Oracle® Hospitality Materials Control

Security Guide
Release 8.31.0
E80620-02

April 2017

Contents

Preface

This document provides security reference and guidance for Materials Control.

Audience

This document is intended for:

- System administrators installing Materials Control.
- End users of Materials Control.

It is assumed that the readers have general knowledge of administering the underlying technologies and the application.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at http://docs.oracle.com/en/industries/hospitality/

Revision History

Date	Description of Change
December 2016	• Initial publication
April 2017	• Added password content restrictions to the password rules.

1 Materials Control Security Overview

This chapter provides an overview of Oracle Hospitality Materials Control security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See Performing a Secure Materials Control Installation for more information.
- **Learn about and use the Materials Control security features.** See Implementing Materials Control Security for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" website: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Overview of Materials Control Security

Starting from release 8.31.0, database password and encryption-key defining parameters will be stored in Protected Configuration (https://msdn.microsoft.com/en-us/library/53tyfkaw%28v=vs.100%29.aspx). Storing sensitive information in a non-readable format improves the security of our applications by making it difficult for an attacker to gain access to the sensitive information, even if an attacker gains access to the file, database, or other storage location. Materials Control is using RSA machine-level key container, which enables using single one for all applications and optional modules and simplifies the deployment on other PCs.

Keep in mind that Materials Control is secured as underlying infrastructure is – so make sure that Windows workstations and servers are hardened and secured by best-practice rules. More details in Component Security.

Understanding the Materials Control Environment

When planning your Materials Control implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as credit-card numbers.
  - You need to protect internal data, such as proprietary source code.

    - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?** For example, you need to protect your subscribers’ data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What will happen if protections on strategic resources fail?** In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Recommended Deployment Configurations

Materials Control can be deployed on-premises only.

The most common deployment architecture is the one shown in Figure 1. As a client-server application, a single database server connected to multiple Microsoft Windows PC workstations can handle most customer requirements. Optionally used handheld devices can be operated using a direct connection to a workstation (cradle).

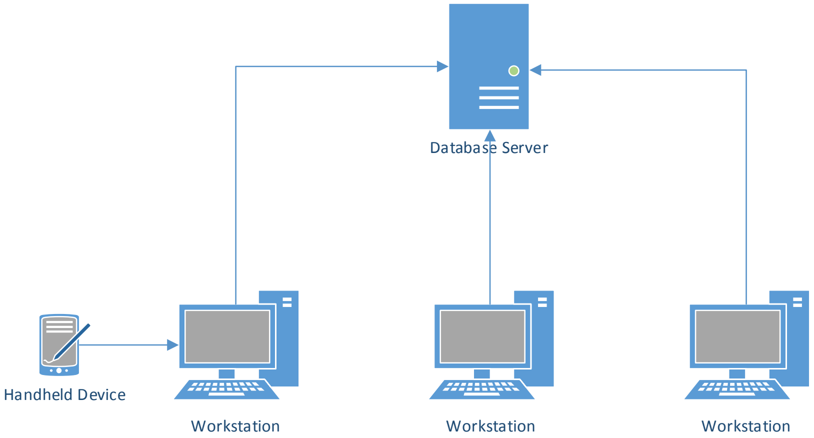

Figure 1 – Single Server Deployment Architecture

In cases where a customer wants to use additional, optional components such as the MCweb intranet web frontend or web-services powered Mobile Solutions, this document recommends adding a separate web server as shown in Figure 2.

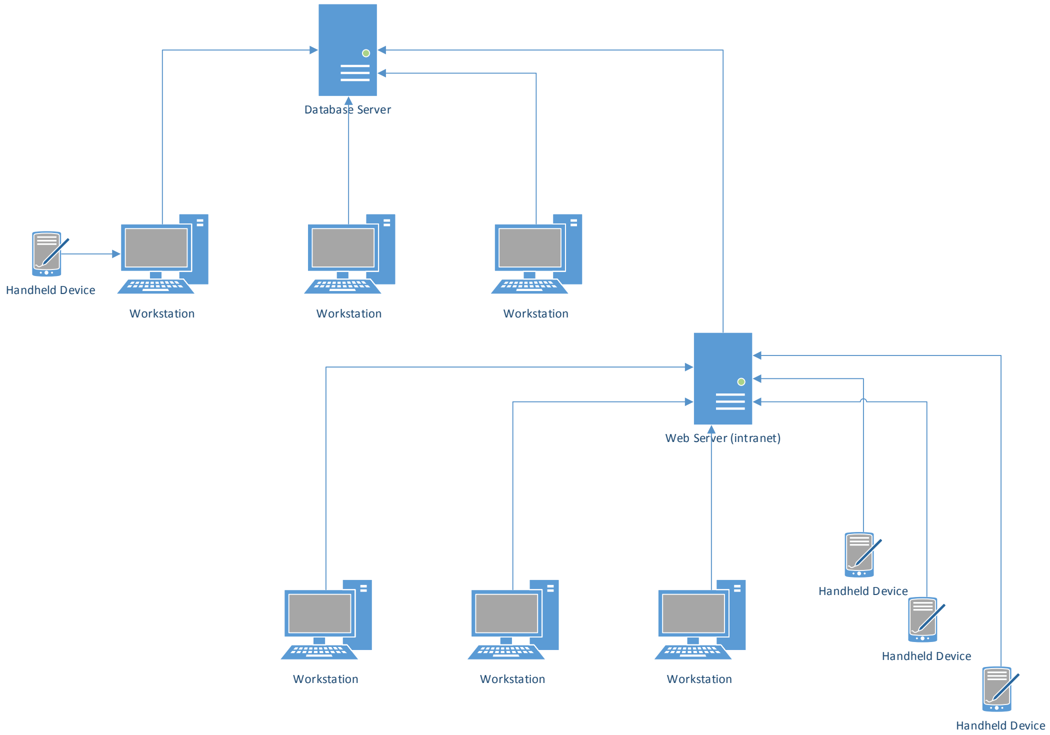

Figure 2 – Two-Server Deployment Architecture

Component Security

Operating System Security

See the following documents:

- Guide to Secure Windows Server 2008 R2 (https://technet.microsoft.com/en-us/library/dd548350%28v=ws.10%29.aspx)
- Guide to Secure Windows Server 2012 R2 and 2012 (https://technet.microsoft.com/en-us/library/hh831360.aspx)
- Guide to Secure Windows 7 (https://technet.microsoft.com/en-us/library/ee712767.aspx)
- Guide to Secure Windows 10 (https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-10-enterprise-security-guides)

Oracle Database Security

See the *Oracle Database Security Guide*.

Internet Information Services (IIS) Security

See *Security Best Practices for IIS (https://technet.microsoft.com/en-us/library/jj635855.aspx)*

2 Performing a Secure Materials Control Installation

Oracle Hospitality Materials Control Deployment Guide contains instructions and information regarding installing Oracle Hospitality Materials Control. Optional components, such as the MCweb intranet web front-end application and the intranet web services, are installed manually without an installation wizard.

Pre-Installation Configuration

Pre-installation configuration includes database schema setup. Use the password strength guidelines provided in *Oracle Database Security Guide* for setting up the database credentials.

Customized files: During installation or update, the installation wizard copies several customized files to the client application.

The Materials Control Installation

Materials Controls now stores database passwords and encryption-key defining parameters in Protected Configuration (https://msdn.microsoft.com/en-us/library/53tyfkaw%28v=vs.100%29.aspx). Storing sensitive information in a non-readable format improves the security of the application by making it difficult for an attacker to gain access to sensitive information even if the attacker gains access to the file, database, or other storage location. Materials Control uses an RSA machine-level key container, which enables us to re-use for all applications and simplifies the deployment on other PCs.

The *Oracle Hospitality Materials Control Deployment Guide* contains information and instructions for installing the application.

You cannot use Unattended Installation and Remote Update due to the changes introduced with Protected Configuration encryption.

Post-Installation Configuration

Oracle Hospitality Materials Control Password & User Account Management contains further information and instructions regarding users, groups, and passwords.

Change Admin Account

Materials Control installs with a default Admin user. You can change the login name of the default Admin user, or you can create a new user with administrator privileges and then remove all privileges from the default Admin user.

Change Default Passwords

Materials Control installs with default passwords. You must change the passwords as soon as possible.

Define Roles, Users and Permissions

Define roles and users according to your organization structure and business process. Make sure to give just enough privileges as needed for each role. You can override privileges at the user level. Keep administrative privileges for administrators only. Chapter 3 contains further information and instructions.

Activate Password Rules or LDAP login

Materials Control can enforce the following password rules:

- Expiry
- Complexity
- Blacklist
- Re-use protection.

You can activate these password rules or use LDAP login. Chapter 3 contains further information and instructions.

3 Implementing Materials Control Security

Besides encrypting and hashing sensitive information, Materials Control offers other security mechanisms, like authentication, access control and audit.

Use Password Rules

Password rules allow following:

- Force user to change password on next login.
- Force Password Expiry (in days).
- Force Password Strength with minimum length and password mask.
- Forbid Password Reuse, where system will not allow user to use one of last eight used passwords.
- Define Password Retry Count and Account Lockout.
- Password Blacklist – manage list of not-allowed passwords.
- Forbidden Passwords - block item names, login names, user names, vendor names and Cost Center names from being used as a password.
- Automatic Account Locking – lock-out accounts not in use for configurable number of days.

You cannot use the following words in the password:

- ORACLE
- MICROS
- FIDELIO
- ADMIN

Use LDAP authentication via NTLM

Linking of Materials Control users to Microsoft Windows domain users, allowing the authentication and password management on OS level. Supported by both client-server desktop application and web front-end.

Access Control

Materials Control controls access by granting privileges at the role or user level. You can implement fine-grained control by overriding role-level privileges at the user level. Besides controlling access to separate modules, privileges can control the availability of business-critical processes inside modules.

Materials Control supports the compartmentation of data by defining the access rules to data using Cost Center filtering and Ownership concept. You can use item and recipe group filtering at the role and user levels to apply finer access controls to items and recipes.

You can control certain business-critical processes using the Authorization Flow by defining a custom approvals workflow for the ordering and transfer process.

Audit

Materials Control audits the following business-critical actions in the system log:

- Login/logout
- Document status change/deletion
- Master data changes (recommended)

Appendix A Secure Deployment Checklist

This appendix lists actions that need to be performed to create a secure system.

- Install only what is required.
- Keep encryption configuration safe.
- Change default user password.
- Enforce password rules / LDAP login
- Define roles, users and their privileges. Grant necessary privileges only.
- Enforce Cost Center filtering, ownership
- Apply all security patches and workarounds.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Monitor who accesses your systems.
  - Harden the operating system.