administration 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

Security Features

Connector for Microsoft Outlook offers the following security mechanisms:

- SSL/TLS support for all the protocols: IMAP, SMTP, HTTP (WABP, REST, and WCAP), IWCP, and LDAP
- Option to prevent the saving of login passwords
- S/MIME support (message signing and encryption)
- Certificate-based authentication

See the discussion about certificate-based authentication in *Connector for Microsoft Outlook Installation and Administration Guide* for more information.

Secure 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 environment, consider which resources you want to protect and what level of security you must provide:

   - Protocols: HTTP, SMTP, WCAP, IMAP, WABP, REST, IWCP, and LDAP

- Dependent products and services: Directory Server, Messaging Server, address book provisioning server (Convergence or Contacts Server), Calendar Server, and Convergence (for user settings and preferences)

  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 happens if the protections on strategic resources fail?

   In some cases, a fault in your security scheme is easily detected and considered but 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 helps you protect it properly.

Deployment Topologies

Connector for Microsoft Outlook depends on a Calendar Server, Messaging Server, and either a Contacts Server or Convergence deployment. These deployments must be deployed, configured, and set up for security. See the security documentation for Messaging Server, Calendar Server, Contacts Server, and Convergence for more information.

Connector for Microsoft Outlook is not a server by itself, but a client that communicates with Oracle and Unified Communications Suite servers. If the servers are configured for security, you can enable secure communications between Connector for Microsoft Outlook and the Unified Communications Suite servers.

Installing Infrastructure Components

Connector for Microsoft Outlook does not require any infrastructure components, as it is a client. The servers with which it communicates, however, must be installed, configured, and set up for security. See the installation and security documentation for the following products for information about installing and securing them:

- Oracle Directory Server Enterprise Edition
- Messaging Server
- Calendar Server
- Contacts Server
- Convergence

Configuring Security for Connector for Microsoft Outlook

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

1. Ensuring your Unified Communications Suite servers are configured for security.

   See the installation and security documentation for Messaging Server, Calendar Server, Contacts Server, and Convergence for more information.

2. Preparing a comprehensive Deployment Plan.
3. Downloading and installing the Deployment Configuration Program (DCP).
4. Using the DCP to create end-user packages that install Connector for Microsoft Outlook with secure connections and features.

   By default, the DCP suggests secure port values and enables the **SSL** option.

5. Deploying end-user packages.

See *Connector for Microsoft Outlook Installation and Administration Guide* for more information about deployment planning, downloading, installing, and using the DCP, and distributing and installing end-user packages.

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 that have purchased support 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 9.0
E63671-01

in an applicable agreement between you and Oracle.